/protector

Patentstyret
Første avdeling
Postboks 8160 Dep.
0033 Oslo

Oslo, 15. juni 2012

Deres ref.: 2010 0308
Vår ref.: P3819NO00-DT

**Patent i Norge nr.: 330271**
**Tittel: Mobil betaling**
**Søker: mCASH Norge AS**

---

Det vises til innsigelse datert 08.12.2011 oversendt fra Patentstyret 16.12.2011.

Vi er uenige med innsigeren og vil gå gjennom innsigerens punkter.

I-1 og I-2
Når det gjelder oppfinnelsens tekniske effekt antar vi at dette allerede er vurdert av saksbehandleren, og innsigeren bringer ikke noe nytt inn i sin argumentasjon. Dette er et område der det allerede foreligger andre patenter av samme type, som kjennetegnes ved hvordan deler av et system kommuniserer. Anførte P1 er et eksempel på dette.

I-2.2
Omtalte P1 er allerede diskutert og beskrevet under saksbehandlingen og i patentbeskrivelsen. I forhold til tabellen har vi følgende bemerkninger:

1. Innledningen viser at oppfinnelsene er innen samme felt.

2. En kjenningskode for terminalen, f.eks telefonnummer. Sammenligningen er den universelle (og ikke utdypede forklaringen): identification or authentication of the customer. Det er en distinkt forskjell mellom å gi terminalen en kjenningskode (f.eks. at din mobiltelefon har nummer 12345) kontra at brukeren angir et nummer 12345. mCASH skiller på terminalen og brukeren ved at terminalen har en identitet og at brukeren har en annen som bekreftes med PIN kode senere i forløpet av transaksjonen, det er summen av de 2 som utgjør tofaktor-autentisering). Innsigeren trekker her samme informasjon fra to avsnitt som ikke er direkte knyttet til hverandre og i realiteten omhandler to forskjellige ting.

**Protector IP Consultants AS**
**Adresse / address:** Oscarsgate 20, NO-0352 Oslo, Norway
**Telefon / Telephone:** (+47) 22 95 74 40
**Telefax:** (+47) 22 95 74 50
**E-mail:** mail@protector.eu
**Internet:** www.protector.eu
**Foretaksnr. / Enterprise No.:** 979409524 mva

Stavangerkontor / Stavanger office:
iPark, bygning i4, Prof. Olaf Hansensvei 7A,
(+47) 51 87 47 03

3. I foreliggende patent beskrives i detalj hvordan vår server vil være koblet til en database som inneholder nødvendig informasjon. Igjen kombinerer innsigeren to avsnitt som ikke har teknisk relasjon til hverandre, der [0024] gir en generell angivelse av kommuniksjonsnettverket og [0027] gir en diskusjon av en metode for transaksjoner, men ingen av disse avsnittene nevner bruk av en database.

4. Neste del er viktig, da man her mener å kunne sammenligne mCASH mot motpart system, noe som er helt galt. Her beskriver mCASH:
Et brukersted (butikk) som har en kasse (terminal) som kan snakke med mCASH Serveren, der mCASH Serveren kjenner kontoen som butikken vil ha sine betalinger utbetalt til. Dialogen er i patentet beskrevet som at kassen snakker med mCASH over etablert nettverk (altså en direkte dialog mellom kassen om mCASH). I sammenligningen beskrives en HELT annen løsning der kassen i butikken snakker med systemets server gjennom betalerens mobiltelefon. Dvs. at det IKKE er beskrevet noen forbindelse mellom kassen og systemet utover den som opprettes gjennom betalerens mobiltelefon. Dette er en dramatisk forskjell da det ikke vil være aktuelt å la en mobiltelefon kontrollert av brukeren ha det autoritære svaret overfor kassen.

5. Dette er ikke utdypet tilstrekkelig til å diskuteres.

6. Det er riktig at en overføringsordre sendes i begge systemene, men som nevnt over er kommunikasjonsveien en helt annen.

7.Her har vi samme kommentar som over.

8. Her er forskjellen som er avgjørende: Vi ber terminalen, når den mottar beskjed fra server, om å bekrefte betalingen med en kode (les: PIN kode). Det er ikke angitt i P1 og det er en dramatisk forskjell å ikke be kunden om å bekrefte sine belastninger med noen form for kode.

9. Belastningen blir utført. Innsigeren hopper over behovet for bekreftelse fra kunden i denne sammenligningen, en essensiell del av vårt krav, som spiller på behovet om sikkerhet i dialogen mellom partene i systemet, samt betalers bekreftelse med PIN-kode.

10. mCASH lar kassen lese av strekkode eller annen kode, mens de snakker om en kode som overleveres til kassen over en kommunikasjonskanal som er opprettet mellom enhetene. Det er stor forskjell mellom å la kassen lese av en kode, og det å sende en identifikator gjennom en forbindelse opprettet, slik som beskrevet i P1. Det angitte eksempelet: der en strekkode skannes er lett og er en etablert standard som ikke krever ny maskinvare. Å opprette en Infrarød forbindelse (slik P1 beskriver) mellom kassen og terminalen krever nytt utstyr i kassen og på i mobiltelefon, i tillegg til at det ikke inneholder kjente beskyttelser (sikring) av de data som evt. skulle bli overført. Dette er vel også den eneste "tekniske" delen av klagers patent (at de snakker om at man kobler kassen og telefonen gjennom infrarød).

Dermed finnes det vesentlige forskjeller mellom den foreliggende oppfinnelsen og teknikkens stand representert ved P1.

Når det gjelder de øvrige motholdene vil vi kommentere noen av dem
:

US2009164371
Systemet som er beskrevet ligner mye på mCASH, men med noen vesentlige unntak. For det første sendes PIN over nettverket som SMS, dette er usikkert og er noe vi evt. bør ta bort fra vår søknad om det er mulig, da vi aldri vil bruke SMS for å overføre data. Dette gir ingen sikkerhet på noe vis. Videre er teleoperatøren involvert ved at data slås opp av teleoperatøren, som tilsynelatende kan bekrefte kundens PIN, da denne er den samme son benyttes for å låse opp SIM. Det er for meg ukjent om teleoperatøren kjenner kundens PIN, da denne kan endres av kunden selv og dermed antas å være lokal for SIM-kortet (du kan endre PIN, uten adgang til nettverket), så mener jeg at grunnlaget for flyten i nevnte patent dessverre ikke fungerer. Men det berører jo ikke oss. Vi har ingen verifikasjon av data mot teleoperatøren.

US2008222048
Også her finnes noen vesentlige forskjeller. For det første benyttes igjen SMS for overføring av data mellom aktørene. Videre er det ett poeng at butikken kontakter server for å lage en kode (eksempel: Rema ringer til mCASH og sier "jeg vil ha en betalingskode verdt 150 kroner"). Server leverer en kode til butikken, som deretter butikken får kunden til å fotografere. Innholdet sendes fra brukerens telefon til server (beskrevet som SMS, men dette er ikke mulig over SMS protokollen), som der gjør oppslag av koden og finner dermed ut at brukeren ønsker å betale 150,- til butikken. For å forsikre seg om at brukeren er rette vedkommende sender server beskjed tilbake til brukere om at han må oppgi PIN. Brukeren sender PIN via SMS til server. (igjen er SMS livsfarlig). Når serveren er har godtatt brukerens identitet (pga PIN mottatt på sms) ringer serveren opp til brukeren og ber ham oppgi kredittkortinfo. Som et alternativ ser det ut til at brukeren også kan taste dette inn i en SMS.

Systemet beskriver i detalj hvordan man med offset "krypto" kan bytte rundt på kredittkort-tallene for å gjøre prosessen av å sende kredittkort rundt om kring veldig sikkert. Det er ikke korrekt at dette er sikkert, ettersom du sender data i en SMS. Systemet er åpenbart dramatisk forskjellig. Hos mCASH sender ikke brukerstedet først beskjed til server om et beløp, som deretter hentes tilbake og som brukeren skal fotografere. Utveksling av beløp skjer på serversiden (fra brukersted til mCASH og fra mCASH til bruk som så bekrefter transaksjonen)

EP1727085
Beskriver et system der en betaling blir bekreftet ved at brukere mottar en forespørsel (payment menu) til sin telefon som vedkommende må bekrefte. Den dekker også mer tekniske begreper om hvordan dette skal skje, slik som bruk av dataforbindelser og evt. programvare som kan installeres på den aktuelle telefonen. Hovedforskjellen er hvordan transaksjonen initieres. For det første skal brukeren oppgi mobilnummer til brukerstedet, som deretter sender en betalingsforespørsel til sin payment processing partner som om (eller tilsvarende) en kredittkort-transaksjon, men med bruk av mobilnummer. Dette er ikke mulig da dagens partner ikke vet hvilken kunde som finnes bak nevnte mobilnummer. Antar vi at mobilnummer er kjent av mottakeren i bakkant skal denne produsere en betalingsforespørsel som sendes til mobilen. Det er ikke angitt hvordan dette skjer, ei heller hvilken konto som belastes, annet enn at kundens konto evt. er lagret i en RFID brikke som er omtalt

senere som en ytterligere versjon av løsningen (der man altså går bort fra mobilnummer).

Ved at alle data befinner seg i RFID brukken skal man kunne belaste kontoen. Det er ingen beskrivelse om hvordan data sendes fra brukerstedet til server, fra server til bruker og deretter fra bruker til server med PIN og fra server til eieren av kontoen (bank) og deretter tilbake til både bruker og brukersted (bekreftelse på at betaling er utført). Det kan virke som om patentet i stor grad lener seg på eksisterende løsninger slik som kredittkort-prosessering (som patentet selv beskriver).

Vi anser dermed at de meddelte kravene angår en oppfinnelse som skiller seg vesentlig fra den kjente teknikk på bakgrunn av dette ber vi saksbehandleren avvise innsigelsen.

Med vennlig hilsen
**Protector IP Consultants AS**



Dag Thrane