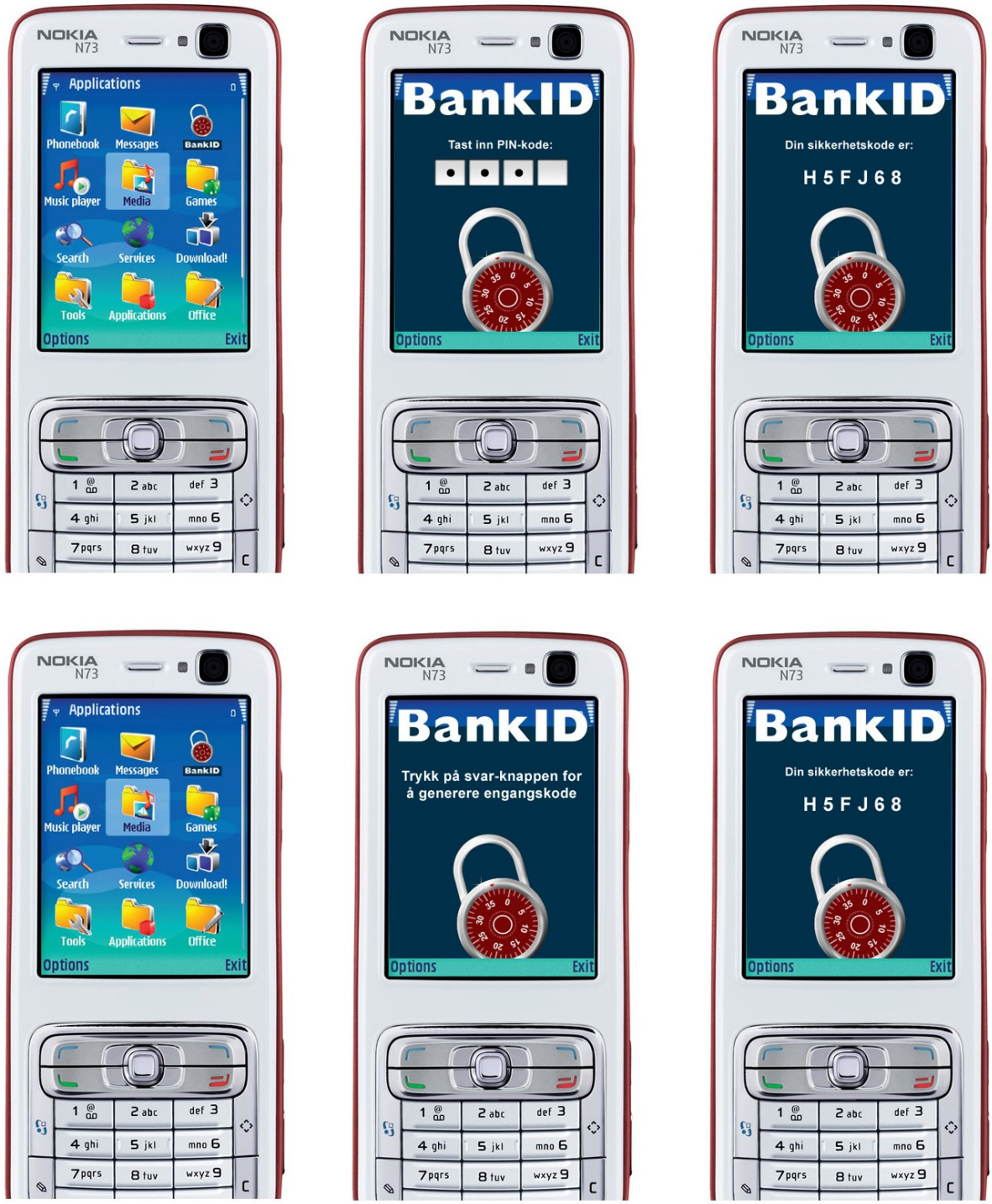
BankID

INF5261, Universitetet i Oslo

7. mai 2008



Prosjektgruppen består av:

Roni Hercz, Kestutis Mintauckis og Trond Sorvoja

Innholdsfortegnelse

Innledning

Det har nå gått flere år siden de første bankene åpnet sine første hjemmesider og begynte å tillate kundene å hente informasjon, foreta tjenestebestillinger og gjennomføre transaksjoner over Internett. Disse har gått gjennom en naturlig evolusjon, og noen av de viktigste målene i denne evolusjonen har vært å lage en nettbank som er like sikker som banken, samtidig som at den er så brukervennlig som mulig.

I disse bankenes datasystemer finnes det derfor mange forskjellige sikkerhetssystemer, hvor de fleste kan sies å være passive i den forstand at de ikke merkes av kunden, eller har direkte påvirkning på kundens bruksmønster ved bruk av nettbanken. Automatisk ut logging er et eksempel på en passiv sikkerhets funksjon. Samtidig har vi det vi kan vi kalle de aktive sikkerhetssystemene, det vil si de løsningene som har direkte påvirkning på bankkundens bruksmønster. Kodekalkulator som brukes både i innloggingsfasen og for noen banker, til å verifisere transaksjoner, er et slikt aktivt sikkerhetssystem.

Dette prosjektet vil beskrive de aktive sikkerhetsløsningene som er på markedet per i dag. I løpet av 2008 er det forventet at en aktiv sikkerhetsløsning vil bli tilgjengelig på mobiltelefon. Vi vil i oppgaven vår se bort fra selveste datasikkerheten og krypteringen til disse systemene, og heller konsentrere oss om brukervennligheten, brukerholdninger og brukeraksepten rundt de verktøyene som finnes på markedet i dag. Vi vil likevel komme inn på noen datasikkerhetshensyn hvor det er naturlig.

BankID er den mest utbredte og brukte elektroniske legitimasjonen i Norge i dag, og virker ved at kundene bruker en kodekalkulator for å identifisere seg. Som nevnt er det i løpet av 2008 planlagt å lansere BankID for mobil, som er et samarbeid mellom Telenor og BankID[1,7]

Her vil BankID applikasjonen ligge i mobiltelefonen i stedet for på egen kodekalkulator, og de nødvendige og tilhørende sikkerhetsnøklene vil ligge på SIM-kortet som er levert av teleoperatøren.

En annen tjeneste, som er opratør uavhening, er den som er under utvikling av Encap (http://www.encap.no). Den er et alternativ til BankID på mobil, og fungerer på liknende måte ved at det er applikasjon på mobiltelefonen som generer engangskoder.

En tredje mobilrelatert løsning som brukes ved innlogging i nettbank er den som brukes av for eksempel Skandiabanken, hvor kunden mottar en engangs kode per SMS som benyttes ved innlogging i nettbanken. Dette er den eneste mobilrelaterte løsningen som faktisk er i bruk av

bankkunder i dag. De andre er i skrivende stund under utvikling.

Dette prosjektet vil se på de tjenestene som er tilgjengelige eller under utvikling, hvor man kan bruke et mobil håndsett i forbindelse med innlogging i nettbanker. Prosjektet vil forsøke å finne svar på hvilken metode som er den mest brukervennlige og praktiske og som egner seg best til å være et verktøy for innlogging i nettbanker, samtidig som man tar hensyn til brukernes holdninger og bruker aksept til disse verktøyene.

Bakgrunn

Den skandinaviske banken Nordea var i 2003 den banken i verden med flest Internett-transaksjoner [4] med over 71 millioner betalingstransaksjoner i første halvdel av 2003. I følge Wikipedia utfører Nordeas 4.8 millioner nettbank kunder 200 millioner betalingstransaksjoner per år[20]. De nordiske landene blir regnet for å være langt fremme sett i forhold til befolkningens bruk av nettbanker og utviklingen av teknologiske løsninger i forbindelse med bruk av nettbank.

En av de større utfordringene med bruk av nettbank har alltid vært spørsmål om løsninger vedrørende sikkerhet. Det er hele tiden en avveining mellom brukervennlighet og behov, hvor bankene forsøker å være i forkant av de som utnytter sikkerhetshull til kriminellaktivitet. Utviklingen blir også påvirket av lønnsomhets faktorer slik at det hele tiden foregår en avveining mellom hvilke prosesser og systemer som skal utvikles og tas i bruk, satt opp mot truslene utenfra og de konsekvenser som kan følge ut fra dette [5]. Sagt med banknæringens egne ord: "En god sikkerhetsløsning vil alltid innebære en avveining mellom brukervennlighet og tilgjengelighet, sikkerhet og kostnader. "[2]

I artikkelen "Expanding the 'Mobility' concept"[9]argumenterer Kakihara og Sørensen at begrepet mobilitet bør utvides til å omfatte begrepene romlig mobilitiet, tidsmessig mobilitet og kontekstuell mobilitet. Det å være mobil, dreier seg ikke bare om at folk beveger seg og reiser, men også og mer viktig om hvordan mennesker samspiller. (I oppgaven vår ser vi på hvordan mennesker samspiller og kommuniserer med maskiner. I begge tilfeller brukes maskiner for å utføre samspillet). De argumenter videre for at også objektenes mobilitet i sammenheng med romlig mobilitet bør vurderes. Enkelte objekter er designet for at de skal brukes som om de var en del av den menneskelige kropp, og at de beveger seg sammen med den. I våre undersøkelser gjenkjenner vi dette, og ser at det finnes et følt behov for å ha med seg "nøkkelen" til å komme inn i (nett)banken til enhver tid.

Videre forklarer de forandringen av den tidsmessige orden både med at teknologi skapes for å

frigjøre tid og at søken etter frigjøring av tid skaper ny teknologi, og at den økende tidsmessige mobiliteten vedrørende menneskelig samspill både skaper nye muligheter og hindringer i det sosiale livets økologi. Dette gjenkjennes også ved at ny teknologi har ført til at kundene ikke lenger trenger å hverken gå til banken eller ha direkte (menneskelig) kontakt med bankenes kundebehandlere.

Samtidig vises det til at kontekstuell mobilitet og CMC (Computer mediated communication) eller kommunikasjon med datamaskiner fører til en anonymisering mellom for eksempel kundebehandler og kunde, som igjen kan fjerne kontekstuelle begrensinger som kunne oppstått ved en direkte ansikt-til-ansikt kommunikasjon. Dette kan kanskje være nok en grunn til at bruken av nettbanker har tatt såpass av som det har gjort, uten at vi skal gå inn på en diskusjon rundt akkurat dette i denne oppgaven.

Avgrensning / scope

Primærbrukeren av en nettbank er kundene som benytter banken til å utføre banktjenester. I utgangspunkt så inkluderer denne gruppen alle personer og organisasjoner som har en bankkonto med nettbankfunksjonalitet. Det kan være naturlig å vurdere om denne primærbrukergruppen kan deles opp i undergrupper. Personer som kun benytter nettbanken til å sjekke saldo føler kanskje at aktive sikkerhetstiltak slik som kodekalkulatorer er til større bryderi enn personer som benytter nettbanken til aksjehandel? Bedrifts brukere foretar kanskje mange transaksjoner med store beløp i løpet av en innloggingssesjon, og føler det kanskje betryggende med en separat kodekalkulator for autorisasjon ved innlogging. I dette prosjektet vil vil ikke skille mellom bedriftskunder og privatkunder, men heller se på enkeltmennesket som bruker.

Vi vil for eksempel ikke undersøke om bedriftskunder i det hele tatt føler at kalkulatorer er en ulempe i og med at de enkelt kan ha den tilgjengelig i en kontorskuff for bruk i arbeidstiden. For bedriftskunden er ulempen kanskje at man er redd for at uvedkommende skal kunne få tak i kalkulatoren og på den måten tilegne seg ulovlig tilgang til nettbanken.

Det er også viktig å være klar over at både erfaring, aldersforskjeller og kjønn kan spille, eller spiller sterkt inn på oppfattelsen av og holdningen mot bruken av nettbanker som sådan, og innloggingsproblematikken spesifikt.

Dette prosjektet vil ikke ta hensyn til dette, men oppfordrer alle som er interessert i dette til å arbeide videre med disse viklingene eller utgangspunktene. Vi ønsker altså å se på nettbankkundene under ett, og undersøke hvilke holdninger primærbrukergruppen har til bruk av

mobiltelefonen i innlogging.

Problemstilling og målgrupper

Historikk

Målgruppen er i utgangspunktet vid. Med dette mener vi at det er både ungdommer og voksne personer som er i stand til å benytte elektroniske banktjenester. Vi vil heller ikke skille mellom eldre og yngre mennesker, og i stedet forsøke å la skillet gå mellom brukere som anser seg selv som erfarne brukere kontra de som føler seg mindre erfarne.

De første nettbankene hadde ikke høyere sikkerhetsbarriere enn at de krevde et brukernavn og et passord for å la kunden logge seg inn. Dette brukernavnet var i noen banker rett og slett bare kontonummeret, mens andre banker opprettet egne brukernavn for kundene for bruk kun i nettbanken. I Norge i dag er det vanlig å bruke personnummer for å identifisere seg som bruker.

Når det gjelder passord var det en utvikling også her. Innledningsvis kunne kunden velge passord selv, i noen tilfeller med minimumskrav angående antall tegn og type tegn i passordet. Noen banker krever for eksempel at passordet byttes med jevne mellomrom, som for eksempel en gang hvert kvartal eller halvår, og man kan da ikke velge et tidligere brukt passord[6]. Det som er vanlig i Norge i dag er at man får ha et passord som er sitt eget og som man velger selv, og et passord - gjerne kalt sikkerhetskode eller engangskode - som er nytt for hver innlogging.

Måten denne engangs sikkerhetskoden brukes var tidligere ved at bankkundene fikk til sendt et ark eller et kort med en liste over for eksempel femti sikkerhetskoder. Noen banker, som for eksempel DNB, lot kunden bruke disse sikkerhetskodene i kronologisk rekkefølge slik de var listet opp på kodekortet eller arket. Etter hvert gikk bankene over til å kreve at disse sikkerhetskodene ble hentet i tilfeldig rekkefølge. Dette ble løst ved at det ved siden av koden var trykket et følgenummer, og innloggingssiden i nettbanken oppga et følgenummer for den sikkerhetskoden som skulle tastes inn. Her kunne det selvfølgelig være en svakhet dersom noen kunder strøk over allerede brukte koder med en penn, hvilket synliggjorde de siste ubrukte kodene på et ark som holdt på å bli ferdigbrukt.

Disse svakhetene og behovet for enda bedre sikkerhet førte til at bankene gikk sammen og opprettet et system kalt BankID. BankID og liknende systemer fungerer ved at kundene får til sendt en slags elektronisk kalkulator som oppgir en ny sikkerhetskode for hver gangs bruk. Noen kalkulatorer fungerer ved at kunden må taste inn en fast PIN-kode for å hente ut den unike

sikkerhetskoden, mens det for andre igjen holder med å trykke på en enkelt knapp for å hente ut koden. Felles for slike systemer er at de er dyre for bankene, fordi bankene må gå til innkjøp av små elektroniske maskiner som må sendes til en hver enkelt kunde. Kalkulatorene kan ikke oppdateres eller modifiseres etter at de er sendt ut, og kunden må ha kalkulatoren tilgjengelig for å kunne logge seg inn. Videre er det viktig å være klar over at kalkulatoren utnytter en tids synkronisering som gjør at de uthentede sikkerhetskodene kun kan brukes i løpet av en kortere tidsperiode, helt ned til bare noen få minutter.

Det at kalkulatoren ikke kan modifiseres er i og for seg en sikkerhetsfordel, men det er fordyrende både dersom kunden mister eller ødelegger kalkulator og trenger ny, eller dersom bankene ønsker å forandre sikkerhetsalgoritmene eller andre elementer som krever oppgradering av kalkulatoren – rett og slett fordi de da må sende ut nye kalkulatorer.

I og med at denne kodegeneratoren snart vil være tilgjengelig på mobilen ønsker vi å undersøke om dette er fordelaktig i forhold til separate kodekalkulatorer.

Problemstilling

Som nevnt er det blitt slik at kalkulatoren må være tilgjengelig for kunden i innloggingsøyeblikket. Dette fører til at brukeren blir tvunget til å bære denne med seg dersom hun eller han ønsker å ha muligheten til å logge seg inn i nettbanken til en hver tid. Vi anser dette som en stor ulempe, og det er denne ulempen vi ønsker å se på i denne oppgaven og som utgjør oppgavens problemstilling. Kan vi fjerne ulempen det er å bruke separate kalkulatorer for å kunne logge seg inn i nettbankene?

For eksempel må man ha denne kalkulatoren med seg om man er på reise og ønsker å ha nettbanken tilgjengelig. Noen ville kanskje anta at det holder å hente ut noen koder på forhånd og skrive ned disse på et ark til senere bruk, men det går altså ikke på grunn av tidsbegrensingen som er lagt inn i algoritmen for utkjøring av engangs koder.

På den andre siden vil det for mange brukere føles at det er ulempe å ha kodekalkulatoren på mobiltelefonen. Det betyr jo at dersom mobiltelefonen blir mistet eller stjålet, hvilket ikke er uvanlig, så vil andre mennesker potensielt sett kunne få tilgang til denne kodekalkulatoren. Noen vil kanskje altså føle at det sikreste er å la kodekalkulatoren bli liggende hjemme - eller i kontorskuffen.

Videre er det viktig å være klar over at det kan være en direkte sammenheng mellom valg av nettbank og brukervennlighet, og hvilke valgmuligheter nettbankene gir. Dette gjelder ikke bare

vedrørende innloggingsprosessen, men også etter at man har logget seg inn og ønsker å utnytte de mulighetene som foreligger enten man ønsker å kjøpe tjenester eller utføre transaksjoner. Det kan være en god ide for en annen studie å undersøke dette i en kommersiell sammenheng.

Bankene konkurrerer i dag enten på pris eller tilbud av tjenester og produkter. Kanskje de en dag også vil konkurrere om å være den mest brukervennlige banken, og ikke bare den mest kundevennlige?

Begreper

Sikker pålogging

Hver gang man skal logge seg inn i nettbanken, vil banken være sikker på at det er den rette brukeren som gjør dette. Dette skjer som oftest som oftest ved bruk en kombinasjon av passord, sikkerhetskort, kodekalkulator eller elektronisk sertifikat. Dette kalles en to-faktor løsning og er den vanligste metoden i Norge i dag.

Passord

Det er vanlig at passord blir benyttet når man skal logge seg inn på et system. Passord brukes som oftest i kombinasjon med et brukernavn. Hvis man skriver riktig brukernavn og passord, da kan banksystemet gjenkjenne at du er den riktige personen som logger inn i nettbanken.

Sikkerhetskode / Engangs kode

En sikkerhetskode er en kode som enten blir generert av en kodekalkulator eller oppgitt på et kodekort og som er unik ved hver innlogging.

Pin kode

En pin-kode er fast tallkombinasjon som kan brukes til å gi tilgang til forskjellige systemer. Denne tall kombinasjonen kan enten være bestemt av brukeren eller av en leverandør.

Kodekalkulator

Kodekalkulator er en liten kalkulator som inneholder en algoritme, det vil si en matematisk formel/beregning, som generer en engangs kode eller sikkerhetskode som brukes i forbindelse med innlogging i nettbanken.

Vanligvis finnes det to typer kalkulatorer. Den ene er med PIN-kode, det vil si at brukeren må taste inn en fire-sifrert PIN-kode for å genere engangs koder, mens den andre er uten PIN-kode. Når man har tastet enten PIN-koden eller bare trykket på en aktiveringsknapp, så får man se den

genererte sikkerhetskoden på den innebygde skjermen. Hver gang du taster inn ny PIN-kode eller trykker på aktiveringsknappen, får man oppgitt en ny sikkerhetskode.

Sikkerhetskort Et sikkerhetskort er et forhåndstrykt kort med et større antall sikkerhetskoder og tilhørende kodenummer. Sikkerhetskoden benyttes i tilfeldig rekkefølge og kun en gang i henhold til kodenummeret som oppgis ved innlogging.

BankID

BankID er en tjeneste som tilbyr en personlig elektronisk legitimasjon for sikker signering og identifisering på nettet

Jevnfør http://www.BankID.no/ og Sørensen[16]

Identifisering

I dagens samfunn er det blitt helt vanlig at person må identifisere seg ovenfor ukjente for å få utført forskjellige tjenester slik som bank tjenester. Disse tjenestene utføres oftere og oftere av maskiner, derfor har det oppstått et behov for å identifisere seg ovenfor disse. Det er i denne sammenheng at bankene har utviklet og tilbyr BankID. Det finnes også andre måter å foreta maskinell identifisering som for eksempel Bypass-løsning og pinkode fra selvangivelsen.

I Sikkerhetslovens paragraf3 [11]er autorisasjon under pkt.17 definert som:

> [En] avgjørelse, foretatt av autorisasjonsansvarlig, om at en person etter forutgående sikkerhetsklarering **(med unntak for tilgang til informasjon sikkerhetsgradert begrenset)**, bedømmelse av kunnskap om sikkerhetsbestemmelser, tjenestelige behov samt avlagt taushetsløfte, gis tilgang til informasjon med angitt sikkerhetsgrad.

Se også [12, 19, 21]

Analyse

Hva finnes på det norske markedet i dag?

Per 31.12.2006 var det 124 sparebanker, 15 forretningsbanker og 8 filialer av utenlandske banker i Norge[10]. Mange av disse bankene bruker fellesløsninger slik som de som er utviklet av for eksempel EDB. Det er særlig kun de største bankene som utvikler sine egne nettbanksystemer, slik som for eksempel DNB og Nordea. Allikevel er de norske bankene flinke til å samarbeide med utviklingen av fellessystemer. Et tidligere slikt samarbeid ble manifestert gjennom Bankenes Betalingssentral (BBS) som innførte det felles transaksjonsystemet Bankgiro [18].

Når det gjelder innloggingssystemer ser det ut som om BankID kommer til å bli det viktigste verktøyet i tiden framover; i og med at det utvikles i samarbeid med bankene.

Som nevnt tidligere kreves det en egen kalkulator for å lage engangs kodene som brukes av BankID. I tillegg finnes det fortsatt banker som bruker kodekort, mens noen banker bruker utsendelse av engangs koder per SMS til mobiltelefoner for å gi brukeren innloggingstilgang i nettbanken. Noen banker lar brukeren velge mellom flere av disse metodene.

Svakheten ved å bruke kodekalkulator er som nevnt over relatert til det at brukeren må ha kalkulatoren tilgjengelig for å kunne logge seg inn i nettbanken. Dette kan i mange tilfeller være upraktisk. Genererer man for mange koder på en gang uten å ta de i bruk, vil systemet falle ut av synkroniseringen, og forbindelsen mellom banken og kalkulatoren må nullstilles.

Et annet system som også er i bruk i Norge er det som Skandiabanken har valgt med utsendelse av engangs koder per SMS til kundens mobiltelefon https://www.skandiabanken.no/. Den store ulempen med dette sett fra kundens ståsted er at det kan skje at SMS-meldingen blir forsinket eller ikke kommer frem i det hele tatt. Det er i disse tilfellene likegyldig for kunden om det er teleoperatøren som er skyld i at han eller hun ikke mottar SMS med engangs kode når man forsøker å logge seg inn i nettbanken. Særlig ved reise i utlandet kan denne problemstillingen være godt synlig. For at bankene skal kunne sende ut SMS til kundene sine på denne måten må de enten knytte seg opp mot en leverandør av masseutsendelse av SMS (Se for eksempel: http://www.partnerportalen.no) , eller undertegne en CPA-avtale med hver enkelt mobiloperatør. Se for eksempel http://cpa.telenor.no/cpa/ .

Det første er som regel det billigste og mest hensiktsmessige for bankene så lenge de ikke trenger tilbakemeldinger fra kundene per SMS, og heller ikke ønsker å ta betalt av kundene for å få tilsendt engangskoder. Prisen på masseutsendelse ligger hos Netcom fra 21 øre per SMS (før

rabatt)[13]. Prisen man oppnår gjennom en CPA-avtale er som regel en god del dyrere, og man må også ha en egen avtale med hver enkelt av de fire mobilnettverksoperatørene som finnes i Norge (Telenor, Netcom, MTU og Network Norway) og i tillegg de operatørene som har virtuelle nettverk (MVNO) slik som for eksempel Tele2, TDC, Venteleo og Vectone her i Norge. Har man ikke disse avtalene vil ikke tjenestene fungere for disse operatørenes kunder. (Unntak gjelder for MVNOer dersom disse har egne avtaler med nettverkoperatøren som tillater oversendelse av CPA-meldinger). CPA-utsendelser gjenkjennes ofte ved at avsendernummer bruker et kortnummer på fire eller fem siffer.

Systemet som er mest gunstig er derfor enkel masseutsendelse fra vanlig nummer i stedet for fra CPA-nummer. Da holder det med en avtale med en enkelt leverandør. Vanlig masseutsendelse fungerer ved at man setter opp meldingsinnhold som sendes ut til en liste med mottakere. I bankenes tilfelle fungerer dette litt annerledes ved at meldingens innhold blir generert for hver utsendelse, og at det på forhånd ikke finnes noen lister over mottakere. Dette blir uansett besørget av bankens egen server. I denne prosessen er det per dags dato ikke behov for å legge inn spesielle sikkerhetsterskler, og den er nettverks uavhengig. Prosessen fungerer ved at man under innlogging i nettbanken klikker på en knapp som trigger utsendelsen av SMS-meldingen med engangskoden. Denne meldingen blir så sendt til et forhåndslagret telefonnummer, som kunden ved en tidligere anledning har definert.

Fordelene med et slikt system er at man ikke trenger å utvikle egne kalkulatorer som igjen må sendes til kundene. Prismessing er det for oss vanskelig å vite om dette systemet fører til en kostnadsbesparelse i forhold til utsendelse av kodekalkulatorer, fordi dette kommer an på hvor ofte man må sende kalkulatorer til kundene sammenliknet med prisen man oppnår per SMS-utsendelse. For at det skal være billigere å sende ut engangs koder per brev, bør man sende kanskje 50 engangs koder per utsendelse fordi bare brevportoen koster minst kr. 5,70 .

Ulempen med SMS-utsendelse av engangs koder er som nevnt over at de ikke alltid kommer frem[3]. En annen ulempe er at gamle SMS-meldinger bør slettes fra telefonen. Dette krever at kunden enten en gang i blant, eller etter hvert SMS-mottak, sletter mottatt melding. Det er viktig å bemerke at det ikke har noen sikkerhetsmessige konsekvenser dersom kunden utelater å slette disse meldingene fra mobilhåndsettet.

Fordelen med SMS-utsendelse sett fra kundens ståsted er stor. Hun eller han trenger ikke å bære med seg en egen kalkulator, og det er nærliggende å anta at de fleste enkeltpersoner i dag har en mobiltelefon tilgjengelig. I tillegg kan man forhåndsdefinere flere mobilnumre for mottakelse av

SMS, slik at flere i en familie eller bedrift kan motta kode, og dersom man har abonnement hos flere operatører eller til og med bruker egne mobilabonnement i utlandet. Ekstra bra er det at dette systemet er uavhengig av typen mobiltelefon og operatør kunden har. Dersom kunden bytter mobilhåndsett så vil dette fortsatt fungere. Dersom kunden bytter mobilnummer, så må denne sørge for å definere det nye nummeret i banksystemet.

Det er viktig å bemerke at Skandiabanken benytter seg av et sertifiseringsystem

(https://www.skandiabanken.no/SKCert/GIBCert/Login.aspx), hvor brukeren må laste ned et sertifikat på datamaskinen sin for å kunne logge seg inn i nettbanken. Kontoholderen får til sendt en e-post hver gang et slikt sertifikat lastes ned, og dette øker sikkerhetsnivået i den forstand at det ikke går an å logge seg inn i nettbanken fra datamaskiner hvor kontoholder ikke vet at det er lastet ned et sertifikat. Det er verdt å merke seg at Skandiabanken har laget en nettapplikasjon som kunden kan bruke for å logge seg inn i nettbanken, eller mobilbanken som det da i blant blir kalt, uten bruk av slikt sertifikat. Har du fått tak i en annen persons mobiltelefon, og kjenner personnummeret, så holder det å finne ut hva det personlige passordet er for å kunne logge seg på. Engangs passordet som kreves blir jo sendt til mobiltelefonen. Usikkerhet rundt dette er gått beskrevet i hovedoppgaven til Thomas Tjøstheim ved Universitetet i Bergen[17]

Konsept

For å oppsummere kan vi si at vi har tre forskjellige måter å tilegne seg engangskoder. Man kan lese ut fra et til sendt kodekort trykket på et papirark, man kan bruke en tilsendt kodekalkulator eller man kan få til sendt kode per SMS. I tillegg må vi huske at man vil kunne laste ned applikasjoner på mobiltelefonen som muliggjør innlogging direkte i mobilbank, det vil si, ikke i nettbank. Et norsk firma som har jobbet mye med dette og har et nært samarbeid med bankene er Systek[17]. De tilbyr en mobil-løsning som bankene kan modifisere og tilpasse til sitt eget tilbud og profil, som brukeren kan benytte for å gjennomføre for eksempel banktransaksjoner. Andre systemer er de som holder på å bli lansert av BankID og Encap (http://www.encap.no/)

Vår ide er å beskrive og undersøke mottakelsen og brukervennligheten ved en egen applikasjon som kan ligge på det mobile håndsettet, slik at det kan generere engangs koder og sammenliknet med for eksempel til sendelse av engangs koder per SMS. I denne forbindelsen er det noen hensyn og avveininger man må drøfte. Under har vi listet opp syv innfallsvinkler vi ønsker å undersøke for å finne svar på om en slik applikasjon kan være riktig løsning:

1. Skal det være slik at man må taste inn en PIN-kode hver gang man generer en engangskode? Er det nødvendig? Hva taler for og i mot?
2. Hvilke mobiloperativsystemer skal eller bør applikasjonen fungere på?
3. Kan man bruke teknologier som SMS, hidden-SMS eller dataoverføring for å oppdatere applikasjonen, holde den i live, generere nøkler etc?
    - Hva med kostnader relatert til dette?
    - Hva med innstillings oppsett ved bruk av dataoverføring?
    - Hva skjer dersom applikasjonen ikke får kontakt med serveren?
    - Hva skjer dersom kunden bytter mobilabonnement og/eller operatør?
4. Hva skjer dersom brukeren bytter mobilhåndsett? Hvordan sørger man for at tidligere applikasjon blir deaktivert?
5. Vil brukerens oppfattelse av systemets sikkerhet være tilfredsstillende? Når og hvorfor vil brukeren foretrekke andre metoder?
6. Installasjons prosessen. Hvordan kan installering av et slikt system på kundens mobilhåndsett gjøres brukervennlig nok til at kunden faktisk vil bruke det?
7. Hvilke tanker har bankene rundt dette i dag?

Prototyper

Prototyper et et godt verktøy for å diskutere og undersøke design ideer, prototyping blir regnet for å være en viktig del av design prosessen. Prototyping kan bidra til å avdekke svakheter og feil ved design, og til å oppdage elementer som ikke var klart definert i spesifikasjonsfasen.

I forbindelse med dette prosjektet så er papir prototying et godt alternativ. Papir prototyper krever få ressurser å utvikle, gir mulighet til å evaluere flere design konsepter samtidig, er egnet for å evaluere skjermbilder og for å avdekke nye bruker krav. Vi ønsker derfor i forbindelse med sluttevalueringen å utvikle et par papirprototyper som kan evalueres av brukere slik at vi kan komme frem til en løsning som tar hensyn til tilbakemeldingene fra brukerne.

Et annet viktig aspekt, særlig når man snakker om mobilapplikasjoner, er hvordan man får applikasjonene på mobilen. Dette kan enten være forhåndslagret i mobilen, på SIM-kortet eller man kan laste det ned eller overføre det fra andre mobiler og datamaskiner. I tillegg er det ofte man trenger å foreta diverse innstillinger. I blant sendes disse usynlig for brukeren, men ofte sendes de i form av SMS-meldinger fra leverandøren av tjenesten. Noen ganger må man foreta disse innstillingene manuelt. Dette pleier å være meget tungvint selv for erfarne brukere, og det

gjør heller ikke saken lettere at det er så mange forskjellige mobiloperativsystemer og versjoner ute. Dette skaper dessuten mye hodebry for tjenesteleverandøren.

En tredje aspekt dreier seg om typen installasjon som for eksempel den som er ment brukt av BankID på mobilen. Der er det slik at selveste applikasjonen blir liggende på telefonen, eller mobilhåndsettet, mens de private PKI-nøklene blir liggende i SIM-kortet[14]. Telenor på sin side hevder at dette er gunstig fordi de mener at SIM-kortet kan knyttes opp mot brukeren[14]. Dette er ikke nødvendigvis riktig i og med at det er veldig lett å skaffe seg et SIM-kort, under falskt navn og også lett å identifisere eieren av en funnet mobiltelefon. Å skaffe seg annen persons personnummer gjøres enklest ved å ringe til Skatteetaten og få oppgitt personnummer på en navngitt person man ønsker å bruke, for deretter å f.eks. kjøpe et SIM-kort i butikken og deretter registrere det selv over SMS, telefon eller Internett med denne informasjonen.

Telenor skriver også "Brukerstedet har avtale med Telenor om tilgang til PKI-baserte funksjoner i SIM-kortet til brukeren".[14]. Dette innebærer også problemer fordi en tredjepart, nemlig mobiloperatøren, blir en del av formelen. Mest sannsynlig vil teleoperatøren, i dette tilfellet Telenor, ta seg betalt for disse tjenestene. Dessuten blir tjenesten operatøravhengig noe som er ugunstig for brukeren og fører til en ufrivillig binding mot en leverandør som egentlig ikke er partner i denne konstellasjonen. Dette berører spørsmålene rundt prinsippet om at nettverksleverandørene ikke skal kontrollere innholdet, enten det gjelder Internett eller mobiltrafikk[8]

Når dette er sagt, ønsker vi å lage prototyper av og sammenlikne følgende fire modeller:

1. Skandiabankmetoden - utsendelse av SMS til brukeren med engangs kode som deretter tastes inn i nettbankens innloggingsvindu. Dette krever ingen installasjon foruten registrering i nettbanken.
2. Pin-kode løs metode - egen applikasjon på SIM-kortet som generer engangs koder bare ved å kjøre applikasjonen, dvs. uten å kreve PIN-kode.
3. Encapmetoden - egen Java-applikasjon lastet inn på mobilen som generer engangs koder etter inntasting av PIN-kode. Krever kun engangs installasjon av programvare.
4. BankID-metoden - egen Java-applikasjon som ligger på mobilen, men som henter PKI-nøkler fra SIM-kortet. Krever engangs installasjon av programvare og binding til spesifikt SIM-kort.

Når det gjelder de to siste modellen så er de i prinsippet helt like for brukeren så lenge man ikke skifter SIM-kort. Her ønsker vi derfor også å se litt på installasjons prosessen og viktigheten for

brukeren til ikke å være bundet mot et spesifikt SIM-kort.

Når det gjelder "Vår metode" så vil hovedspørsmålene dreie seg om:

1. Vil det være sikkert nok å generere engangs koder uten inntasting av PIN-kode? (Det gjøres slik med vanlig BankID kodekalkulator i dag.
2. Vil brukerne oppfatte at det er sikkert og trygt nok å bruke en slik metode?
3. Vil bankene mene at dette er sikkert nok?

Evaluering

Evalueringen av prototypene skal foretas på et utvalg av brukere som vil kunne være typiske brukere av disse innloggingsmetodene på mobiltelefon. Vi vil i denne fasen ikke ha samtaler med banker eller organisasjonene som i dag jobber med utviklingen av slike verktøy for å høre om hvilke tanker de har om dette, og eventuelt om det er andre problemstillinger vi ikke har kommet inn på ennå. Dette overlater vi til de som fortsetter på oppgaven vår.

Vi vil forsøke å finne svar på hvilken innloggingsmetode eller prosess brukeren foretrekker, også sett i lys av sikkerhetsoppfattelsen av denne prosessen. Vil vil også forsøke å sette dette i et relevant perspektiv som kan ha med andre ting å gjøre, som for eksempel hva som er mest praktisk og kostnadseffektivt for bankene.

Brukerundersøkelser

Om nettbank og BankID

Vi har gjennomført strukturerte intervju med 14 personer om bruk av nettbank og BankID.

Nettbank benyttes

Det overveldende flertall benytter seg i dag av nettbank, med 12 som svarer bekreftende på dette spørsmålet med to negative svar. Men bare en person benytter seg i dag av mobilbank, med tretten negative svar.

BankID var ukjent for mange

På spørsmål om man kjenner til BankID og man kjenner igjen BankID logoen var gruppen delt i

to. Seks kjenner til BankID og 8 kjenner ikke igjen BankID, 8 kjenner der i mot igjen BankID logoen, mens seks ikke kjenner den igjen. Dette viser at BankID ikke er noen veletablert merkevare, og at noen benytter seg av BankID uten å gjenkjenne dette.

Hvordan nettbank benyttes

Av de som benytter nettbank så var det seks som benyttet kort med koder, og seks som benyttet seg av SMS sendt på kode i fra banken. Fire benyttet kodekalkulator som ikke krever PIN-kode, mens fire benytter som av kodekalkulator som benytter PIN-kode. Det antas at de seks som fikk tilsendt kode fra banken er Skandiabanken kunder fordi dette er den eneste banken som er kjent som bruker av et slikt system i dag.

Vilje til bruk av BankID på mobiltelefonen

Det viser seg at 7 var villig til å benytte seg av en applikasjon på mobiltelefonen som var levert av BankID, mens 6 ikke kunne tenke seg dette. Det bemerkes at flere sa seg villig til å benytte seg av en slik applikasjon enn de som kjente til bank ID. Så det kan antas at folk stoler på en tjeneste bare den er der. Litt færre var villige til å benytte en applikasjon som ikke var levert av bank ID, med fem positive mot syv negative svar. Der i mot så var det flere 9 positive mot 4 negative som var villig til å laste ned å installere en slik applikasjon på mobiltelefonen, dette kan skylles at en slik mulighet det kan være fint å ha i bakhånd som en reserveløsning.

Sikkerhet er viktig

Det overveldende flertall syntes det var meget eller noe viktig at en slik kodegenererende applikasjon var beskyttet av pin kode, men det merkes at to ikke syntes dette var viktig. På spørsmålet om at det var lette å identifisere eieren til applikasjonen så var det også et overveldende flertall som syntes dette var negativt eller noe negativt, kun to svarte at det ikke var negativt i det hele tatt.

BankID blir betraktet som en banktjeneste og ikke som en mobiltjeneste

Mindretallet var villig til å bytte mobiloperatør for å få tilgang til BankID, men det merkes av tre av tretten svar svarte at de var villige til å gjøre dette.

På spørsmålet om hvilken kundeservice man ville ringe til ved problemer med en BankID applikasjon så mente de fleste (10svar) at de ville ringe bankens kunde service, mens tre ville ta kontakt med mobiloperatøren. Dette viser at BankID blir oppfattet som en bank tjeneste, og ikke i

like stor grad som en mobiltjeneste.

Hvor lange er brukere villig til å ikke ha tilgang til nettbank

På spørsmål om hvor mange dager personene var villig til å være uten tilgang til nettbank ved problemer med BankID applikasjonen så svarte alle at de ikke var vilig til å vente (9 svar på 0 dager) eller vente svært kort tid(2 svar på 1 dag). Dette viser at det er liten aksept for tekniske problemer med selve tjenesten. Ved spørsmål om hvor lenge man var villig til å vente hvis mobilen var sperret på grunn av ikke betalt regning, så svarte 9 at de ikke ville akseptere å være uten nettbank (0 dager), en var villig til å være uten nettbank i en dag, og en var villig til å vente i 7 dager. Dette viser at en slik applikasjon ikke blir oppfattet som en del av mobilabonnementet, men som en helt uavhengig tjeneste.

Ved bytte av SIM-kort var det større spredning i svarene, men de fleste (6 svar) var ikke villig til å vente (0 dager), 2 var villig til å være uten nettbank i en dag, og en person var mulig å være uten nettbank i 2 dager. Kun to person var villig til å vente i fem dager eller mer.

Ved bytte av mobiloperatør så var det en noe større aksept for at man ble uten nettbank, 4 var ikke villig til å vare uten nettbank (0dager), mens 4 var villig å å være uten nettbank i en eller to dager (3 svar på en dag, ett svar på to dager), 3 personer var villige til å være uten nettbank i fem dager eller mer.

På spørsmål om man forventer at BankID på mobiltelefonen skulle fungere i alle banker man har konto i svarte 3 at det var nok at det virket i kun en bank, mens 10 svarte at applikasjonen burde virke i alle banker.

Nedlasting og installasjon

På spørsmål om hvor lang tid man var villig til å vente på nedlasting av BankID så var en person ikke villig til å vente. Fem var villige på å bruke ett minutt. Fire var villige til å bruke fem minutter, mens 4 var villige til å bruke lengere tid. Det merkes at en bruker var villig til å benytte 30 minutter og en var villige til å bruke en time.

Hver tredje bruker er villig til å betale for å laste ned BankID

På spørsmål om man var villig til å betale for å laste ned BankID svarte 4 ja, mens 9 svarte nei.

Om levering av engangs kode per SMS

For å undersøke holdninger og erfaringer brukere har til levering av engangs koder per SMS gjennomførte vi strukturerte intervju med 9 brukere. I intervjuet skillet vi mellom de som var Skandiabanken kunder og de som ikke var det.

Vi snakket med 4 som ikke var kunder i Skandiabanken og 5 som var det.

De som ikke var Skandiabanken kunder

Av de som ikke var Skandiabanken kunder var det 2 som benyttet kodekalkulator med pin kode og 1 som benyttet kodekalkulator, med pin kode. To av de spurte mente levering av engangs passord per SMS kunne være et alternativ til bruk av kodekalkulator. De som var positiv mente at så en fordel i at hun ikke trengte å ha kodekalkulatoren tilgjengelig hvis passordet kom per SMS, mens en av de som var negativ mente at SMS kunne være en fordel hvis kodekalkulatoren ikke var tilgjengelig.

Skandiabanken kunder

Av de fem Skandiabanken kundene vi snakket med så var det tre som foretrakk å benytte kodekort, mens tre kun benyttet passord levering via SMS.

Erfaringer med levering av passord per SMS

To hadde opplevd å ikke få levert bestilt SMS med engangs passord, og på spørsmål om hvor lenge de var villige til å vente på at SMSen skulle leveres var svarene 10 sekunder, opptil et halvt minutt, umiddelbart og inntil 5 minutter. To brukere hadde opplevd at mottatt engangs passord ikke var gyldig. Skandiabanken lar brukerene registrere mer enn ett mobilnummer i nettbanken, men kun en av de spurte hadde gjort det, denne brukeren hadde også bestilt engangs passord til levering til andre telefonnummer enn sitt primærnummer. To av de spurte hadde bestilt engangs passord fra utlandet, og begge hadde erfaring med problemer med å få levert passordet.

Sikkerhet

Samtlige av de spurte opplevde levering av engangs passord per SMS som trygt. En var bekymret for å bli frastjålet lommebok og mobil samtidig, mens en annen mente at å bli frastålet telefonen ikke var noe skumlere enn å bli frastjålet et kodekort. Den tredje var overhode ikke bekymret for sikkerheten. Ingen av de spurte var bekymret for at kontoen sin kunne bli tappet hvis de mistet

mobiltelefonen, en bemerket at tyven fortsatt ville trenge PIN-koden. To av brukerne ville varslet Skandiabanken hvis mobiltelefonen ble stjålet, mens en bruker ikke ville varslet Skandiabanken i det hele tatt hvis mobilen kom på avveie.

Ulemper med SMS-leveranse av passord

En bruker påpekte sikkerhet som en ulempe med SMS-levering av passord. Brukeren sa at sikkerhetskortet alltid er i leiligheten, mens SMS alltid ble brukt ute slik som på jobb og på hytta. Faren i følge denne brukeren var at hvis lommeboken blir stålet samtidig som mobilen så vil tyven være i besittelse av kontonummer, personnummer og mobilen som benyttes til å ta i mot engangs koder.

En annen bruker påpekte at det var en ulempe å måtte slette SMS-meldinger med engangs koder, og at engangs kodene var så lange at det var vanskelig å huske de uten å se på mobilen to ganger.

Den siste brukeren kunne ikke påpeke noen ulemper med engangs kode levering per SMS.

Konklusjon

BankID og andre mobilrelaterte løsninger for innlogging i nettbank blir for det meste regnet for å være banktjenester, hvilket ser ut til å ha en betryggende påvirkning på bankkundens villighet til å prøve produktet. Samtidig innføres nye aktører i forhold til innloggingsprosessen, hvilke kan ha en uønsket effekt på samspillet mellom nettbanken og bankkunden. På den ene siden viser det seg at noen kunder har opplevd begrensninger med Skandiabankens løsning, mens andre igjen tydeliggjør baksiden ved at en BankID-applikasjon er knyttet til en spesifikk mobiloperatørs SIM-kort.

Uansett, så er og vil forskjellige løsninger til å bruke mobiltelefonen som verktøy for innlogging i nettbanken manifestere seg. Teknologien ser ut til å muliggjøre bruken og presse frem nye bruksmønstre, og skaper med det et behov som kanskje tidligere var ukjent. Dog virker det tydelig at jo mer IKT-kyndig man er, jo mer villig er man til å bruke, og mer ønskelig er det for disse med en mobilrelatert løsning.

Dersom man var sikret å ikke ha problemer med mottak av SMS med Skandiabankens løsning ville nok dette ha vært vinneren. Den kanskje minst ønskelige løsningen ser ut til å være den som snart vil bli lansert av BankID fordi den skaper en kunstig binding mellom bankkunde og mobiloperatør. Tilsvarende er Encap sin løsning meget gunstig fordi den gjør den samme jobben som BankID, bare uten å være knyttet til mobiloperatørens SIM-kort.

Et annet viktig hensyn vedrørende applikasjoner som ligger på mobilhåndsettet er behovet for nedlasting og installering av programvare. Nedlasting kompliserer villigheten til å ta systemet i bruk, både på grunn av at det koster penger å laste ned programvare med mobilen, og fordi det kan være vanskelig for mange å installere slik programvare. Igjen ser det ut til at dette er en mindre terskel å forsere for de som betegnes som IKT-kyndige.

I tillegg er det viktig å være klar over den opplevde sikkerheten i de forskjellige systemene og hvilken uttalt påvirkning dette har på viljen til å ta i bruk teknologien. De langt fleste ønsker for eksempel at det skal kreves PIN-kode for å genere engangs koder, selv om det kanskje ikke kreves av dagens kodekalkulatorer, og ihvertfall ikke for å lese av forhåndstrykte kodekort.

Videre kan man se en formildende faktor i det at tjenesten i det hele tatt eksisterer, eller kommer til å eksistere, og at den er eller blir levert av bankene selv. Denne faktoren, at banken leverer denne tjenesten, senker terskelen for å ta den i bruk.

Referanser

1)BankID.no, "Telenor og en samlet banknæring lanserer BankID på mobil", http://www.BankID.no/index.db2?id=3845 (hentet 11.03.08)

2)DnbNor.no, seminar om BankID, https://www.dnbnor.no/portalfront/nedlast/no/bedrift/kurs_seminar/BankID/080204GS_BankID_publ.pdf (hentet 10.03.08).

3)DnbNor, "SMS tjenester", https://www.dnbnor.no/person/mobilbank/sms/sporsmal_svar.html

4)Digi.no,"Nordea har verdens mest brukte nettbank", http://www.digi.no/php/art.php?id=92429 (hentet 03.03.08)

5)e24.no, "Sikkerhet lønner seg ikke for nettbanker", http://e24.no/it/article2233891.ece (hentet 10.03.08)

6)fibi.co.il, "Data Security", http://www.fibi.co.il/fibi/site/en/fibi.asp?pi=245&doc_id=4148 (hentet 02.05.08)

7)Finansnæringens hovedorganisasjon, "Faktaark Bank ID på Mobil", http://www.fnh.no/Faktaark_BankID_p_mobil_GqJ63.doc.file (hentet 12.03.08)

8)IDG.no,"Vil signere for det offentlige": http://www.idg.no/bransje/bransjenyheter/article17935.ece).

9)Kakihara og Sørensen,"Expanding the 'Mobility' concept", London School of Economics and Political Science, 2001

10)Kreditttilsynet, Tilsyn med bank, finans og forsikring, http://www.kredittilsynet.no/wbch3.exe?p=1184, (hentet 03.03.08)

11)Lovdata, Sikkerhetsloven, http://www.lovdata.no/all/hl-19980320-010.html#3, (hentet 03.03.08)

12)Nasjonal sikkerhetsmyndighet,"Autisisasjonshåndboka med rettelser", http://www.nsm.stat.no/Documents/Handboker/Autorisasjonshaandboka_mrettelser%20201206.pdf (hentet 29.02.08)

13)Netcom, "CPA priser", https://netcom.no/omnetcom/partnere/cpa-innholdsleverandorer/priser.html?fane=trafikkavgifter

14)Sjursen, H, "Erfaringer og planer for Telenor og bankenes BankID løsning", http://www.studiemotet.no/Images/Assets/2007%20bilder/07s1f2.pps

15)Systek, "Verdens mest brukervennlige mobilbank?", http://www.systek.no/losninger.aspx?docid=100

16)Sørensen G. "Behov for sikkerhet ikke lenger en hindring", Næringslivsdagene 2004 Tromsø

17)Tjøstheim, T, "A critical view on Public Key Infrastructures" - http://www.ub.uib.no/elpub/2004/h/413001/Hovedoppgave.pdf

18)Wikipedia, Bankgiro, http://en.wikipedia.org/wiki/Bankgiro (hentet 03.03.08)

19)Wikipedia, "Identifikasjon", http://no.wikipedia.org/wiki/Identifikasjon)hentet 29.02.2008])

20)Wikipedia, "Nordea", http://en.wikipedia.org/wiki/Nordea (hentet Mar. 3, 2008, 11:54 CET)

21)Wikipedia, "Sikkerhet",http://no.wikipedia.org/wiki/Sikkerhet (Hentet 29.02.2008)