Midtveis rapport

«BANK ID»

INF5261 Utvikling av mobile informasjonssystemer

”Det eneste vi vet med sikkerhet er at alt er usikkert”

Francois de Voltaire
1694 – 1778

Innhold

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 utlogging 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 analysere de aktive sikkerhetsløsningene som er på markedet per i dag, for deretter å se om det finnes alternative løsninger som kan være gunstigere for brukeren å ta i bruk. Vi vil i oppgaven vår se bort fra selveste datasikkerheten og krypteringen til disse systemene, og heller konsentrere oss om brukervennligheten rundt verktøyene som finnes og se på mulige forbedringer av disse. 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 har som regel fungert ved at kundene bruker en såkalt kodekalkulator for å identifisere seg. Nå er det i løpet av 2008 planlagt å lansere BankID for mobil, som er et samarbeid mellom Telenor og BankID (se http://www.bankid.no/index.db2?id=3845, hentet 11.03.08) og (se http://www.fnh.no/Faktaark_BankID_p_mobil_GqJ63.doc.file, hentet 12.03.08). 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 nettverksuavhengig, er den som er utviklet 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 autoriseres ved å sende en SMS med et engangspassord til kundens mobiltelefon.

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.

Bakgrunn

Den skandinaviske banken Nordea var i 2003 den banken i verden med flest Internett-transaksjoner [Se Digi.no,Nordea har verdens mest brukte nettbank, http://www.digi.no/php/art.php?id=92429 (hentet Mar. 3, 2008, 11:54 CET)] 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.[Se Wikipedia, Nordea, http://en.wikipedia.org/wiki/Nordea (hentet Mar. 3, 2008, 12:03 CET]. 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 og 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 egen vinning. Utviklingen blir også påvirket av lønnsomhetsfaktorer 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 [Se e24.no, Sikkerhet lønner seg ikke for nettbanker, http://e24.no/it/article2233891.ece (hentet Mar. 3, 2008, 12:35 CET)]. Sagt med banknæringens egne ord: "En god sikkerhetsløsning vil alltid innebære en avveining mellom brukervennlighet og tilgjengelighet, sikkerhet og kostnader. " https://www.dnbnor.no/portalfront/nedlast/no/bedrift/kurs_seminar/bankid/080204GS_bankid_publ.pdf (hentet Mar. 10, 2008, 23:25 CET).

Brukere

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 brydderi enn personer som benytter nettbanken til aksjehandel? Bedriftsbrukere 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 vinklingene eller utgangspunktene. Vi ønsker altså å se på nettbankkundene under ett, og undersøke på et generelt grunnlag hvordan vi kan gjøre innloggingsprosessen enklere for disse.

Problemstilling og målgrupper

Målgruppen er i utgangspunktet vidt. 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 (Eksempel: http://www.fibi.co.il/fibi/site/en/fibi.asp?pi=245&doc_id=4148). 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 tilsendt 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 tilsendt 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 tidssynkronisering 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. Det jobbes nå med å lansere en BankID for mobil i løpet av 2008.

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 engangskoder.

På den andre siden vil det for mange kanskje være en følelsesmessig ulempe for noen 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 oppgave 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 deg som logger seg inn i nettbanken. Det er som oftest i bruk en kombinasjon av passord, sikkerhetskort, kodekalkulator eller elektronisk sertifikat. Hvis man bruker en kombinasjon av personligkode og engangskode, kalles det to-faktorløsning.

TO-FAKTORLØSNING

To-faktorløsning er en kombinasjon av en personlig kode sammen med kodebrikke/kortleser. Når man logger inn i nettbanken, så taster man først inn en personlig kode (dvs. fødselsnummer og personlig kode). Etter dette må man trykke på kodebrikke, eller kodekalkulator, for å få generert en engangskode. Kode kan bestå av for eksempel åtte siffer, men man må kanskje bare taste inn de første seks sifrene. De to siste sifrene er da bare ment som kontrollsifre for brukeren. Hvis de to siste sifrene ikke stemmer overens med det som vises på nettbankens hjemmeside, må man kontakte med banken. Hvis alt er i orden, så godtar systemet disse kodene, og tillater brukeren å komme inn i nettbanken.

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.

KODEKALKULATOR

Kodekalkulator er en slags liten kalkulator (se bildet) som inneholder en algoritme, dvs. en matematisk formel/beregning, som generer en engangskode eller sikkerhetskode som brukes i forbindelse med innlogging i nettbanken.

Vanligvis finnes det to typer kalkulatorer. Den ene er med PIN-kode, dvs. at brukeren må taste inn en fire-sifret PIN-kode for å genere engangskoder, 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 ny sikkerhetskode. Hvis legger inn med den riktige genererte koden, så vil systemet til banken godkjenne deg som rettmessig bruker av nettbanken og logge deg inn.

SIKKERHETSKORT

Et sikkerhetskort fungerer på nesten samme måte som en kodekalkulator, men det finnes ikke noen PIN-kode slik at man kan generere sikkerhetskoder. På sikkerhetskortet er det på forhånd trykket opp mange koder, som er nummerert i en betemt rekkefølge. Brukeren får mulighet til å benytte engangskoden bare en gang og det er banken som spør etter den konkrete koden (for eksempel Kortnummer 55219 og kodenummer 17). Når man taster alt riktig da er man velkommen inn i nettbanken.

NETTSVINDEL - TROJANERE

Svindlerne kan skaffe seg tilgang til en konto ved å plante et datavirus på brukerens datamaskin. Ulike sikkerhetskoder vil ikke stoppe denne typen angrep, blir det hevdet i Bergens Tidende [se BT.no, http://www.bt.no/na24/article356698.ece (hentet den 5. Mars 2008, 23:10)]. Her blir det fortalt at det er kriminelle som lager et datavirusprogram i form av trojanere. Disse onde programmene sprer seg på forskjellige PC´er og ligger inne på brukernes PC´er og overvåker aktivitetene.

Hvis bruker logger seg inn i banksystemet, så våkner datavirusprogrammet. Etter at det er blitt samlet nok informasjon om brukeren, blir denne informasjonen sendt tilbake til bakmenn. Denne informasjon inneholder opplysninger om kontonumre i Norge, hvilke kontonummer pengene skal overføres til, eiernes fornavn, etternavn, adresse etc.

BankID

BankID er en personlig og enkel elektronisk legitimasjon for sikker identifisering og signering på nettet. Jevnfør http://www.bankid.no/ (Hentet 10. Mar, 2008. 23:30 CET). Se også denne lenken for presentasjon av BankID (Behov for sikkerhet ikke lenger en hindring): http://www.norinnova.no/content/download/63790/206332/file/Grete%20Sørensen%20-%20040321GS_BankID_NLD_2004_Tromso.pdf

Forskjell mellom identifisering og autorisasjon, kort om sikkerhet

"Identifikasjon er fastslåelse av identitet og brukes for å fastslå en persons identitet ved å sammenlignet målte biologiske mønstre mot en database som inneholder lagret informasjon om personer og deres biologiske mønstre" skriver Wikipedia. Det finnes flere måter å måle biologiske mønster på som for eksempel fingeravtrykk, håndavtrykk, signatur, DNA, regnbuehinne osv.

Identifisering

Formålet med identifisering er at uvedkommende blir hindret i å gjøre ulovlige operasjoner.

I dagens samfunn er det blitt helt vanlig at person må identifisere seg når man skal benytte for eksempel åpne e-mail boks for å lese nye meldinger, netthandelen, ta ut penger fra minibank etc. Bank tilbyr elektronisk legitimasjon såkalt BankID, slik at banksystemet kunne identifisere kunden. Det finnes også andre måter å identifisere seg over internet som for eksempel Bypass-løsning og pinkode fra selvangivelsen.

I Sikkerhetslovens $3 [Se Lovdata, Sikkerhetsloven, http://www.lovdata.no/all/hl-19980320-010.html#3, (hentet Mar. 3 13:18 CET)]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, tjenestelig behov samt avlagt taushetsløfte, gis tilgang til informasjon med angitt sikkerhetsgrad.

Dette innebærer at en får tillatelse fra offentlig myndighet for å gjøre en bestemt virksomhet for eksempel man som vil jobbe som nettverksadministrator må ha Microsoft Certified Professional (MCP) sertifikat. Dette er bevis for at denne personen er autorisert på dette fagfelt. En annen eksempel kan være en tolk. Hvis man vil jobbe som tolk, må man bestå autorisasjonsprøve. Hensikten med dette er at myndigheten vil kontrollere alle som driver med virksomheten.

Ut fra disse opplysningene over kan vi klart skille ut forskjellen mellom identifisering og autorisasjon.

Et annet nøkkelbegrep som vi vil nevne er sikkerhet. Sikkerhet er et begrep som omfatter hvilke sannsynligheter det er i forhold til at uønskede situasjoner kan oppstå. Sikkerhet er i de fleste fagdisipliner knyttet til begrepene risiko, hendelse, frekvens og konsekvens, skriver Wikipedia.

Når vi tenker på datasikkerhet så er det et begrep som beskriver sikring av data informasjon. Som oftest er informasjonen tilgjengelig for identifiserte brukere, men tvert imot for uvedkommende.

Fagområder som datasikkerhet, informasjonssikkerhet og IT-sikkerhet er knyttet til nøkkelbegrepene integritet, konfidensialitet og tilgjengelighet. Nøkkelbegrepet konfidensialitet betyr å sikre at en bruker har tilgang til informasjon. Integritet betyr å sikre at informasjon er

korrekt og fullstendig, mens tilgjengelig betyr å sikre at bruker får adgang til informasjon innenfor de krav som er satt.

http://no.wikipedia.org/wiki/Identifikasjon [Besøk: 29.02.2008]

http://www.nsm.stat.no/Documents/Handboker/Autorisasjonsh%C3%A5ndboka_mrettelser%20201206.pdf [Besøk: 29.02.2008]

http://no.wikipedia.org/wiki/Sikkerhet [Besøk: 29.02.2008]

Analyse

Hva finnes på det norske markedet i dag?

Per 31.12.2006 var det 124 sparebankar, 15 forretningsbankar og 8 filialer av utenlanske banker i Norge. [Se Kreditttilsynet, Tilsyn med bank, finans og forsikring, http://www.kredittilsynet.no/wbch3.exe?p=1184, (hentet Mar. 3, 13:36 CET)].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 transaksjonssystemet Bankgiro [Se Wikipedia, Bankgiro, http://en.wikipedia.org/wiki/Bankgiro (hentet Mar. 3, 2008, 13:44 CET)].

Når det gjelder innloggingssystemer ser det ut som om BankID kommer til å bli det viktigste verktøyet i tiden framover. Som nevnt tidligere kreves det en egen kalkulator for å lage engangskodene som brukes av BankID. I tillegg finnes det fortsatt banker som bruker kodekort, mens noen banker bruker utsendelse av engangskoder 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. Tar man ut 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 engangskoder per SMS til kundens mobiltelefon https://www.skandiabanken.no/ (Hentet 10. Mar, 2008. 23:30 CET). Den store ulempen med dette sett fra kundens ståsted er at det hender for mange ganger 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 engangskode 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 (https://netcom.no/omnetcom/partnere/cpa-innholdsleverandorer/priser.html?fane=trafikkavgifter) fra 21 øre per SMS (før rabatt), og med en slik pris er dette til og med billigere enn å sende ut engangskoder trykket på papir og sendt som vanlig post. 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 nettverksoperatøren som tillater oversendelse av CPA-meldinger). CPA-utsendelser gjenkjennes ofte ved at avsendernummer ofte er 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 nettverksuavhengig. 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. Prismessig er det 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 engangskoder per brev, bør man sende kanskje 50 engangskoder per utsendelse fordi bare brevportoen koster minst kr. 5,70 . Men som nevnt tidligere, så kan slike brev utgjøre en sikkerhetsrisiko.

Ulempen med SMS-utsendelse av engangskoder er som nevnt over at de ikke alltid kommer frem. (Se: https://www.dnbnor.no/person/mobilbank/sms/sporsmal_svar.html) En annen ulempe er at gamle SMS-meldinger må 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 sertifiseringssystem (Se: 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 tilsendt 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. Dog er det litt komisk 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. Engangspassordet som kreves blir jo sendt til mobiltelefonen. Usikkerhet rundt dette er gått beskrevet i hovedoppgaven til Thomas Tjøstheim ved Universitetet i Bergen i 2004 (A critical view on Public Key Infrastructures - http://www.ub.uib.no/elpub/2004/h/413001/Hovedoppgave.pdf)

Konsept

For å oppsummere kan vi si at vi har tre forskjellige måter å tilegne seg engangskoder. Man kan lese ut fra et tilsendt kodekort trykket på et papirark, man kan bruke en tilsendt kodekalkulator eller man kan få tilsendt 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 (http://www.systek.no/losninger.aspx?docid=100). 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 brukervennligeheten ved en egen applikasjon som kan ligge på det mobile håndsettet, slik at det kan generere engangskoder sammenliknet med for eksempel tilsendelse av engangskoder per SMS. I denne forbindelsen er det noen hensyn og avveininger man må drøfte. Under har vi listet opp syv innfalsvinkler 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 innstillingsoppsett 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. Installasjonsprosessen. 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 svaketer å 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 papirprototyer 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 forskellige mobiloperativsystemer og versjoner der 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. (Se litt om disse planene her: http://www.studiemotet.no/Images/Assets/2007%20bilder/07s1f2.pps). Telenor på sin side hevder at dette er gunstig fordi de mener at SIM-kortet kan knyttes opp mot brukeren. (www.fnh.no/Faktaark_BankID_p_mobil_GqJ63.doc.file). Dette er ikke nødvendigvis riktig i og med at det er veldig lett å skaffe seg et SIM-kort, under falskt navn. 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". (http://www.studiemotet.no/Images/Assets/2007%20bilder/07s1f2.pps). 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 denne konstellasjonen. Dette berører spørsmålene rundt prinsippet om at nettverksleverandørene ikke skal kontrollere innholdet, enten det gjelder Internett eller mobiltrafikk. (Se også "Vil signere for det offentlige": http://www.idg.no/bransje/bransjenyheter/article17935.ece).

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

1. Skandiabankmetoden - utsendelse av SMS til brukeren med engangskode som deretter tastes inn i nettbankens innloggingsvindu. Dette krever ingen installasjon foruten registrering i nettbanken.
2. Vår metode - egen applikasjon på SIM-kortet som generer engangskoder bare ved å kjøre applikasjonen, dvs. uten å kreve PIN-kode.
3. Encapmetoden - egen Java-applikasjon lastet inn på mobilen som generer engangskoder etter inntasting av PIN-kode. Krever kun engangsinstallasjon av programvare.
4. BankID-metoden - egen Java-applikasjon som ligger på mobilen, men som henter PKI-nøkler fra SIM-kortet. Krever engangsinstallasjon 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 installasjonsprosessen 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 engangskoder 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. Vil vil også forsøke å ha samtaler med banker eller organisasjonene som i dag jobber med utviklingen av slike verktøy for å høre litt om hvilke tanker de har om dette, og eventuelt om det er andre problemstillinger vi ikke har kommet inn på ennå.

I evalueringsprosessen vil vi bruke flere annerkjente evalueringsmetoder. 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.