INTERNATIONELLA HANDELSHÖGSKOLAN
HÖGSKOLAN I JÖNKÖPING

Användarnas förtroende för mobila tjänsters säkerhet

– Vilka säkerhetskrav uppfyller mobila betalningstjänster och vilket förtroende finns för sådana tjänster?

Filosofie Magisteruppsats Informatik

Författare: Linus Andersson
Mattias Johansson

Handledare: Jörgen Lindh

Jönköping 2006 juni

JÖNKÖPING INTERNATIONAL BUSINESS SCHOOL
Jönköping University

User trust in the security surrounding mobile services

– Trust and performance regarding mobile security?

Master thesis in Informatics

Author: Linus Andersson
Mattias Johansson

Tutor: Jörgen Lindh

Jönköping 2006 June

Magisteruppsats inom Informatik

Titel: Användarnas förtroende för mobila tjänster säkerhet.

Författare: Andersson, Linus
Johansson, Mattias

Handledare: Jörgen Lindh

Datum: 2006-06-07

Ämnesord: Mobil säkerhet, mobila transaktioner, användares förtroende för mobil säkerhet, Internetsäkerhet

---

Sammanfattning

Tekniken kring mobiltelefoni är under ständig utveckling och mobiltelefonen har idag fått nya funktioner utöver dess grundfunktion röstsamtal. Efterfrågan efter nya mobila tjänster drivs hela tiden framåt då mobilen får allt större kapacitet och prestanda. Bland de tjänster som växts fram märks möjligheten att utföra monetära transaktioner. Detta innebär helt enkelt att använda sin mobiltelefon för att betala och utföra allehanda tjänster kopplade till användarens monetära tillgångar. Överföringen av pengar kräver dock hög säkerhet. Vad vet egentligen konsumenterna om säkerheten kring dessa tjänster? Många betalningar och transaktioner sker idag över Internet och bankerna förmedlar budskapet om att säkerheten runt deras Internettjänster är mycket hög, men vad säger de om säkerheten för deras mobila alternativ? Finns den höga säkerheten även för de mobila tjänsterna och har användarna förtroende fullt ut för dessa?

Finns inte användarnas förtroende för säkerheten hos de nya mobila tjänsterna kommer de troligtvis inte heller användas. Vi ämnar därför i denna uppsats utreda om säkerheten i en mobil betalningstjänst motsvarar den som finns när den utförs på en dator i hemmet och har detta i slutändan användarnas förtroende?

Syftet med detta arbete är att undersöka vilket förtroende användarna har för säkerheten hos mobila betalningstjänster samt om dessa tjänster uppfyller samma säkerhetskrav som när de används via normal datoranvändning.

Studien påbörjades med en genomgång av befintlig litteratur inom säkerheten för mobilt Internet samt Internetanvändande vid hemdatorn. Sedan genomfördes intervjuer av personer med stor kunskap kring säkerheten hos mobilt Internet. För att få reda på användarnas förtroende kring mobila betaltjänster genomförde vi sedan en webbaserad surveyundersökning varvid en fokusgruppsundersökning användes till hjälp gällande framtagningen av frågorna. Utfallen från intervjuerna samt surveyundersökningen analyserades sedan tillsammans med utvald teori.

Våra resultat visar att majoriteten av respondenterna inte känner förtroende för säkerheten hos mobila betalningstjänster. De flesta anser att det inte är lika säkert att surfa via mobilen som via datorn i hemmet. Däremot kan hälften av individerna i populationen tänka sig att betala över Internet med mobiltelefonen och en betydande del kan även tänka sig att utföra finansiella affärer med hjälp av mobiltelefonen. Vi anser också att en mobiltelefon inte når upp till samma säkerhetsnivå som hos en stationär dator med fast Internet.

Master Thesis in Informatics

Title: User trust in the security surrounding mobile services.

Authors: Andersson, Linus
Johansson, Mattias

Tutor: Jörgen Lindh

Date: 2006-06-07

Subject terms: Mobile security, mobile transactions, user trust for mobile security, Internet security

---

Abstract

The mobile technology is under constant development and the mobile phone today has many other functions besides just talking. The demand for new mobile services is constantly getting stronger since the mobile phone becomes more and more powerful. Among these services is the possibility to perform transactions of money. With this we mean using the mobile phone to pay bills and other services that is connected to a user's assets. The transaction of money of course requires high security. What do the consumers know about the security surrounding these kinds of services? Today many payments and transactions that involve money takes place over the Internet from the home computer and the banks that offers these services claims that this is safe. But what do they say about the security surrounding their mobile alternatives? Does the necessary security exist for these mobile services and does it have the consumers trust?

If the users do not trust the security surrounding the mobile service, they will probably not use them. We will therefore with this thesis try to investigate if the security that surrounds the mobile payment services is equivalent to when the services is used on a home computer and if the services has the users trust?

The purpose with this thesis is to investigate the users trust regarding mobile payment services and if these services fulfil the same security demands as when they are used normally at the home computer.

The study began with a review of existing theories regarding the security for mobile Internet and Internet usage on the home computer. Thereafter interviews took place with experts having great knowledge regarding mobile Internet security. We then performed a web-based survey to get information about the users trust for the security surrounding mobile payment services. We used a focus group with the aim of helping us selecting relevant questions for the survey. The results from the interviews and the survey study were then analyzed with the chosen theory.

On the basis of our survey we can draw the conclusion that the majority of respondents do not trust the security that surrounds mobile payment services. The majority is of the opinion that it is not as safe to use mobile Internet services as to use the corresponding service from the computer at home. However half of the population could very well consider paying bills with the mobile phone and a large part of the respondents would also like to use financial transactions with this kind of media. We also conclude that a mobile phone does not reach the security standard of a home computer.

Författarnas tack

Vi vill inledningsvis tacka dem som hjälpt oss att genomföra denna uppsats
och så generöst delat med sig utav sin tid och kunskap;

Jörgen Lindh, Filosofie doktor
Universitetslektor informatik
Internationella Handelshögskolan i Jönköping
– för bra handledning och feedback i vårt uppsatsarbete

Anders Larsson, Senior Officer WIP
– för trevligt bemötande vid intervju

Joakim von Braun, von Braun Security Consultants
– för trevligt mottagande och hjälp vid intervju och hänvisningar

---

Svein Willassen, Simcon
– för trevligt bemötande vid intervju

Stefan Axelsson, System manager Ericsson AB
– för trevligt bemötande vid intervju

Fokusgruppens medlemmar
– för tid och aktivt deltagande i fokusgruppen

Klas Åkerskog, Bollplank och Kontaktkoordinator
– för all hjälp och tid du ägnat åt oss

Tor Karlsson, konstruktör av webbenkät
– för all hjälp och tid du ägnat åt oss

Innehåll

Figurförteckning

Bilagor

1 Inledning

1.1 Bakgrund

Mobiltelefoni är i dag en välkänd teknik som mer och mer integreras i samhället. Begreppet definieras av National Encyklopedin som ”ett radiosystem som medger anknytning av mobila terminaler till det publika telenätet” (National Encyklopedin, 2005). Sedan tekniken med mobila telenät tog fart 1981, i och med att Bell Telephone Laboratories och de nordiska televerken introducerade var sitt system som klarade av landsomfattande analoga teletjänster, har tekniken varit under ständig utveckling (National Encyklopedin, 2005).

Den senaste tekniken som nu är i drift är tredje generationens mobiltelefoni (3G, förklaras i ordlistan, bilaga 13) som introducerades i Europa 2002 (National Encyklopedin, 2005). Standarden för detta system kallas UMTS (Universal Mobile Telecommunications System), vilken strävar efter att ge användarna ett världstäckande mobilt kommunikationssystem, som på ett effektivt sätt skall kunna erbjuda olika tjänster upp till 2 Mbit/s (National Encyklopedin, 2005).

Användandet av mobiltelefoner ökar hela tiden och i en undersökning utförd av Stelacoin 2003 innehade 86 % av samtliga svenska hushåll en mobiltelefon. I takt med att fler människor använder mobiltelefoner ökar samtidigt utbudet konstant med tjänster utanför telefonens grundfunktion röstsamtal. SMS var den första tjänst som idag ligger i paritet med utnyttjandet av röstsamtal bland det svenska folket (Stelacoin, 2003). Men i och med att mobiltelefonerna hela tiden får större kapacitet att behandla avancerade funktioner drivs efterfrågan av mobila innehållstjänster hela tiden framåt (Aspiro, 2005).

Bland de många tjänster som under senare tid växt fram återfinns möjligheten att utföra monetära transaktioner via mobiltelefonen; att helt enkelt använda sin mobiltelefon för att betala och utföra allehanda tjänster kopplade till användarens monetära tillgångar. Hos Nordea kan exempelvis kunderna idag bland annat överföra pengar mellan konton och betala räkningar via mobiltelefonen (Nordea, 2005). Ericsson har tillsammans med Eurocard testat tekniker som gör det möjligt för konsumenten att betala med mobiltelefonen i affärer (Ericsson, 2001). Mastercard och Nokia har med hjälp av telefonens radiosignaler testat ett betalningssystem i USA (Nokia, 2003). Utvecklingen för dessa företag tyder på att möjligheterna att i framtiden använda sin mobiltelefon för allehanda transaktioner kan bli mycket vanliga.

Överföring av pengar kräver dock hög säkerhet. Det största motivet till detta är självklart att förhindra brott, men också för att övertyga kunderna om att börja använda dessa transaktionstjänster. Om säkerheten hos mobila enheter kan läsas i Computer Sweden från 2005-06-17 att Sverige är bäst på denna sorts säkerhet i världen med produkter som Appgate och Columbitech. Vackra ord med vad vet egentligen konsumenterna om säkerheten bakom de tjänster som används idag?

Många betalningar och transaktioner sker redan idag över Internet. I en undersökning gjord av bankföreningen 2003 fanns det hela 5,2 miljoner internetbankskunder i Sverige (Svenska bankföreningen, 2004). Enkelheten och möjligheterna att själv hemma eller direkt på sitt företag utföra sina bankbehov istället för att faktiskt bege sig till själva banken tycks vara en mycket populär företeelse. Givetvis ser bankerna potentialen inom denna nya sektor och utvecklingen av tjänster för detta kommer vi säkerligen att se lång tid framöver.

Bankerna förmedlar budskapet om att säkerheten runt deras Internettjänster är mycket hög, men vad säger de om säkerheten för deras mobila alternativ? När banktjänsterna övergår

till att finnas direkt i våra mobiltelefoner måste naturligtvis säkerheten vara mycket hög. Kundernas förtroende för mobila banktjänster tror vi skapas genom god service men även genom hög säkerhet. Finns den höga säkerheten för de mobila tjänsterna och har användarna fullt förtroende för dessa?

1.2 Problemdiskussion

Runt de nya mobiltelefontjänsterna där konsumenten kan utföra betalningstjänster och köp av varor/tjänster uppkommer vissa frågor. Först kring de rent tekniska aspekterna som:

- Är det lika säkert att utföra banktjänster och betalningar via en mobiltelefon som via en stationär dator med fast Internet?
- Finns det några skillnader mellan dessa två förfaranden rent säkerhetsmässigt?

De svar vi erhåller från de ovan nämnda frågeställningarna kan sedan ligga till grund för utformningen av en undersökning som riktas mot allmänheten. Denna undersökning ämnar att ge svar på vad användarna anser om dessa tjänster. Intressanta frågor som allmänheten kan ge svar på är:

- Har användarna förtroende för säkerheten hos tjänster av dessa slag?
- Är de användare som idag utför betalningstjänster via sin hemdator även beredda att utföra dessa via sin mobiltelefon?
- Finns behov hos användarna att utföra bank- och betalningstjänster via sin mobiltelefon?

Det är i slutändan användarna som bestämmer om ett koncept kommer att bli framgångsrikt och användas. Finns inte användarnas förtroende för säkerheten hos de nya mobila tjänsterna kommer de troligtvis inte heller användas. Vi ämnar därför i denna uppsats utreda om säkerheten i en mobilbetalningstjänst motsvarar den som finns när den utförs på en stationär dator och har detta i slutändan användarnas förtroende?

1.3 Forskningsfrågor

Följande frågor kommer att vara huvudfrågorna i uppsatsen:

1. Har användarna förtroende för säkerheten hos mobila betalningstjänster?
2. Är det lika säkert att utföra betalningstjänster och betalningar via en mobiltelefon som hos en stationär dator med fast Internet?

1.4 Syfte

Syftet med detta arbete är att undersöka vilket förtroende användare har för säkerheten hos mobila betalningstjänster, samt om den här typen av tjänster uppfyller samma säkerhetskrav som gäller vid normal datoranvändning.

Med normal datoranvändning menas här stationär dator med fast Internet.

1.5 Avgränsning

Uppsatsen avgränsas till att undersöka säkerheten kring banktjänster som utförs via en mobiltelefon. Genom att avgränsa uppsatsen till att undersöka en typ av tjänst där ett mycket högt säkerhetstänkande alltid behövs, anser vi att uppsatsen täcker in frågan om samma säkerhet finns i det mobila systemet som i det fasta. Vi anser även att avgränsningen till banktjänster är lätt att tillfråga allmänheten om då många idag använder just bankernas tjänster från hemmet. Avgränsningen utgör heller inget hinder för att i uppsatsen dra slutsatser om andra betalningstjänster för den mobila marknaden, då vi anser att avgränsningen inte hindrar från att få svar på hur tjänsterna inom denna sektor fungerar.

1.6 Intressenter

Resultatet av uppsatsen ämnar ge kunskap gällande säkerheten hos mobila Internettjänster och om vad allmänheten anser om säkerheten med mobilt Internetanvändande. Därav är uppsatsens intressenter alla företag som på något sätt har en verksamhet där de använder mobila tjänster, där betalningsmoment eller andra penningtransaktionsmoment ingår med banker. Detta för att få vetskap om användarna har förtroende för dessa tjänster, samt om en tillräckligt stor massa är intresserad.

Det kan även vara intressant för utvecklare av mobiltelefoner att identifiera vad användarna är intresserade av för att anpassa telefonerna för framtiden.

Ur akademisk synvinkel är arbetet av intresse för forskning inom mobil säkerhet och resultatet bör i viss mån kunna ses som ett vetenskapligt bidrag till utvecklingen av framtidens säkerhetssystem för mobil säkerhet.

2 Metod

2.1 Kunskapsanalys

Vårt uppsatsarbete inleddes med en inledande undran som växte fram hos oss som uppslag till denna magisteruppsats. Denna undran föddes ur våra erfarenheter, genomgånga kurser samt personliga reflektioner kring det allmänna säkerhetsmedvetenhetandet i dagens samhälle. Den utveckling som idag pågår och som hela tiden genererar mer och mer avancerade maskiner och tekniska lösningar fruktar vi även kan öppna dörrar för säkerhetsmässiga brister. Vi tror att tekniken kanske går väl fort fram ibland och eventuellt missas bitar i säkerhetstänkandet. Likväl tror vi att gemene man många gånger kan ha svårt att inneha en uppfattning om hur de nya systemen fungerar och om dessa är säkra.

Tanken som har fötts genom detta resonemang utmynnar i att vi ställer oss skeptiska till många företags idag utåt sett mycket positiva förhållningssätt till nya applikationer och tjänster. Nygjorda applikationer och tjänster ser vi dagligen inträda i samhället, vilka i många fall verkar vara goda förbättringar i det moderniserande samhället. Men vi får känslan av att säkerhetsmedvetenheten ibland glöms bort eller försakas gentemot viljan att skapa nya produkter. Mer eller mindre alla nya system ser vi senare ha brustit mot normala säkerhetsregler då de har hackats eller på annat sätt gjorts tillgängliga genom att någon förbipasserat de system som skall hålla obehöriga borta från informationen.

I vår kandidatuppsats granskade vi en befintlig turistapplikation för mobiltelefoner. Detta område tycktes oss intressant, varvid våra tidigare återgivna tankar konfronterades med denna teknik. Allt detta har mynnat ut i vår undran om hur säker mobiltelefontrafiken egentligen är idag?

2.1.1 Kunskapskaraktärisering

Med utgångspunkt från resonemanget i föregående avsnitt utvecklades våra två huvudfrågor, vilka återgavs i inledningskapitlet under punkten 1.3. För att besvara de två frågorna vi fastställt till våra två huvudfrågor måste vi utreda vilken kunskap som bör utvecklas för att ge svar på dessa. Detta gör vi genom en kunskapskaraktärisering som ger oss svar på vilken typ av kunskap vi behöver utveckla (Goldkuhl, 1998).

För att besvara den första frågan behöver vi utveckla kunskap om vad användare av mobila betaltjänster anser om säkerheten. Vi ser också, för att svara på andra frågan, att vi behöver ta fram kunskap rörande de tekniska aspekterna runt mobiltelefonsäkerhet och hur dessa skiljer sig från fast Internet och dess säkerhet. Här behöver vi få förståelse kring vad som används och hur detta används för att om möjligt detektera eventuella brister eller påvisa vad som håller en god säkerhetsnivå

För att få fram kunskap om allmänhetens förtroende för mobiltjänsters säkerhet vill vi ta fram en förklarande kunskap. Detta därför att vi vill just få svar på vad användarna anser i säkerhetsfrågor relaterade till mobiltelefoni, samt att kunna bygga vidare på detta och se om det föreligger någon 'mjuk kausalitet' som förklarar användarnas uppfattningar, s k meningspåverkan. På detta sätt kan sägas att vi utvecklat en hypotesform som en del av vår undersökning (Goldkuhl, 1998). Hypotesformen används här för att undersöka om det finns en misstro hos användarna mot säkerheten vid användandet av mobiltelefontjänster och om detta leder till att tjänsterna används i mindre omfattning?

I nästkommande steg, där vi vill få svar på de tekniska bitarna avser vi att ta fram karaktäriserande kunskap för att förklara hur säkerheten kring de mobila tjänsterna fungerar. Vi av-

ser att explorativt och komparativt utreda de uppfattningar från olika aktörer som finns och väva samman dessa med den textanalys som finns nedtecknad inom området mobiltelefonsäkerhet. Genom detta avser vi frambringa en förklarande kunskap som om möjligt kan överföras till normativa handlingsföreskrifter för att generera råd och riktlinjer kring säkerheten runt mobiltelefontjänster.

Vi strävar alltså i denna uppsats efter att ta fram svar på vad användarna av mobiltelefontjänster anser om säkerheten och om detta påverkar det allmänna användandet av mobila tjänster. Dessutom vill vi ge ett svar på hur säkerheten kring mobiltelefontjänster fungerar idag och om möjligt se till de eventuella brister som finns och då föreslå förbättringsstrategier för dessa.

2.1.2 Design av genomförande

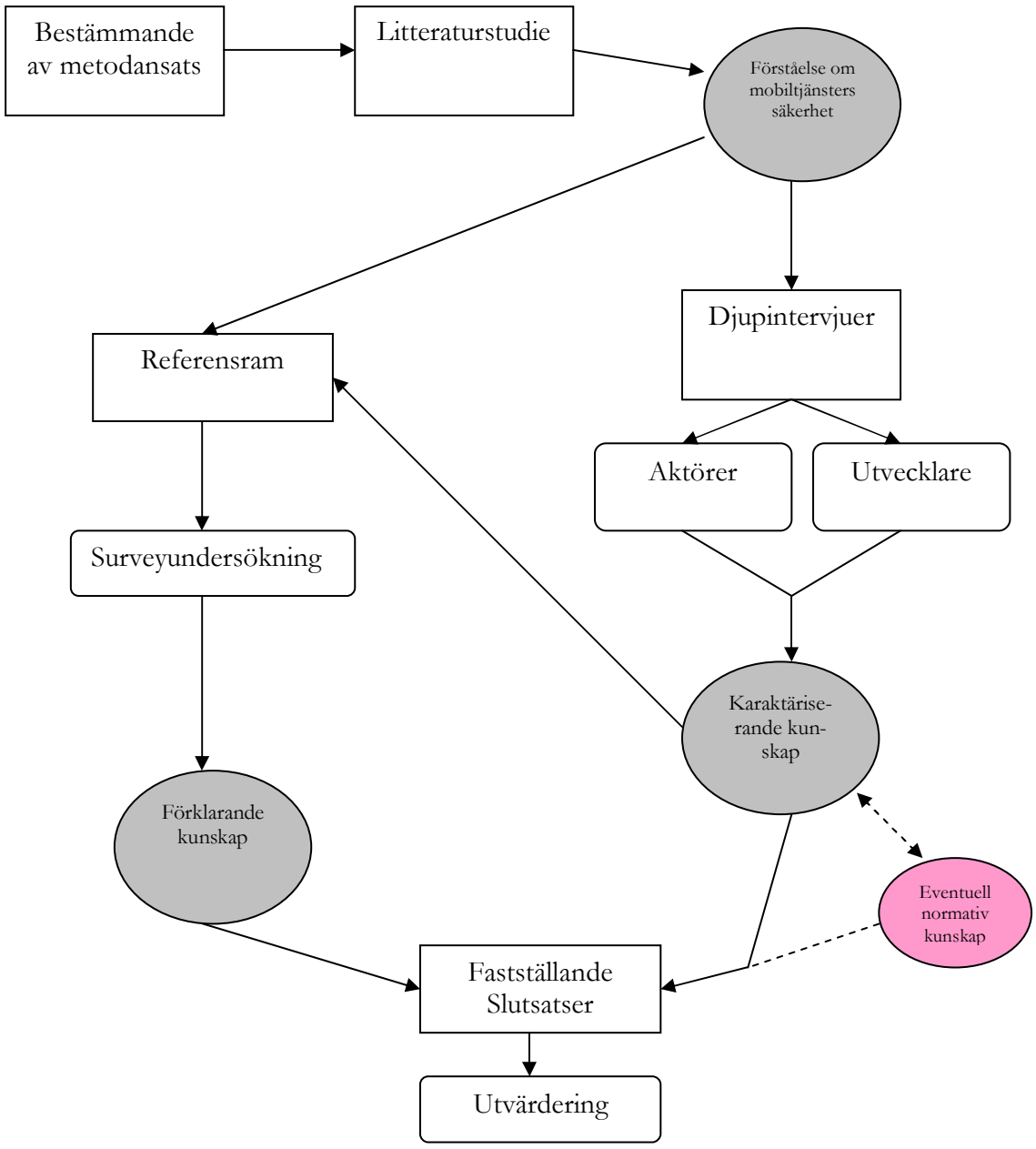
För att nå den kunskap vi vill generera avseende de tekniska aspekterna kommer vi att genomföra en litteraturstudie inom områdena mobiltelefonsäkerhet och Internetsäkerhet. Vi ämnar ej beröra ämnen inom förtroende och förtroendeskapande då vi inte har för avsikt att psykologisera och teoretisera kring hur förtroende skapas/etableras eller vidmakthålles.

Genom litteraturstudien vill vi få en grundförståelse inom ämnet för att sedan kunna genomföra djupintervjuer med några aktörer som förmedlar mobiltelefontjänster, samt någon aktör som utvecklar dessa tjänster. Denna ansats tror vi leder fram till information som kan hjälpa oss att besvara forskningsfråga 2, samt om möjligt (beroende av resultat) utveckla normativ kunskap om detta.

Detta ger oss en förståelse för mobiltelefoners säkerhet, vilket leder oss vidare till vår hypotes om allmänhetens förtroende för mobila betaltjänster. Denna önskar vi undersöka genom en surveyundersökning vars mål är att ge oss information som gör att vi kan svara på vår första forskningsfråga.

Inom ramen för surveyundersökningfasen planerar vi också för en fokusgrupp, vilken kommer att fungera som ett diskussionsforum för att stärka kvalitén hos undersökningen, samt eventuellt kunna bidra till ytterligare förståelse av användarnas syn kring mobiltelefontjänsters säkerhet.

Vi presenterar en struktur av vårt arbete i en arbetsmodell (se figur 1).



Figur 1 – Arbetsplanering

2.2 Metodansats

I uppsatsarbetet kommer vi att använda oss av två metoder; kvalitativ och kvantitativ undersökning. I första delen av vår undersökning genomförs kvalitativa intervjuer. Detta för att vi vill uppnå djupare kunskap om ett visst fenomen, då krävs det enligt Andersen (1994) en kvalitativ undersökning. Stor vikt läggs vid att forskningsprocessen uppfattas som en tvåvägskommunikation mellan forskare och studerat fenomen (Andersen, 1994). Vi är ute efter att erhålla en djupare förståelse för hur företagen arbetar med säkerhetsfrågor för mobiltelefoner respektive Internettjänster, vilket medför att nämnt metodval passar bäst. En kvalitativ analys av ett färre antal företag bör kunna ge djupare förståelse och en bred kunskapsgrund gällande dessa företag. Ett annat sätt att samla in kvalitativa data är genom att använda en fokusgrupp där olika frågeställningar diskuteras bland deltagarna (Ritchie &

Lewis, 2003). Fokusgruppens roll kommer främst att vara att hjälpa oss att ta fram en passande surveyundersökning.

Nästkommande fas består av en kvantitativ studie. Vi avser i denna del av undersökningen att utforma en surveyundersökning som tar vara på användarnas åsikter kring betaltjänster. Litteraturstudien avser att generera kunskap om de tekniska lösningarna vad gäller säkerheten hos mobilt Internet, medan information om användarnas förtroende avses erhållas från surveyundersökningen. Andersen (1994) beskriver också att det inte utan vidare går att sätta igång med en kvantitativ undersökning. Författaren pekar på att först måste en kvalitativ kartläggning göras för att lära känna det aktuella forskningsområdet, sedan måste också ett pilottest genomföras för att kontrollera de frågor som är tänkbara för enkätundersökningen. För att få precisa observationer måste forskarna enligt ovan nämnda författare objektivt mäta dem. Ett pilottest kommer först att genomföras för att vi skall erhålla feedback på de tilltänkta surveyfrågorna. Genom vår kvantitativa surveyundersökning så kan vi genom olika rangordningsmått dra slutsatser av de svar vi får in (Andersen, 1994).

De två nämnda metoderna kan sedan sammanbindas i en tredje fas vilket enligt Bell (1995) kallas triangulering. Denna del går, enligt samma författare, ut på att sammanbinda olika metoder i analysen för att på så vis undersöka eventuella samband dem emellan. Genom att jämföra vissa delar av intervjuerna med svar från fokusgruppen och surveyundersökningen hoppas vi finna intressanta samband som sedan kan stärka våra slutsatser.

2.2.1 Kvalitativ undersökning

Den kvalitativa undersökningen kommer att i första hand omfatta de intervjuer vi genomför i uppsatsarbetet, djupintervjuer på olika företag, men även arbete med s k fokusgrupper.

2.2.1.1 Fallstudie

För att få inblick i verksamheten gällande mobila säkerhetsfrågor på olika företag så kommer vi att genomföra mindre fallstudier på dessa. ”Fallstudier” är enligt Lundahl & Skärvad (1999) när ett eller ett mindre antal fall, det kan vara ett företag, studeras i detalj. Studie av fall utgör en viktig del av den kvalitativa metodteorin. Vissa forskare anser att fallstudier är synonymt med kvalitativa undersökningar (Lundahl & Skärvad, 1999).

I vår studie vill vi erhålla information från företag om hur deras system är uppbyggda och hur de arbetar med säkerheten kring sina tjänster. Detta kallas, enligt sistnämnda författare, för en beskrivande fallstudie. Genom att illustrera de olika företagens tjänster och säkerhetsaspekter hoppas vi sedan kunna jämföra dessa med varandra, samt med delar av insamlade data från fokusgruppen och surveyundersökningen. Det finns också en fara med att bara genomföra en fallstudie. Lundahl & Skärvad (1999) betonar att enbart en fallstudie kan bli alltför situationsspecifik för att vara intressant för andra aktörer. Vi ämnar dock studera flera fall för att få en mera fullständig uppfattning om hur långt marknaden nått vad gäller säkerhetstänkande kring mobila tjänster. Ovan nämnda författare anser att denna jämförelse av andra fall kan vara nödvändig för att upptäcka det verkligt intressanta i de olika fallen. Studierna som vi avser genomföra är inte processtudier utan ögonblicksstudier (Lundahl & Skärvad, 1999) Detta då vi anser att det räcker med att studera varje företag vid en tidpunkt för att se hur långt de nått med sitt arbete. Det är ej nödvändigt, och finns ej heller tid och möjlighet, att genomföra flera studier på varje företag. Samma författare beskriver även att fallstudiens resultat är en fallbeskrivning som kan användas som underlag vid analys, tolkning och resultat/slutsats.

2.2.1.2 Fokusgrupp

Fokusgruppens roll (se mer om detta i Kap 2.3.3) är att ge oss feedback och information kring vår uppsats. Genom interaktion mellan deltagarna skapas nya idéer, infallsvinklar och information som kommer att leda oss vidare i uppsatsarbetet (Ritchie & Evans, 2003). Vi hoppas även att denna diskussion ska ge oss synpunkter som vi kan använda för att konstruera en surveyundersökning av bättre kvalitet för att på så sätt få ett starkare och mer trovärdigt underlag till analysarbetet.

2.2.2 Kvantitativ undersökning

Då vi inte endast är ute efter kvalitativ data så är vi tvungna att genomföra en kvantitativ undersökning. Utgångspunkten vid arbetet med kvantitativa metoder är enligt Andersen (1994) att det som studeras görs mätbart och att resultaten från dessa presenteras numeriskt. Den kvantitativa undersökningen vi ämnar genomföra är en enkätundersökning där vi vill få fram människors syn på och förtroende för mobila betaltjänster. Det finns enligt Lundahl & Skärvad (1999) olika sorters enkätundersökningar och den vi kommer att använda oss av kallas surveyundersökning (Kap 2.3.4).

Vår undersökning kommer att vara kvantitativ i så måtto, att vi genomför en insamling av data som är kvantifierad, det vill säga presenterad i siffror och sedan i diagram, men vår analys kommer inte att vara statistiskt genomförd utan vara en kvalitativ analys av siffrorna och diagrammen.

2.3 Datainsamling

2.3.1 Litteraturstudie

Vid undersökningar av olika slag är det enligt Andersen (1994) viktigt att känna till och läsa in sig på den litteratur som finns inom ämnesområdet. Syftet med detta är att ta till sig den kunskap som finns inom området för att på sätt kunna framställa en mer precis problemställning. Vi kommer att genomföra en omfattande litteraturstudie inom teman som mobil säkerhet, m-commerce, betalningsmedel, trådlös kommunikation, mobiltelefoni och informationssäkerhet. Detta för att ge oss en introduktion till tidigare nämnda ämnesområden och för att vi på så sätt skall kunna erhålla kunskap, vilken kan vara till nytta vid senare undersökningar.

Vi avser att inleda informationssökningen med nytt material då vårt ämnesval kräver uppdaterad och aktuell information. Andersen (1994) beskriver också vikten av att studera det senaste materialet först för att få bredast möjliga teckning, då dessa kan innehålla värdefulla hänvisningar till äldre litteratur.

Då de olika ämnesområdena inom mobil säkerhet är relativt nya och aktuella områden, är också Internet en värdefull källa. Internetbaserade källor uppdateras relativt ofta vilket ger färsk information till forskaren. Dock finns det skäl till att vara källkritisk till dessa källor då olika webbsidor har olika grad av seriositet. I vårt arbete med informationssökning så är vi väl medvetna om detta och funderar mycket på vilka källor som är trovärdiga att använda.

2.3.2 Fallstudie/Intervjuer

Det finns enligt Lundahl & Skärvad (1999) olika sätt att samla in data vid fallstudier. Det kan ske genom intervjuer, genomgång av skriftligt material, enkäter, studerande av planer,

budgets, protokoll, utredningar och andra handlingar som kan vara relevanta för studien. Den metod som vi främst kommer att använda oss av för insamlande av information vid fallstudierna är intervjuform (Intervjuer se bilaga 1-4).

Den intervjuform vi avser använda oss av är semistandardiserade intervjuer. Det är enligt senast nämnda författare en hybrid mellan standardiserade och icke-standardiserade intervjuformer. Samma författare diskuterar vidare att vid hög grad av standardisering är såväl frågorna som ordningen på dessa bestämda i förväg. Frågorna och dess ordning skall också vara oförändrade genom samtliga intervjuer i undersökningen.

När det gäller icke-standardiserade intervjuformer så är fallet det omvända. Forskaren kan välja både frågeformuleringarna och deras inbördes ordning mer fritt (Lundahl & Skärvad, 1999). Dock är det av stor vikt att frågorna täcker det informationsbehov som ställts upp i förhand. Denna intervjuform är enligt senast nämnda författare mer flexibel och situationsanpassad.

Då vi väljer att använda oss av semistandardiserade intervjuer innebär det att vi bestämmer ett antal frågor i förväg som skall ges till samtliga respondenter. Vi kan då också ställa följdfrågor till respondenterna, vilket innebär att vi kan få ut mer information av intervjuerna som vi eventuellt missat i planeringsstadiet. Frågor som är av mer anpassad art till respektive respondent kan också ställas.

Vi finner det heller inte nödvändigt för respondenten att svara strukturerat som t.ex. genom olika svarsalternativ. För att få ut så mycket information som möjligt ur intervjuerna vill vi att svaren enligt Lundahl & Skärvads (1999) råd skall vara ostrukturerade så att respondenten själv får formulera sina svar.

För att inte missa något av respondenternas svar vid intervjuerna planerar vi att använda oss av inspelningsutrustning när så är möjligt. Vissa intervjuer kommer möjligen att genomföras via telefon varvid inspelning då ej är möjlig. Dessa intervjuer hanteras genom stödord under intervjuerna varefter en sammanfattning skrivs då intervjun är utförd. Intervjuerna kommer att redovisas i form av sammanfattningar i textform (Bilaga 1-4).

2.3.3 Fokusgrupp

En fokusgrupp kan lämpligen bestå av mellan 6-8 deltagare (Richie & Lewis, 2003; Seal, Gobo, Gubrium & Silverman, 2004). Cesam (2005) diskuterar värdet av fokusgrupper för att nå ny kunskap om ett visst fenomen. Genom gruppens olika erfarenheter och tankar uppstår ny kunskap om ett bestämt tema (Cesam, 2005). Denna typ av metod används ofta när forskaren inte är riktigt säker på hur relevant olika teman eller perspektiv är (Seal et al, 2004). Genom gruppens diskussioner får forskaren en bild av de frågor som diskuteras vilket genererar information om deras relevans och betydelse för gemene man. De olika deltagarna får chans att bemöta varandras argument och åsikter fritt, vilket genererar djupare förståelse för det diskuterade ämnet (Richie & Lewis, 2003). Denna förståelse genom diskussion leder enligt samma författare till att fokusgruppsmötet kan resultera i mer genomtänka slutsvar då olika ståndpunkter presenteras och diskuteras.

Många författare (Cesam, 2005; Richie & Lewis, 2003; Seal et al, 2004) belyser också vikten av att mötesledarna är väl insatta i ämnet och kan se till att det som ska diskuteras verkligen lyfts fram under mötet. Cesam (2005) fortsätter också med att det är mötesledarnas uppgift att se till att alla deltagare kommer med i diskussionen och att de olika kunskaper som finns i gruppen lyfts fram.

Fokusgruppens roll i uppsatsarbetet är att diskutera olika frågeställningar vi kommer fram till i det inledande uppsatsarbetet. Genom gruppens interaktion diskuteras lösningar och åsikter kring säkerhet gällande mobiltelefoner kontra Internettjänster, vilket enligt Ritchie & Lewis (2003) kan leda till nya synpunkter och idéer.

Fokusgruppsmötet kommer att ta plats i ett av IHHJ: s (Internationella Handelshögskolan, högskolan i Jönköping) lokaler. Seal et al, (2004) betonar vikten av att mötesplatsen hålls neutral vilket inte alltid helt kan uppfyllas. Högskolan är dock en plats där vi har möjlighet att få en lokal samt den presentationsutrustning som kan vara till hjälp. Det är även en enkel och ren miljö, vilket bidrar till att fokus hålls på mötet (Seal et al, 2004). Samma författare betonar även vikten av att placeringen av deltagarna ordnas så att alla kan se varandra, därför kommer vi att placera deltagarna runt bord sammansatta till en fyrkant.

Mötet kommer att inledas med en kort presentation om oss och ett kort föredrag om ämnesinriktningen vars syfte är att tydliggöra avsikten och förutsättningarna med mötet vilket Cesam (2005) rekommenderar. Detta är av stor vikt då vi tidigare enbart kort förklarat mötets grundidéer via e-mail eller telefon. Efter presentationen får deltagarna kort presentera sig själva, deras bakgrund och erfarenheter för att alla i gruppen ska förstå de olika roller som finns representerade.

Vi kommer innan mötet att förebereda ämnet som vi avser att fokusgruppen ska diskutera med varandra. Dessa berör bland annat åsikter kring mobil användning och dess säkerhet. Något som också kommer att belysas är en diskussion kring frågorna till vår surveyundersökning. Det är enligt Dillman (1997) viktigt att testa surveyundersökningens frågor på några oberoende personer så att exempelvis frågornas innehåll och formulering är av god kvalitet. En genomtänkt och kvalitetsrik surveyundersökning leder till mer användbar information för senare analysarbete och kan därvid generera starkare slutsatser.

Vår roll är som mötesledare och vi anser därför att vi ej ska delta för mycket i diskussionen utan enbart leda in respondenterna på ”rätt spår”. Detta då målet med fokusgruppen är att få andra åsikter och idéer än våra egna gällande vårt ämnesval. Vi har även tidigt funderat på de olika egenskaper/deltagare som vi ville ha med i gruppen. Det är enligt Seal et al (2004) viktigt att ha en vid kunskapsbredd representerad i gruppen för att kunna lyfta upp så mycket information som möjligt till ytan. Vår avsikt är även att gruppen skall vara jämnt fördelad både vad gäller kön och ålder.

Då vi har erfarenhet från ett tidigare genomfört fokusgruppsmöte anser vi oss kunna använda de erfarenheterna vi fick där för att ytterliggare förbättra vårt beteende som mötesledare för fokusgruppsmötet. En svårighet vi upptäckt tidigare är att se till att allas åsikter lyfts fram så att det inte bara är några få som diskuterar ämnet. Detta är något som vi som mötesledare är tvungna att styra upp. En annan stor punkt är att se till att deltagarnas diskussion håller sig till ämnesvalet och inte vandrar iväg för mycket.

2.3.4 Surveyundersökning

En surveyundersökning definieras enligt Jarneving (2005) som en undersökning som inbegriper en enkät och/eller intervjuer och ett stort antal respondenter. Då dess syfte är att införskaffa information om åsikter och attityder (Jarneving, 2005; Lundahl & Skärvad, 1999) anser vi att denna metod passar vårt syfte bra, då vi är ute efter attityder och åsikter kring säkerheten hos betalningstjänster för mobiltelefonen. Vi kommer att genomföra undersökningen genom en webbaserad enkät (Bilaga 6-7) som Lundahl & Skärvad (1999) beskriver som en icke-experimentell frågeundersökning. Grundtanken i denna metod är att alla frågor skall vara standardiserade, vilket innebär att respondenterna får samma frågor att svara

på. Detta skapar enligt samma författare bra förutsättningar för kvantitativ bearbetning vilket i sin tur leder till en kvantitativ analys av svaren. Det finns också olika sorters surveyundersökningar. Då erfarenheter och attityder kring en produkt eller tjänst eftersträvas rekommenderar nyss nämna författare en deskriptiv marknadsundersökning, vilket enligt Jarneving (2005) är den vanligaste surveyundersökningen.

Jarneving (2005) delar med sig av några tankar om hur frågorna i en surveyundersökning bör ställas för att erhålla ett så bra resultat som möjligt:

- Håll ner antalet frågor då det annars finns risk för svarsbortfall
- Frågorna bör vara enkla och lättförståliga
- Eventuella facktermer bör förklaras
- Undvik ledande frågor
- Dela upp eventuella sammansatta frågor
- Tänk på respondenternas integritet

Ovanstående punkter kommer vi att beakta vid framställningen av surveyundersökningen.

För att få så många svaranden som möjligt till vår surveyundersökning kommer vi att sprida ut adressen till den på olika forum på Internet. Genom att använda olika forum så ser vi också till att få en stor bredd på respondenterna vad gäller kön, ålder och intresse. Vi kommer slumpmässigt att ta fram de forum vi tänker använda oss av genom att söka på www.google.se efter termen ”forum”. Sedan lägger vi in adressen till vår surveyundersökning på de forum som först dyker upp i resultatet av sökningen tills vi uppnår ett tillfredsställande antal inlägg. De forum vi kommer att använda oss av framgår av Bilaga 10.

Tillvägagångssättet vad gäller surveyundersökningen rent tekniskt planeras att gå till på följande vis. Vi kommer att lägga upp frågorna på en webbsida (Se Bilaga 6) där respondenterna får gå in och ange sina svar genom att klicka i svarsalternativ. Dessa svar planeras sparas automatiskt i en databas. Vi ställer sedan olika SQL-frågor mot databasen för att få ut den informationen, som respondenterna har angett, i siffror. Denna information kommer vi sedan att sammanställa med hjälp av Excel där vi avser göra grafiska exemplifieringar av den insamlade datan vilket ger utrymme för tolkningar från vår sida i analyskapitlet.

2.3.4.1 Surveyfrågor – forskningsfrågor

Under följande kapitel redovisar vi våra tankegångar/avsikter med de frågor vi tagit fram till vår surveyundersökning. En diskussion förs för att påvisa varför de olika frågorna ställs och hur de är relaterade till våra forskningsfrågor.

Då vår uppsats är uppdelad i två delar genom de två olika forskningsfrågor vi ställt (Kapitel 1.3), krävs det för läsaren en diskussion hur surveyfrågorna är kopplade till dessa. Då enkätens syfte bl.a. är att generera kunskap om allmänhetens förtroende för mobil säkerhet är frågorna vi ställt kopplade till forskningsfråga 1 (Har användarna förtroende för säkerheten hos mobila betalningstjänster?).

Fråga 1 & 2 - Kön & Ålder

Kön och ålder är av stort intresse då olika människor har olika attityder och värderingar gentemot produkter och tjänster. För att få en uppfattning om vilka det är som svarat på

enkäten har vi valt att ta med dessa faktorer. Detta då olika människor har olika förutsättningar vilket gör att de kan svara olika på samma eller liknande frågor.

Fråga 3 - Har du en mobiltelefon med åtkomst till Internet?

Denna fråga relaterar till att få en uppfattning om hur många det är som verkligen har WAP i sina mobiltelefoner. De flesta moderna mobiltelefoner har i nuläget WAP så frågan kan också ge information om hur moderna mobiltelefoner människor har idag. Vissa människor kanske inte vet om att de har WAP dock och i så fall kan deras svar bli felaktigt.

Fråga 4 - Använder du denna möjlighet till åtkomst av Internet?

För att få en uppfattning om hur många det är som använder WAP idag så motiveras valet av denna fråga till undersökningen. Frågan svarar på hur stort intresse det finns av mobiltelefonägarna att använda sin WAP-funktion. Det ger också en inblick genom vidare ställda frågor (Fråga 12) hur många det är som använder WAP även fast de inte anser detta som säkert vilket kan vara av intresse.

Fråga 5 - Om ja vad använder du?

Det är av intresse för oss att få en uppfattning om vilka mobila tjänster som används. Detta för att få en uppfattning om hur många det är som verkligen använder betaltjänster och andra tjänster. Det kan dels ge en bild både av hur stort förtroende är hos säkerheten (När denna fråga ställs mot fråga 9 och fråga 12) hos mobila tjänster och dels vad som är intressant för användarna.

Fråga 6 - Hur ofta använder du dessa tjänster?

Denna frågeställning motiveras av att se hur ofta människor som har WAP använder denna funktion. Detta kan ge svar på hur ofta WAP används i människors normala liv och popularitet hos denna sorts tjänst.

Fråga 7 - Vilka tjänster skulle du vilja använda?

Frågan besvarar vår undran om vilka tjänster allmänheten vill ha genom sin mobiltelefon. Det kan vara så att människor inte vet om vilka tjänster som existerar i dagsläget men det kan också vara så att vissa tjänster helt enkelt anses mer relevanta än andra.

Fråga 8 - Skulle du kunna tänka dig att betala över Internet med mobiltelefonen?

Frågeställningen relaterar till hur många det är som skulle kunna tänka sig att använda mobiltelefonen för att betala över Internet. Frågan ger dock inte bara svar gällande säkerhetsaspekter utan kan också innehålla frågor som gäller t.ex. smidighet att betala med mobiltelefonen.

Fråga 9 - Skulle du kunna tänka dig att sköta dina finansiella affärer via mobiltelefonen? (Såsom bankärenden, aktiehandel, köp av varor m.fl.)

Vi är intresserade att veta hur många mobilanvändare som kan tänka sig att använda mobiltelefonen som ett hjälpmedel för att hantera sina finansiella affärer. Frågan kan också ställas emot fråga 12 (Känner du förtroende för säkerheten vid användandet av en finansiell tjänst i din mobiltelefon) för att få en uppfattning om hur många som skulle kunna tänka sig att sköta sina finansiella affärer via mobiltelefonen men samtidigt inte har förtroende för säkerheten.

Fråga 10 - Anser du att det är lika säkert att surfa o mobilen som via datorn i hemmet?

För att få ett svar från allmänheten gällande deras tankar om skillnaden ur säkerhetssynpunkt mellan datorn i hemmet och mobilen ställde vi denna fråga. Detta kan ge svar om hur stort förtroende människor har för mobilen kontra datorn.

Fråga 11 - Känner du förtroende för säkerheten vid användandet av en finansiell tjänst via datorn i hemmet? (Såsom överföringar av pengar, betala räkningar o andra banktjänster)

Frågans besvarar om allmänheten har förtroende för säkerheten hos datorn i hemmet när det gäller att sköta sina finansiella affärer via den. Tror användarna att datorn är tillräckligt säker för tjänster såsom överföring av pengar, betala räkningar osv.

Fråga 12 - Känner du förtroende för säkerheten vid användandet av en finansiell tjänst i din mobiltelefon? (Såsom överföringar av pengar, betala räkningar osv.)

Frågans syfte är att ge ett svar på om allmänheten har förtroende för säkerheten hos mobiltelefoner när det gäller att sköta sina finansiella affärer via den. Tror allmänheten att det är säkert att använda sin mobiltelefon för överföring av pengar, betala räkningar osv.

2.3.5 Pilottest

Utifrån Andersens (1994) råd om att en provundersökning bör genomföras innan den slutgiltiga undersökningen genomförs, avser vi att genomföra ett pilottest på de frågor som vi vill ha med i surveyundersökningen. Vi vill få svar på om de slutgiltiga respondenterna uppfattar frågorna på rätt sätt och att urvalet av frågor är lämpligt. Syftet med ett pilottest är enligt Rubin (1994) att förstå misstag eller fel på det som ska testas. Ett pilottest kontrollerar utformningen på undersökningen innan slutresultatet betyder något. Det kan enligt samma författare vara svårt att få fram en entydig och ojävig undersökning, speciellt när forskaren har stor kunskap inom ämnet, vilket ökar betydelsen av ett pilottest. Då vi är inlästa på området kan vi eventuellt använda oss av komplicerad terminologi som respondenterna har svårt att förstå. Ett test av denna art kan enligt Dillman (1997) svara på om:

- Frågekategorierna uppfattas lika intressanta att besvara
- Det finns motsättningar att besvara en viss fråga
- Eventuella öppna frågor ger relevanta svar
- Vilken responsgrad undersökningen troligtvis kommer att få
- Responsgraden är tillräcklig för att behandla informationen på ett ändamålsenligt sätt

Rubin (1994) diskuterar också ytterligare punkter som ett pilottest kan resultera i:

- Idéer för andra frågor
- Identifiering av överflödiga frågor
- En bättre uppskattning om hur lång tid det tar att genomföra enkäten

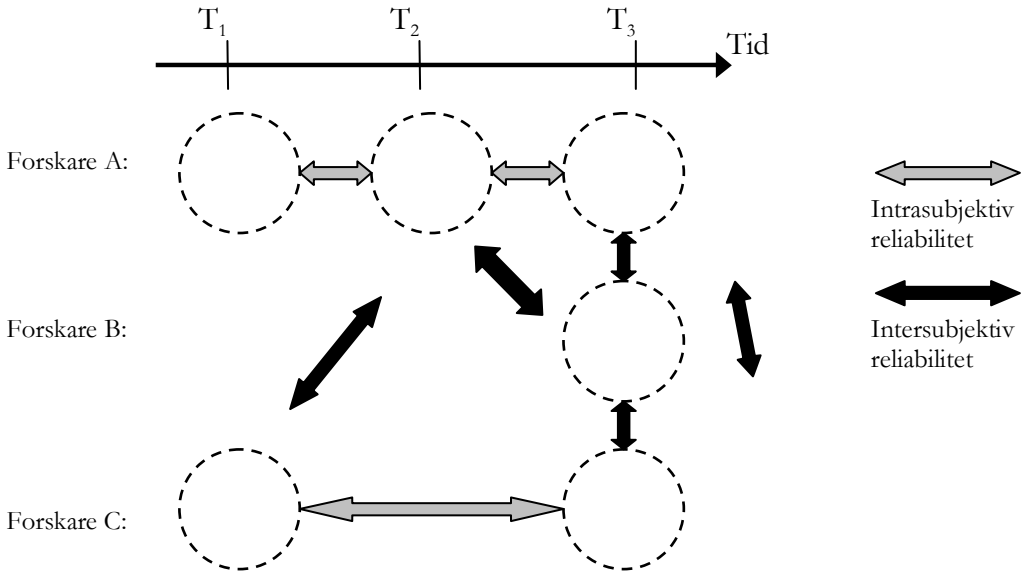
Genom pilottestet avser vi få svar på de ovan uppställda punkter som Dillman (1997) och Rubin (1994) diskuterar.

Vår avsikt är att genomföra pilottesten på 20 slumpvis utvalda personer i vår omgivning. Vårt mål är att åldersfördelningen är mellan 15-60 år och består till hälften av kvinnor och hälften män, detta för att få åsikter från ett så representativt urval som möjligt inför den slutgiltiga surveyundersökningen. Dessa respondenter får då möjlighet att kommentera eventuella oklarheter och med hjälp av deras utvärdering kan vi eventuellt förbättra våra frågor. Detta leder förhoppningsvis till att vi kan minska risken för mätfel som beror på felkonstruerade frågor vilket i sin tur kan leda till högre validitet.

2.4 Metodvärdering

2.4.1 Reliabilitet

God reliabilitet, eller pålitlighet, är en förutsättning för att i ett forskningsresultat kunna påvisa att de faktiska förhållanden som iakttagits är pålitliga (Andersen, 1994). Författaren skiljer på två olika sorters av reliabilitet vilka är intersubjektiv samt intrasubjektiv reliabilitet. Med detta menar han att intersubjektiv reliabilitet är graden av överensstämmelse mellan olika mätningar av samma fenomen för olika forskare, medan den intrasubjektiva reliabiliteten är graden av överensstämmelse mellan samma forskares olika mätningar av samma fenomen. Detta beskrivs i följande figur



Källa: Andersen, 1994

Figur 2 – Reliabilitet

Detta leder till att vi för att nå en hög reliabilitet i vår undersökning eftersträvar att nå intersubjektiv reliabilitet genom att söka fakta i andras undersökningar och jämföra med den vi själva utför. Vi anser att vi ej kan uppnå intrasubjektiv reliabilitet då det inom ramen för uppsatsarbetet ej finns möjlighet att utföra mer än en undersökning.

Begreppet reliabilitet kan också beskrivas som frånvaro av slumpmässiga mätfel (Lundahl och Skärvad, 1999). När en undersökning genomförs är det därför mycket viktigt att i re-

sultatet erhålla en hög reliabilitet. Om inte hög reliabilitet föreligger kan det medföra att resultatet inte överensstämmer med verkligheten.

Slumpmässiga mätfel kan utgöras av att i exempelvis en intervju konfrontera respondenterna i skilda miljöer (Lundahl och Skärvad, 1999). De skilda miljöerna kan enligt samma författare kraftigt påverka respondenternas svar, därför är det av hög vikt att i en undersökning utföra konfrontationerna med respondenterna i en så likartad miljö som är möjligt. Det finns alltid enligt ovan nämnda författare en risk att slumpmässiga mätfel uppkommer när en undersökning genomförs, för att undvika detta är det därför viktigt att införa standardiseringsförfaranden för att tillförsäkra en hög reliabilitet.

För att undvika slumpmässiga mätfel i vår undersökning genomför vi denna i ett standardiserat utförande genom att samma frågor ställs till alla respondenter. Vi väljer dessutom att konfrontera respondenterna i en så likartad miljö som möjligt vid utfrågningstillfällena. Även sättet frågorna ställs till respondenterna beaktas så vi inte själva ställer dessa med olika tillvägagångssätt.

2.4.2 Validitet

Validitet kan beskrivas som giltighet (Andersen, 1994). En undersökning som genomförs med hög validitet mäter det som den var avsett att mätas (Ritchie & Lewis, 2003). Om en undersökning har frågor som tolkas eller är skrivna på ett sådant sätt att det inte ger svar på vad undersökningen efterfrågar föreligger hög risk att validiteten blir låg. Detta då respondenterna i det fallet antingen kan misstolka frågan och inte förstå den eller tro sig förstå frågan, men svarar egentligen på fel sak vilket ger ett missvisande resultat (Ritchie & Lewis, 2003).

I detta uppsatsfall föreligger validitetsbegrepp i de tre undersökningsfaserna intervjuer, fokusgrupp samt underökning. I dessa tre metoder, vilka kommer att ligga till grund för vår studie, är det av stor prioritet att vi ser till att validiteten bibehålls hög för att undvika ett missvisande resultat. Detta görs genom att utforma de frågor som kommer att ställas i såväl intervjuerna, fokusgruppmötet samt undersökningen så att de klart och tydligt genererar svar till de frågeställningar vi satt upp. Vad vi även anser viktigt är att i alla sammanhang förklara frågorna för alla respondenter och få dem att tolka frågorna likadant. Detta menar vi bidrar till att minimera risken att respondenterna ger svar på frågorna tolkat från ett synsätt vi inte avsett i frågeställningen. Att ge goda förklaringar till frågor kan även föra med sig att respondenterna verkligen svarar på våra frågor. Förstår inte respondenterna frågorna ordentligt eller känner sig tveksamma i vad som menas kan det föreligga risk att frågorna inte besvaras sanningsenligt. Det finns då även en fara att respondenterna inte lägger ner tillräckligt med kraft och energi att besvara frågan om de inte fullt ut förstått den eller misstolkar den.

De intervjuer som utförs under ramen för uppsatsarbetet kommer att utföras verbalt och på grund av detta undersökningsgenomförande kommer svar i talspråk att erhållas. När sedan intervjuerna omsätts till text omvandlas de svar respondenterna avgett till skriven löptext. Detta förfarande diskuteras av Patel & Davidson (2003), och de nämner att det är viktigt i ett förfarande av denna art att inte innebörden av respondentens svar förändras. Författarna fortsätter med att förklara att eftersom talspråk kan bestå både av grammatiska fel samt talfel, vilka förfinas vid överföring till skriven löptext, finnes det en risk att innebörden i svaren förändras. Denna risk kommer vi ha i åtanke då vi efter utförda intervjuer överför talspråket till skriven text för att i denna förhindra validitetsfel av den art Patel & Davidson (2003) diskuterar.

Både reliabilitetsbegreppet samt validitet är enligt Lundahl och Skärvad (1999) beroende av varandra eftersom om det föreligger en låg reliabilitet inte har någon betydelse om validiteten är hög.

2.4.3 Generalisering

I vår studie genomförs förfrågningar riktade mot allmänheten för att få svar på vissa frågor. Det är av naturliga orsaker inte möjligt att undersöka hela populationen, och därför avser vi att göra ett urval ur populationen. När ett urval görs skall detta på ett så bra sätt som möjligt representera hela populationens åsikter och så att en generalisering kan göras för hela populationen (Patel & Davidson, 2003). För att få en så tillförlitlig bild som möjligt av hela populationens åsikter kommer vi att eftersträva så god representativitet som möjligt i vårt fokusgruppsval samt i den övriga undersökningen (se tidigare diskussion under 2.3.3). Då det i vår intervjufas inte finns möjlighet att intervjua tillräckligt med personer för att täcka in hela branschens är där möjligheterna till generalisering begränsade, och inriktningen är istället efter att få en god helhetsuppfattning för fortsatta arbetet under fokusgruppsfasen samt undersökningsfasen.

3 Teoretiskt ramverk

Det teoretiska ramverket har följande struktur: Först förklarar vi ingående vad mobil säkerhet innebär, vilket roller i m-commerce är en utveckling av. Efter det presenteras OSI-modellen, som vi anser grundläggande för förståelse av trådlös kommunikation och därför fått ett eget avsnitt. Sedan följer avsnitt om sårbarheten i WAP nätverk, vilka säkerhetsprotokoll som används och hot om virus. Kapitlet avslutas med en presentation av WPKI konceptet.

3.1 Mobil säkerhet

Då säkerhet är ett väldigt stort område krävs det en definition av vad vi menar med säkerhet inom just vårt område. Hu, Lee & Kou (2005) diskuterar m-commerce säkerhet som de tekniska och ledningsstyrda procedurerna vilka appliceras på m-commerce för att tillhandahålla följande funktioner för m-commerce information och system:

- *Konfidentiellitet* – Informationen och systemen får inte avslöjas för obehöriga personer, processer eller anordningar. Vid transaktioner antas det att bara avsändaren och mottagaren kan förstå meddelandet i klartext. Genom konfidentialitet försäkras det att andra obehöriga individer inte kan ta del av meddelandets innebörd. Detta sker oftast med hjälp av kryptering.

- *Verifiering* – Försäkrar inblandade parter i en transaktion att de inte är bedragare och kan anses som pålitliga. Detta sker genom att parterna (oftast avsändare och mottagare) måste bekräfta varandras identiteter. Detta uppnås oftast genom användning av nätverksbaserade auktoriseringsprotokoll.

- *Integritet* – Försäkrar att informationen och systemen inte har förändrats av någon utomstående. Inget meddelande skall kunna förändras oavsiktligt eller avsiktligt utan att detta upptäcks av mottagarsidan i ett m-commerce system. Med denna säkerhetsfunktion kan inte en obehörig person lura mottagaren genom att förändra meddelandet. Genom att lägga till elektroniska signaturer i meddelandet uppnås integritet.

- *Auktorisering* – Procedurer måste finnas för att bekräfta att en person är behörig att genomföra efterfrågad transaktion

- *Tillgänglighet* – En auktoriserad person måste ha förfogande till uppdaterad och pålitlig tillgång till information för att kunna genomföra m-commerce transaktioner. Detta försäkrar också att användaren har säker tillgång till informationen eller systemet. Systemet skall vara uppbyggt på så sätt att det minimerar effekterna av DoS-attacker vilket kan medföra att m-commerce tjänsterna blir ostabila eller oåtkomliga under långa perioder. Det bästa skyddet mot detta är korrekt konfigurerade brandväggar.

- *Ej förnekbar* – Försäkrar att en användare inte kan förneka inblandning i en transaktion. Användaren tillhandahålls med bevis om transaktionen och mottagaren blir försäkrad om användarens identitet. Varken avsändaren eller mottagaren skall kunna förneka att transaktionen ägt rum. Avsändaren kan med andra ord bevisa att mottagaren tagit emot meddelandet och vice versa. Detta sker oftast genom användning av digitala signaturer.

Lösningar på ovan nämnda säkerhetsfrågor måste vara uppfyllda för att transaktioner mellan företag och individer skall kunna ske utan att brister inom säkerheten skall förekomma.

Hu et al (2005) beskriver att mobil säkerhet är en kritisk del av m-commerce. Utan säkert utbyte av information och säkra elektroniska monetära transaktioner över mobila nätverk skulle varken företagen som tillhandahåller tjänster av detta slag eller deras kunder lita på m-commerce system. Författarna fortsätter med att säga att ur ett rent tekniskt perspektiv så är m-commerce över trådlösa nätverk mindre säkert jämfört med e-commerce över fasta nätverk. Skälen till detta är enligt samma författare:

- Reliabilitet och integritet – Störningar och döda signalzoner gör att trådlösa kanaler oftare går ner under vissa perioder.
- Konfidentiellitet– Sändningen av radiosignaler genom luften gör det lättare att avlyssna dessa. Kommunikationen kan bli upptagen och avlyssnad utan större problem om inte någon säkerhetsmekanism används som t.ex. kryptering.
- Identifiering och autentisering – Mobiliteten hos trådlösa enheter introducerar en ytterligare komplexitet vad gäller identifiering och autentisering av mobila terminaler.
- Kapacitet – Trådlösa enheter har ofta mindre databehandlingskapacitet, minnesstorlek, bandbredd och batterikraft. Allt detta leder till att det kan vara svårt att använda hög säkerhetskryptering som 256-bit kryptering.

3.2 Roller i m-commerce

För att förstå säkerhetskraven inom m-commerce så inleder vi här en diskussion gällande vilka roller som kan existera inom m-commerce. Hu et al (2005) beskriver följande basroller:

1. Användare - Det är personen som tar initiativet för transaktionen. Inom m-commerce är det vanligtvis en person som är på resande fot och använder en mobil enhet, t.ex. en pda eller mobiltelefon.
2. Nätoperatör - Detta är en organisation eller individ som tillhandahåller den tjänst som användaren är intresserad av. Tjänsten innebär ofta att en kostnad som betalas av användaren men tjänsten kan också vara gratis. Olika serviceleverantörer kan vara restauranger, banker och telefonoperatörer.
3. Nätägare - Detta innebär den organisation som tillhandahåller tillgången till nätverket för användaren.
4. Andra parter - Det finns andra individer eller organisationer som deltar i en transaktion. Detta kan t.ex. vid ett telefonsamtal vara den användaren konverserar med.

Det finns också andra roller när det gäller m-commerce som har rollen att tillhandahålla referenser om användaren. Dessa är enligt ovan nämnda författare:

1. Kreditreferens – Den här rollen har ofta en kreditkortsorganisation. Denna organisation kommer in när användaren väljer att betala en tjänst med sitt kreditkort.
2. Autentiseringsmyndighet – Det här kan vara en organisation som bekräftar att användaren är den han/hon utger sig för att vara.

Det finns också olika förhållanden mellan de olika rollerna vilka kommer att diskuteras under följande rubriker (Hu et al, 2005):

3.2.1 Autentisering

Program som kräver persondata kräver autentisering av användaren från en nätoperatör. Detta gäller oftast i det omvända fallet också. Användaren vill säkerligen få bekräftelse på att nätoperatören är en organisation som går att lita på.

3.2.2 Åtkomsträttigheter

Många m-commerce tjänster kan i princip tillhandahållas till anonyma användare, med andra ord behöver inte leverantören av tjänsten alltid autentisera användaren. Detta kan vara fallet när åtkomsträttigheterna redan har behandlats vid en tidigare transaktion.

3.2.3 Betalningskreditiv

Betalningar är en viktig del inom m-commerce. Olika betalningsmetoder kan klassificeras in i två klasser; kontantbaserade och kortbaserade betalningar. Den senare metoden involverar en kreditorganisation som säkerställer för betalningsmottagaren att användarens konto innehåller den summa som betalningen kräver.

3.2.4 Privat kommunikation

Kommunikationen som sker mellan användaren och nätoperatören, och andra möjliga inblandade organisationer eller individer, ska vara privata. Informationen skall med andra ord inte läcka ut till andra obehöriga individer eller organisationer. Ibland ska även bara viss information vara känd för vissa inblandade parter. Detta gäller t.ex. vid kreditkortsbetalningar då affären skall se detaljer om köpta produkter medan kreditföretaget inte skall kunna ta del av denna information.

3.2.5 Meddelandeintegritet

Meddelandeintegritet ser till att meddelanden som utväxlas mellan olika parter vid en transaktion inte förändras genom fel eller av inkräktare.

3.2.6 Verifierade signaturer

Vissa meddelanden eller dokument måste signeras vid viktiga transaktioner. Detta involverar ofta en tredje part som bekräftar att meddelandet eller dokumentet har signerats av rätt person.

3.2.7 Anonymitet

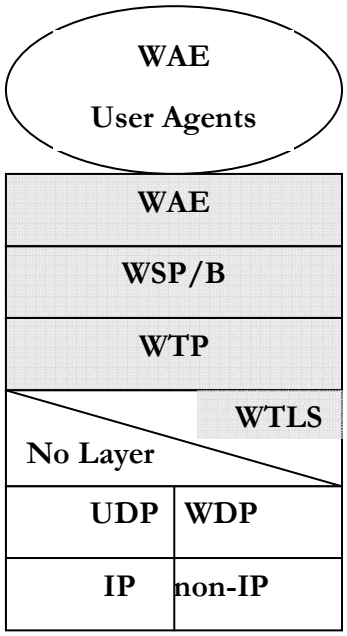
Som tidigare nämnts finns det vissa tjänster som kan tillhandahållas till anonyma användare. I vissa fall kan anonymitet vara att föredra. I vissa fall vill inte individen att någon annan person får reda på vad han/hon köpt. I andra situationer vill inte användaren bli identifierad. För att kunna använda m-commerce program och uppfylla dessa behov så bör alltså det finns ett sätt att behålla sin anonymitet även fast åtkomsträttigheter och betalningskreditiv är uppfyllda.

3.3 WAP

WAP, vars akronym utläses Wireless Application Protocol, är ett protokoll som omvandlar vanliga sidor på Internet så att de kan läsas av mobiltelefoner med WAP-funktion (ESR, 2005). Telenormobile (2005) beskriver WAP som en standard för optimering av dataöverföring mellan trådlösa enheter. Då mobiltelefoner enligt ESR (2005) i dagsläget ej kan ta emot så stora datamängder som genom en fast Internetuppkoppling har WAP fyllt denna funktion. Samma källa fortsätter med att det med en WAP-telefon inte går att gå in på vanliga Internetsidor som kodas i HTML (Hyper Text Markup Language) utan dessa sidor måste kodas om till WAP-språket WML (Wireless Markup Language) vilket är en förenklad version av HTML.

3.3.1 OSI-modellen för trådlös kommunikation

Huvudkonstruktionen av arkitekturen runt WAP kan förklaras genom följande OSI-modell (Wapforum, 2002).



Källa: Wapforum, 2002

Figur 3 – OSI modell WAP

Ordningen av de oberoende nivåerna som också är hierarkiska, har fördelen genom att systemet är väldigt flexibelt. På grund av de olika nivåerna eller stackar så kallas detta en WAP-stack, som är indelad i 5 nivåer.

- Programnivå – Wireless Application Environment (WAE)
- Sessionsnivå – Wireless Session Protocol (WSP)
- Transaktionsnivå – Wireless Transaction Protocol (WTP)
- Säkerhetsnivå – Wireless Transport Security (WTLS)
- Transportnivå – Wireless Datagram Protocol (WDP)

Varje stack överlappar med underliggande stack. Den här arkitekturen med olika stackar gör det möjligt för programtillverkare att utveckla program för enskilda stackar. WAP-stacken är en entitet av protokoll som täcker trådlös överföring av data. Det här inkluderar stackar för layout utöver de stackar som ansvarar för dataöverföring. Den högsta stacken är den som behandlar layout medan en stack på lägre nivå behandlar överföring och säkerhet genom WTLS. Alla stackar under WTLS kallas nätverksstackar. Genom ovan beskrivna hierarki så kan innehållet i nätverksstackarna ändras utan att det berör stackar på högre nivå. Nedan följer en beskrivning av varje stack:

3.3.2 Programnivå (WAE och WTA)

WAE (Wireless Application Environment) och WTA (Wireless Telephony Application) befinner sig på högsta nivån i WAP-arkitekturen. De här två är huvudgränssnitten mot klientanordningen (mobiltelefonen), vilka ger och kontrollerar beskrivningsspråket, scriptspråket från alla applikationer och telefonens specifikationer. WAE och WTA har bara några enkla funktioner på klienten som t.ex. underhållet av en historialista.

3.3.3 Sessionivå (WSP)

WSP (Wireless Session Protocol) innehåller alla specifikationer för en session. Det är gränssnittet mellan programnivån och transportnivån och levererar alla funktioner som är nödvändiga för trådlösa kopplingar. En session består främst av 3 faser: sessionens start, överföring av information fram och tillbaka, och slutet av sessionen. En session kan bli avbruten och starta igen från den punkt där sessionen blev avbruten.

3.3.4 Transaktionsnivå (WTP)

Specifikationerna för transaktionsnivån finns i WTP (Wireless Transaction Protocol). WTP är en del av standardprogrammet från TCP/IP och ser till att det förenklande protokollet är kompatibelt med mobila terminaler. WTP försöker optimera användarens utbyte mot systemet genom att informationen kan mottas när den behövs.

3.3.5 Säkerhetsnivå (WTLS)

Säkerhetsnivån med WTLS (Wireless Transport Layer Security) är en valfri stack som består av säkerhetsfunktioner. En säker överföring är kritisk, och idag också standard, för vissa funktioner som t.ex. m-commerce eller banktjänster via WAP. WTLS innehåller också skydd mot integritet (se kap 3.1), autentisering (se kap 3.2.1) och säkerhet mot gateway.

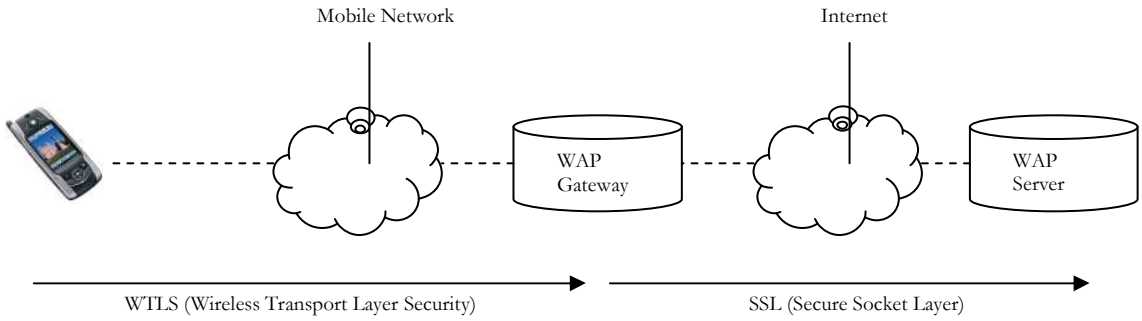
3.3.6 Transportnivå (WDP)

WDP (Wireless Datagram Protocol) representerar transport eller överföringsnivån och är också ett gemensamt gränssnitt för de övre stackarna i OSI-modellen som medför att de kan fungera oberoende av nätverket som används av avsändaren och mottagaren. Med hjälp av WDP kan transportnivån anpassas efter en nätverksoperatörs specifikationer. Det är ett protokoll för att leverera data över trådlösa nätverk.

3.4 WAP-nätverkets sårbarhet

Problemet med WAP-nätverket är enligt Dornan (2001) att det inte täcker hela transportvägen. SSL-tekniken (se kap 3.5) på Internet krypterar data hela vägen från användarens

webbläsare till webbservern. A5-tekniken (Se Kap 3.8) täcker endast den luftburna biten vilket är det samma som WAP gör. Att A5 och WAP endast täcker den luftburna delen i transportvägen lämnar en svag punkt i systemet. Data krypteras säkert med SSL genom det fasta nätet och sedan med samma säkerhetsklass trådlöst genom WTLS men gatewayen däremellan utgör en svag punkt. Innan en lösning tagits fram som krypterar sändningen från början till slut utan någon omvandling emellan är enda sättet enligt tidigare nämnd författare att helt säkerställa en sändning att den som förestår tjänsten själv äger gatewayen.



Figur 4 – WAP modell

Dornan (2001) skriver att banker börjat med att själva äga gatewayen där den mobila sändningen går över till fast nät (WTLS går till SSL). Kunden ringer då upp bankens egen gateway där han eller hon sedan kan använda banktjänster via Internet.

3.5 SSL

SSL står för Secure Socket Layer och är en standardiserad säkerhetsteknik för att skapa krypterade förbindelser mellan en webbserver och en webbläsare (Windowsecurity, 2005). Detta säkerställer enligt nyss nämnda källa att data som skickas t.ex. mellan en webbutik och en privatperson över Internet förblir privat och säker. Tekniken används oftast som skydd för onlinetransaktioner mellan kunder och butik på Internet (Windowsecurity, 2005). I en webbläsare kan en individ se om uppkoppling mot butiken är SSL-säkrad genom att en hänglåsikon visas och att http (Hypertext Transfer Protocol) byts ut mot https (Hypertext Transfer Protocol Secure).

SSL härstammar från mitten av 1990-talet och utvecklades av Netscape (Hardjono, 2005). Författaren förklarar att syftet med SSL är att säkra kommunikationen (http-trafiken) mellan en browser och en webbserver. Idag används enligt samma författare SSL inom tre områden gällande säkerhet mellan en klient och server:

- Autentisering – SSL använder ett system med publika nycklar (t.ex. RSA-algoritm) för ömsesidig autentisering med hjälp av digitala certifikat. Idag kräver de flesta SSL sessioner som är baserade på RSA att enbart webbservern är certifierad medan klienten inte kräver detta. Detta innebär att bara envägs-autentisering är tillhandahållen.

- Dataintegritet – SSL har kontroll över att data inte förändras olovligt i överföringsprocessen.

- Dataskydd – SSL tillhandahåller funktioner för nyckelutbyte mellan klienten och servern, där den resulterande nyckeln används för att kryptera http-trafiken mellan nämnda parter.

3.6 TLS

TLS (Transport Layer Security) är uppföljaren till SSL och har också samma uppgift som SSL (SearchSecurity, 2005).

3.7 WTLS

WTLS (Wireless Transport Layer Security) är baserat på SSL/TLS (Mikal, 2005) och har ungefär samma mål som SSL/TLS. Dess syfte är alltså att tillhandahålla säkerhet och skydda inblandade parter när det gäller transaktioner mellan klient och server i ett nätverk. Författaren fortsätter förklara att medan SSL/TLS tillhandahåller säkerhet över Internet så är WLTS fokuserat på trådlösa applikationer via WAP. Behovet av WTLS, utöver SSL/TLS, finns på grund av de restriktioner som existerar i trådlösa miljöer. Mer specifikt så erbjuder inte SSL/TLS nödvändig support för WAP-telefoner då de har begränsad minneskapacitet och heller inte så stor bandbredd som existerar via Internet (Mikal, 2005).

Ovan nämnda författare beskriver att en WAP-klient (oftast en mobiltelefon) kommunicerar direkt med en gateway som tar emot anropet och översätter det till HTTP som sedan kan kommunicera med lämplig server. I ett säkert WAP-system så krypterar WTLS kommunikationen mellan WAP-klient och gateway. Sedan så dekrypteras WTLS i gateway som sedan krypterar igen med hjälp av SSL för att kunna ansluta till servern. Författaren fortsätter med att denna anslutning via SSL är liknande det som finns genom traditionella säkra Internetanslutningar.

Det finns enligt Mikal (2005) ett par faror med ovan nämna process. Det första är att WTLS tillåter svaga krypteringsalgoritmer. Det finns även vissa WAP-klienter där användarna kan helt slå av WTLS-kryptering. Tillgängligheten av sådana val begränsar kraftigt säkerheten hos WAP. Obehöriga kan också komma åt den WAP-gateway som används. Då denna dekrypterar data mellan WAP-klienten och servern så kan privat data bli upptagen av obehöriga personer. För att förhindra detta bör brandväggar och även fysiska skydd användas.

Dock finns det en ny metod som eliminerar behovet av dekryptering/kryptering vid WAP-gateway (Mikal, 2005). En WAP-klients anrop omdirigeras med hjälp av ett XML-dokument. Detta dokument tillhandahåller klienten med instruktioner om hur en direkt, säker förbindelse med en sekundär gateway med direktåtkomst till servern uppnås.

3.8 Kryptering

För att stärka säkerheten i mobila sändningar används kryptering. Data kan krypteras på flera olika sätt men i huvudsak är det två algoritmer som används för säker data överföring. Dessa delas in i två kategorier vilka är symmetrisk och asymmetrisk kryptering som båda använder en matematisk operation genom ett hemligt nummer som också kallas nyckel (Dornan, 2001). Förutnämnda författare förklarar även att GSM-nätet krypterar all sina data mellan telefonen och basstationen med en krypteringskod kallad A5. Vidare pratar författaren om svårigheten när signaler sänds ut i luften då vem som helst kan ta emot dem. Detta gör att den symmetriska algoritmen inte är lämplig att använda eftersom den kräver att båda de mottagande parterna har samma nyckel. Nyckeln skulle då inte kunna sändas ut

i signalnätet eftersom vem som helst skulle kunna snappa upp den och sedan dekryptera det symmetriskt kodade meddelandet.

Av den orsaken förklarar ovan nämnda författare vidare att den asymmetriska tekniken därför används i A5-systemet. Detta eftersom den använder två separata nycklar, en för kryptering och en annan dekryptering. I den asymmetriska kodningstekniken kan därför krypteringsnyckeln spridas fritt i nätet och vem som helst kan ta emot den medan dekrypteringsnyckel innehas exklusivt av mottagaren.

Nackdelen med att använda den asymmetriska algoritmen i GSM förklarar senast nämnda författare är att den kräver mycket processorkraft vilket gör att ett meddelande som sänds i en mobiltelefon inte kan krypteras i sin helhet. Istället krypterar A5 systemet meddelandet först med en symetrisk algoritm där nyckeln slumpas fram i nätverket och därefter sänds meddelandet genom en asymmetrisk nyckel till handenheten. Detta gör att en hög säkerhet kan hållas samtidigt som den inte kräver för mycket processor kraft vilket annars skulle göra sändningarna mycket långsamma.

3.9 Virus

Virus är ständigt ett hot mot allt som använder någon slags data plattform (Dornan, 2001). Antivirusföretag varnade tidigt för att även mobiler och PDA: er kan utsättas för virus enligt förutnämnda författare vilket gav sig gällande år 2000 då viruset Tomofonica drabbade ett spanskt mobilföretag. Att sedan virus skulle drabba en enskild telefon sågs som mindre sannolikt beroende på deras begränsade funktionalitet. Men med de nya trådlösa terminalerna som blir mer och mer avancerade ökade också känsligheten för virus och 2004 påträffades det första mobila viruset enligt F-secure (2005). Detta säger senast nämnda företag har gjort att dörrarna har öppnats på vid gavel för alla virusmakare. Meddelandetjänster, e-post och Internetuppkopplingar, bluetooth samt även flyttbar lagringsmedia representerar distributionskanaler för mobila virus. Än ser inte hotet från virus för mobiler ut att orsaka några större problem säger Atea security (2005) men de ser ett stort potentiellt hot i framtiden. Det sistnämnda företaget spekulerar i att virus för mobiltelefoner kan bli ett lika stort problem som e-postvirus därför ser de att den bästa lösningen för att slippa problem är att fler redan nu börjar använda antivirusprogram för mobiltelefoner.

3.10 WPKI – WAP Public Key Infrastructure

När den första generationen av WAP släpptes blev inte banktjänster någon större succé bland användarna. Detta berodde enligt Arvidsson (2006) på flera olika orsaker:

- Mobiltelefonerna var omogna och instabila. Presentationen blev otydlig och opedagogisk pga. de små skärmfönstren
- Det var svårt med parametersättning dvs. det var svårt för användarna att själva mata in de nödvändiga manuella inställningar som krävdes för att få WAP att fungera. Detta är idag löst med att inställningarna skickas via sms.
- GPRS-tekniken var ännu inte införd vilket medförde låg hastighet och höga kostnader för kunden.
- WAP-standarden innehöll ingen säkerhetsmetod vilket medförde att innehållet i vissa tjänster som t.ex. mobila banktjänster blev starkt begränsade.

Detta medförde dock inte att inte tanken med att använda mobilen i Internetsammanhang inte var lockande. Nokia, Telia-Sonera och Handelsbanken inledde år 2000 diskussioner kring om det gick att göra Handelsbankens dåvarande mobila banktjänst säkrare (Arvidsson, 2006). Författaren diskuterar fortsättningsvis om att arbetet med att standardisera WAP hade fortsatt och nu fanns det specificerat hur en säkerhetslösning byggd på PKI (Public Key Infrastructure) skulle utformas, den kallas WPKI (Wireless Public Key Infrastructure) och härstammar från WPKI-föreningen (Se Bilaga 8) Då Handelsbanken redan använde en säkerhetslösning baserad på PKI skulle en WPKI-baserad mobiltjänst kunna integreras lättare. De begränsningar som tidigare funnits i utbudet av banktjänster mobilt skulle nu helt kunna elimineras. Enligt Gruvö & Rimming (2004) så var problemen med WPKI liknande de som finns i övrigt i den mobila världen nämligen minnesbegränsningar. Författaren hänvisar till att det inte är lika enkelt som i en Internet browser att lagra en lång lista med betrodda CA-certifikat. Detta har lösts genom att istället för att lagra certifikaten på mobiltelefonen lagra en pekare till en URL-adress där certifikatet ligger. Dock bedömde tillslut WPKI-föreningen att då mobila tjänstelösningar genom WAP hade fått så dåligt rykte att en vidareutveckling av Handelsbankens mobila tjänst var utsiktslös. Dock fanns här en standard för att kunna göra dessa transaktioner säkra (Arvidsson, 2006).

3.11 Sammanfattning teoretisk ramverk

Sammanfattningsvis har den teoretiska genomgången behandlat några centrala teman kring mobil säkerhet. Framförallt vill vi rikta läsarens uppmärksamhet på Hu et al:s (2005) tekniska och ledningsstyrda procedurer vilka appliceras på m-commerce, vilka är presenterade under 3.1. Även riskerna och hoten som finns i WAP-gateway och genom virus är för oss elementära för den kommande analysen.

4 Resultat och analys

Den empiriska undersökningen utfördes genom djupintervjuer (Bilaga 1-4), samt en surveyundersökning (Bilaga 6-7).

En inledande telefonintervju genomfördes med Anders Larsson som arbetar på företaget WIP (Bilaga 1). Detta för att vi skulle få en bättre förståelse för begrepp inom vårt ämnesområde redan i början av uppsatsarbetet. Larsson gav svar på vad som används i dagsläget vad gäller säkerheten kring mobila transaktioner och mobilt Internet användande. Han redogjorde även för möjliga tjänster som finns för fast Internet och vilka möjligtvis kan överföras till den mobila marknaden.

Efter att vi genomfört litteraturstudien och fått en förståelse för mobiltjänsters säkerhet påbörjades arbetet att insamla djupintervjuer med aktörer (bilaga 1-4) och utvecklare samt genomförandet av en Internetbaserad surveyundersökning (bilaga 6-7) vilken resulterade i 705 svarande.

Under följande underrubriker presenterar vi svaren som surveyundersökningen genererat samt vår analys av resultatet. Efter presentationen av surveyundersökningen följer vår analys av säkerheten i dagsläget.

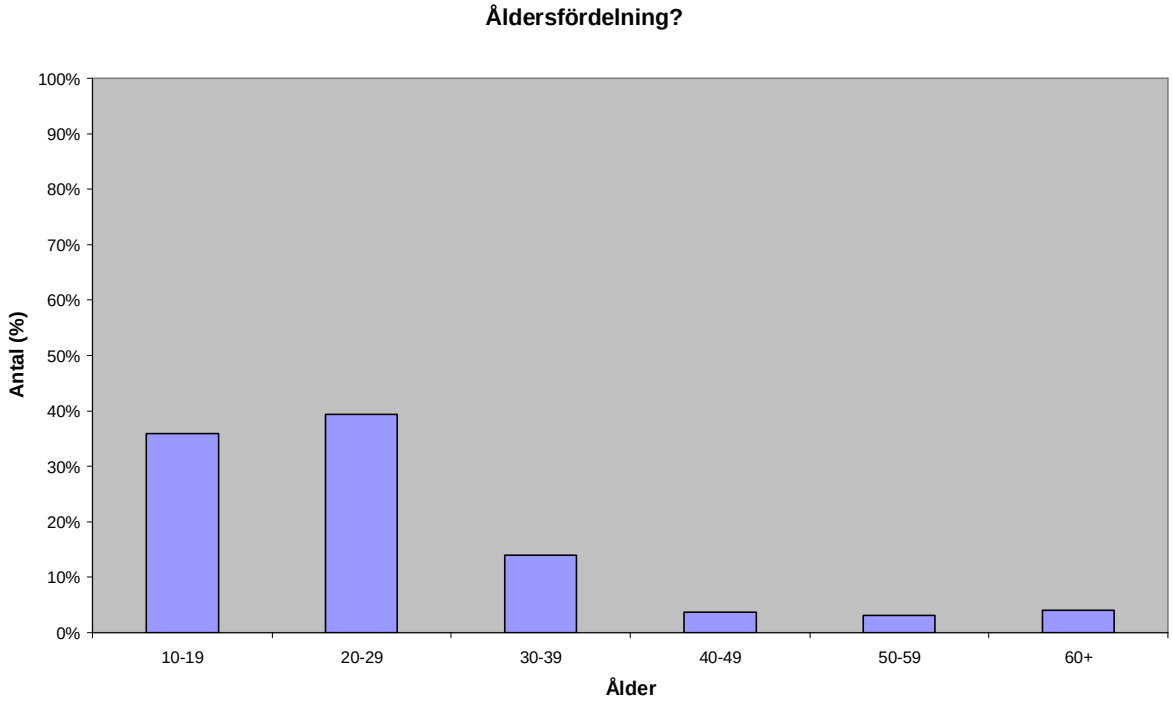
4.1 Surveyundersökning

4.1.1 Fråga 1 & 2 - Kön & Ålder

Första frågan ger svar på respondenternas kön och den andra på åldersfördelningen bland respondenterna. Båda dessa frågor är intressanta då människor i olika åldrar ofta kan ha olika uppfattning gentemot produkter och tjänster likväl som att kön kan ha inverkan. Den uppfattning vi själva har vad gäller ålder och inställning till tekniska tjänster är den att dessa tjänster ofta mestadels tilltalar yngre människor.

Könsfördelningen i surveyundersökningen blev 68 % manliga respondenter och 32 % kvinnliga respondenter.

Åldersfördelningen av respondenterna utföll enligt figur 5. Av resultatet kan vi utläsa att den största gruppen svarande finns i de två första kategorierna med respondenter mellan åldrarna 10 till 29 där kategorin 20-29 år har något större del svarande. Utöver övervikten i de två första kategorierna finner vi om övriga att 30-39 års kategori innehar flest respondenter samt att något fler svarande finnes i 60+ kategorin än mot 40-49 samt 50-59 kategorierna.



Figur 5 – Fråga 2

4.1.1.1 Analys Fråga 1 & 2

Då det genom vår webbaserade surveyundersökning inkommit svar främst från ålderskategorierna 10-19 och 20-29 kan vi konstatera att det är främst personer under 30 som använder olika forum på Internet och har intresse av besvara frågor rörande mobilt Internet. Dessa ålderskategorier anser vi, generellt, ha störst teknikintresse och också mest kännedom om möjligheterna som finns via olika forum och därför använder sig utav dessa. Då det var färre respondenter mellan 40-59 och något mer svarande bland 60+ kan vi göra ett antagande om att i 60+ kategorin återfinns till största del pensionärer som kan ha mer tid att undvara för att svara på frågor av denna karaktär.

Genom att det är främst yngre som svarat på vår enkät kan det eventuellt påverka svaren. Då vi antagit tidigare att det är de yngre som har mest teknikintresse kan det vara så att dessa även använder mobilt Internet i större utsträckning än övriga. Det kan också innebära att de har mer kunskap vad gäller säkerheten i dessa mobila nät vilket kan medföra att de anser att det är säkert. Det går också att vända på detta resonemang och antaga att de äldre som ej är så teknikintresserade inte kan så mycket om säkerheten kring dessa produkter och då eventuellt anser att det är säkert eftersom människor använder tjänsten.

Utifrån könsfördelningen kan vi konstatera att den största delen svarande var män. Detta anser vi bero på att män är generellt mer teknikintresserad och att dessa mer rör sig i forum än vad kvinnor gör. Detta kan enligt samma resonemang som ovan leda till sneda svar.

4.1.2 Fråga 3 - Har du en mobiltelefon med åtkomst till Internet? (WAP)

Av respondenterna ville vi veta hur många som idag innehar en mobil som har möjlighet att använda Internet.

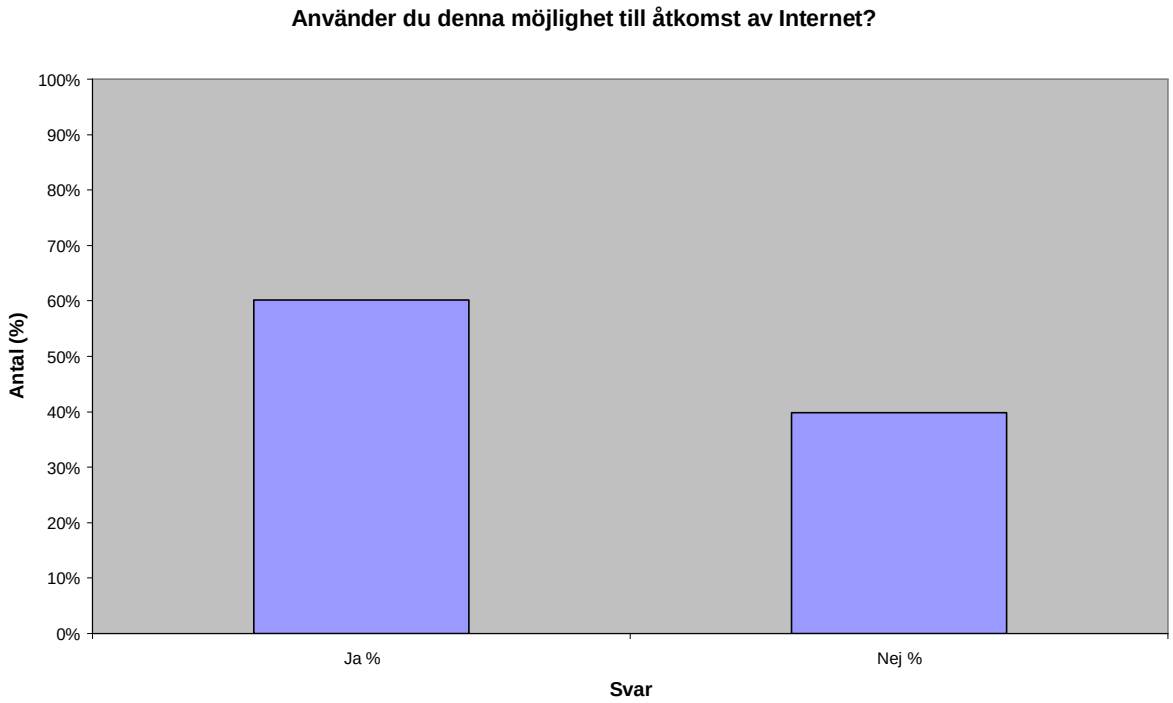
Av de svarande angav 87 % att de idag har en telefon som har möjlighet att använda Internet.

4.1.2.1 Analys fråga 3

Denna fråga ger oss svaret på hur många respondenter som har en mobiltelefon vilket då är intressant att jämföra med nästkommande fråga. Vi kan dock konstatera att de flesta personer har relativt nya mobiltelefoner då det endast är 13 % som inte har en mobil med åtkomst till Internet.

4.1.3 Fråga 4 - Använder du denna möjlighet till åtkomst till Internet?

För att bygga vidare på den föregående frågan och få en uppfattning om hur många som verkligen utnyttjar möjligheten att använda Internet på sin mobiltelefon ställdes fråga 4.



Figur 6 – Fråga 4

Svaren i de två kategorierna utföll i att 60 % svarar att de använder Internet via mobilen och 40 % att de inte gör det.

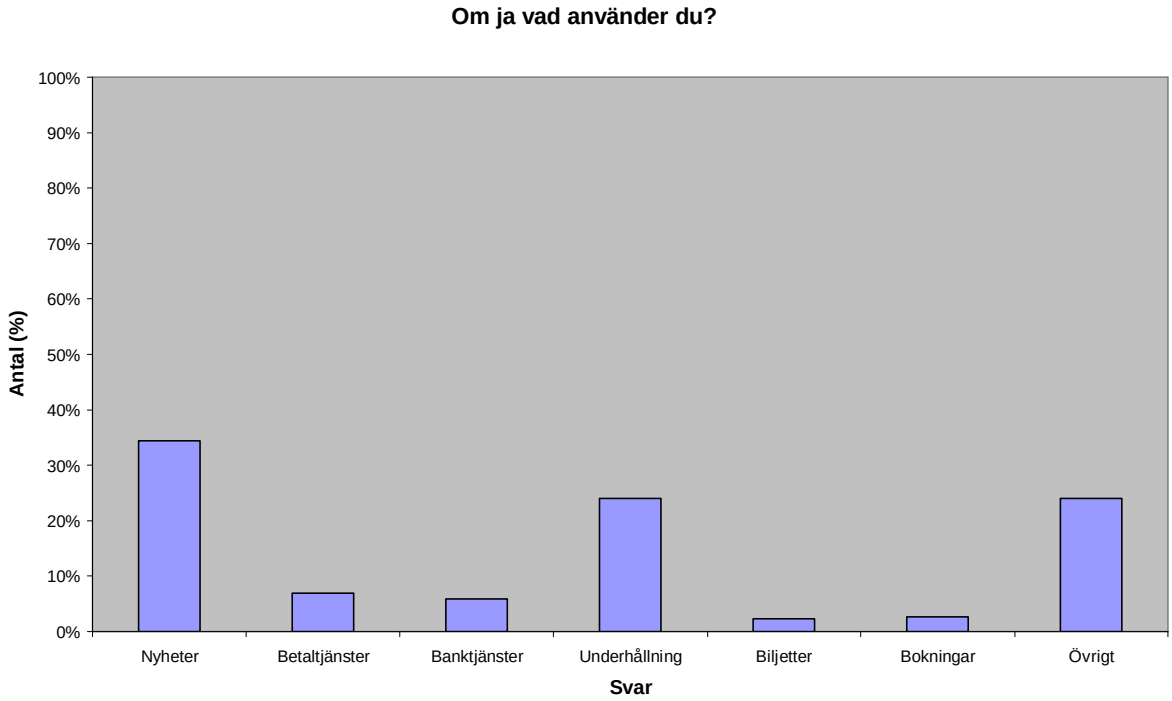
4.1.3.1 Analys fråga 4

Genom att jämföra denna fråga med förgående frågeställning kan vi konstatera, att av de 87 % som har en mobiltelefon är det 60 % som utnyttjar denna möjlighet. Då vi tidigare resonerat kring att yngre användare är mer teknikintresserade kan det vara intressant att se hur många av de yngre respondenterna (10-29 år) som använder möjligheten till mobilt Internet gentemot äldre. Detta även för att se om vårt resonemang kring detta stämmer. I åldrarna 10-29 så är det 78 % som använder sin möjlighet till mobilt Internet vilket då kan ställas mot resterande ålderskategorier (30-60+) där endast 22 % använder möjligheten till mobilt Internet. Här kan vi då dra slutsatsen att inom detta område är det mestadels yngre männi-

skor som använder sig av mobilt Internet. Vi kan också dra slutsatsen att vårt resonemang kring teknikanvändande gentemot ålder stämmer tillfredställande.

4.1.4 Fråga 5 - Om ja vad använder du?

De som gav ett jakande svar på fråga fyra fick nu vidare svara på denna fråga medan de som svarade nekande uppmanades att fortsätta till fråga nummer sju. Frågeställningen i fråga fem besvaras genom att välja de alternativ som respondenten använder mobilt Internet till. Detta för att få svar på vad de som använder Internet idag nyttjar det till.



Figur 7 – Fråga 5

Svaren (figur 7) visar att flest respondenter som använder Internet på sina mobiltelefoner idag utnyttjar nyheter samt underhållningsinformation. Betaltjänster och banktjänster används av vissa medan kategorierna biljetter och bokningar har mycket få svarande. I övrigt kategorin finner vi att 24 % även angett att de använder andra tjänster än de alternativ vi presenterat.

4.1.4.1 Analys fråga 5

Utifrån denna fråga kan vi dra slutsatsen att de flesta respondenterna använder någon sorts tjänst där just säkerheten inte är av stor vikt. Dessa kan då vara tjänster inom underhållning, nyheter och nöje. När det kommer till olika tjänster som kräver hög säkerhet (bank- o betaltjänster) så är det idag endast 12 % av respondenterna som utnyttjar dessa. Vidare kan ses att kategorier som biljett- och bokningstjänster idag inte anses så intressant då de tillsammans endast utgör 5 % av respondenternas svar.

Genom denna låga svarsfrekvens gällande vissa kategorier gör vi även ett antagande att många av respondenterna inte alls vet om att dessa tjänster finns att tillgå. Detta kan också styrkas av att det är betydligt fler som vill använda dessa tjänster (23 %) än som verkligen gör det i dagsläget.

4.1.5 Fråga 6 - Hur ofta använder du dessa tjänster?

Även denna fråga är en följdfråga till fråga nummer fyra och bygger vidare på fråga fem. Här svarade de som använder Internet på sin mobiltelefon och som sedan angett vad de använder för typ av tjänster på hur ofta dessa används.

Resultatet (bilaga 9) visar en jämn fördelning mellan de tre första kategorierna (dagligen, tre dagar i veckan eller mer och en dag i veckan) med cirka 20 % svarande i varje medan den sista kategorin där de som använder tjänsten mer sällan än 1 gång i veckan resulterade i 38 % av de svarande.

4.1.5.1 Analys fråga 6

Här kan vi konstatera att ca 60 % av respondenterna använder mobilt Internet minst 1 ggr/vecka vilket kan anses relativt hög beroende på vilka tjänster som används. Att använda en nyhetstjänst 1 ggr/veckan kan anses relativt sällan medan att boka 1 biljett i veckan anses relativt ofta. Dock är det fortfarande en stor del av respondenterna (ca 38 %) som använder mobilt Internet mer sällan än 1 ggr/vecka.

4.1.6 Fråga 7 - Vilka tjänster skulle du vilja använda?

Frågan ställdes för att få reda på både vilka tjänster de som redan i dagsläget använder Internet vill använda eller se som ytterligare tjänster, samt att få svar från övriga personer om vilka tjänster de kan se som intressanta.

Från frågans svarsalternativ kan ett relativt jämlikt mönster utläsas mellan de olika svarsalternativen (bilaga 9). Det som sticker ut från mängden är att alternativet betaltjänster har ungefär ett hundra mindre svar än de övriga.

4.1.6.1 Analys fråga 7

Intressant under denna frågeställning är att de tjänster som kräver hög säkerhet (bank- o betaltjänster) har lägre svarsfrekvens än övriga. Detta gäller speciellt betaltjänster då frekvensen här är tydligt mindre än övriga tjänster. Genom detta går det att konstatera att återigen är de tjänster som kräver hög säkerhet mindre attraktiva än de övriga tjänsterna. Dock återstår frågan om detta är just på grund av säkerheten eller på grund av andra faktorer.

4.1.7 Fråga 8 - Skulle du kunna tänka dig att betala över Internet med mobiltelefonen?

Frågan ställdes till hela populationen för att få vetskap om hur de ställer sig till att betala med mobiltelefonen över Internet.

Frågan resulterade i (bilaga 9) ett nästan likställt resultat mellan jakande och nekande svar. Av respondenterna svarade 49 % ja och 51 % nej.

4.1.7.1 Analys fråga 8

Människor idag är kluvna inför denna frågeställning. Detta då ca 49 % svarar jakande medan ca 51 % är mer negativa till att betala via mobilt Internet. Då merparten av respondenterna är under 30 år så kan vi då konstatera att hälften av dagens yngre generationer kan tänka sig betala mobilt. Detta bör vara av stort intresse för företag som arbetar med den här typen av tjänster då efterfrågan tydligt finns.

4.1.8 Fråga 9 - Skulle du kunna tänka dig att sköta dina finansiella affärer via mobiltelefonen? (Såsom bankärenden, aktiehandel m.fl.)

Här ville vi få svar på vad allmänheten kan tänka sig att göra finansiella affärer via mobiltelefonen.

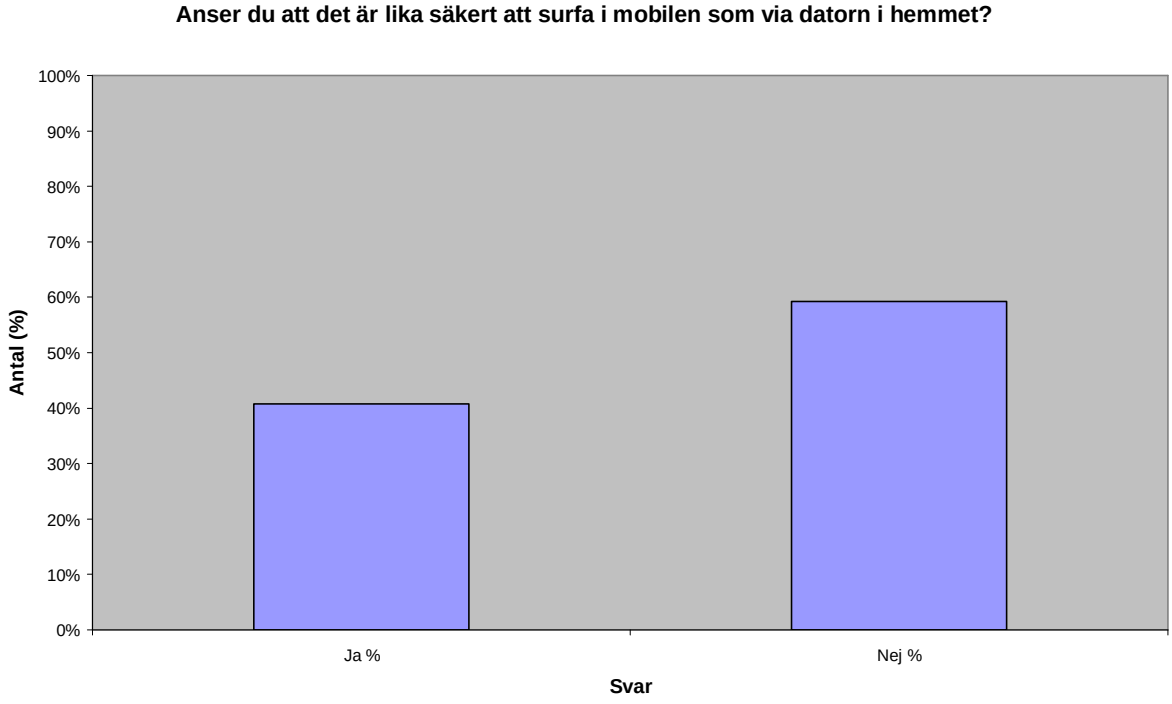
Frågan gav ett svar med övervikt åt nej alternativet då 60 % av respondenterna har svarat att de inte skulle kunna tänka sig att sköta finansiella affärer via mobiltelefonen.

4.1.8.1 Analys fråga 9

Utifrån respondenternas svar på ca 40 % ja respektive ca 60 % nej så kan vi se att hantering av bankärenden och liknande tjänster är något mindre efterfrågade än betalningar (se fråga 8). Detta kan bero på att ofta hanteras större summor i ens bank- och aktieärenden än när en person bara vill betala för en viss inhandlad produkt på Internet. När det gäller att hantera hela sin egen ekonomi kan det kännas säkrare att göra det via medier som upplevs säkrare. Dock är det fortfarande en stor del av respondenterna som skulle kunna tänka sig att sköta sina bankärenden via mobiltelefonen så intresset finns.

4.1.9 Fråga 10 - Anser du att det är lika säkert att surfa i mobilen som via datorn i hemmet?

Anser allmänheten att det är lika säkert att surfa från mobiltelefonen som det är när surfningen sker från en fast dator i hemmet.



Figur 8 – Fråga 10

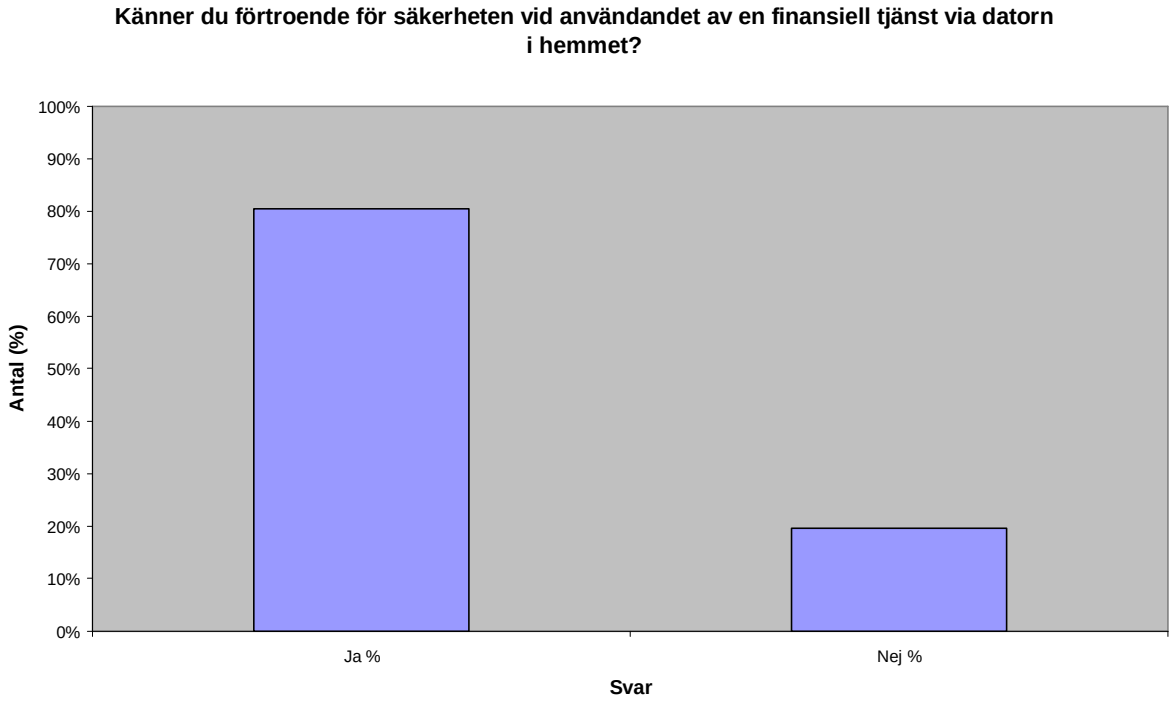
Respondenternas svar på denna fråga gav ett nekande svar då 60 % svarande att de inte anser det lika säkert att surfa i mobiltelefonen.

4.1.9.1 Analys fråga 10

Den här frågan var för oss mycket viktig då den rent ut svarar på hur användare uppfattar säkerheten mellan dessa två olika medier. Då ca 60 % svarade att de ansåg det lika säkert anser vi även här att respondenterna var lite kluvna. Respondenternas svar här kan även jämföras med förgående fråga där ca 60 % sa nej till att sköta sina finansiella affärer via mobiltelefonen. Detta tolkar vi som så att de som inte vill använda mobilen för sina finansiella affärer vill inte det på grund av att de inte anser det lika säkert som att sitta hemma vid datorn och komma åt dessa tjänster.

4.1.10 Fråga 11 - Känner du förtroende för säkerheten vid användandet av en finansiell tjänst via datorn i hemmet? (Såsom överföringar av pengar, betala räkningar o andra banktjänster)

Har allmänheten ett förtroende rörande säkerheten när de använder finansiella tjänster i sina hem med fast Internet uppkoppling.



Figur 9 – Fråga 11

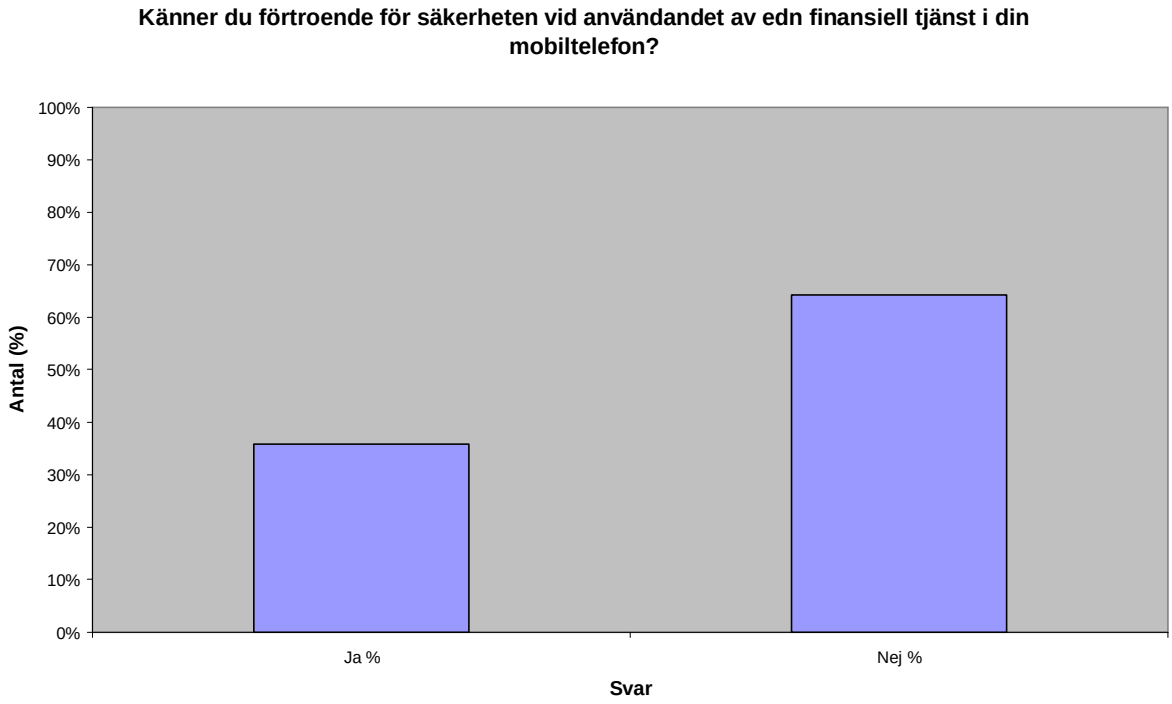
Av surveyundersökningen svarade 80 % att de känner förtroende för säkerheten vid användandet av en finansiell tjänst via sin dator i hemmet.

4.1.10.1 Analys fråga 11

Majoriteten (ca 80 %) av respondenterna ansåg här att det är tillräckligt säkert att använda finansiella tjänster via datorn i hemmet. Respondenterna har med andra ord stort förtroende för en uppkopplad dator i hemmet och känner sig väl skyddade och säkra för att använda dessa tjänster.

4.1.11 Fråga 12 - Känner du förtroende för säkerheten vid användandet av en finansiell tjänst i din mobiltelefon?

Känner individerna i surveyundersökningens population förtroende för säkerheten om de använder en finansiell tjänst i sin mobiltelefon.



Figur 10 – Fråga 12

Resultatet visar att 64 % inte känner förtroende gällande säkerheten runt en finansiell tjänst i mobiltelefonen.

4.1.11.1 Analys fråga 12

Här var svaren från respondenterna mer osäkra jämfört med fråga 11. Endast ca 36 % har förtroende för säkerheten via sin mobiltelefon. Här går det enkelt att konstatera att respondenterna har mer förtroende för datorn i hemmet och anser att det är säkrare att använda tjänster som kräver hög säkerhet via denna. Mobiltelefonen däremot har svårare att bli accepterad rent säkerhetsmässigt. Dock ska det sägas att 36 % verkligen anser att det är säkert så det finns idag marknad för denna typ av tjänster rent förtroendemässigt.

4.2 WAP-säkerhet vid transaktioner

Ett system inom m-commerce måste innehålla vissa funktioner vars syfte är att säkra transaktioner. Hu et al (2005) beskriver dessa funktioner och nedan följer en genomgång av dessa i jämförande med WAP:

4.2.1 Konfidentiellitet

Information som går genom luften är enligt Hu et al (2005) alltid mer osäker än den som går genom fasta nät. Detta därför att det är lättare att fånga upp informationen. För att informationen som sänds över WAP-nätverket inte skall bli tillgänglig för obehöriga personer

måste den krypteras (Hu et al, 2005). Detta är något som enligt Mikal (2005) genomförs i WAP-nätverket genom WTLS och TLS. Dock finns det en svag punkt och det är en WAP-gateway (Dornan, 2001)(Hu e t al, 2005). Mikal (2005) anser även att det finns en lösning på detta (Se kap 3.7). En annan fara är att det på vissa WAP-telefoner går att stänga av krypteringen. All GSM-trafik är även säkrad genom en VPN-tunnel (S. Axelsson, personlig kommunikation, 2006). För att kunna fånga upp dessa signaler krävs det enligt samma källa utrustning på runt 1 miljon kronor vilket medför att detta ej är av intresse. WAP-nätverket uppfyller därför kravet om konfidentiellitet om krypteringen är påslagen.

4.2.2 Verifiering

De iblandade parterna måste kunna försäkra inför varandra att de är den de utger sig för att vara. Detta sker genom verifiering (Hu et al, 2005). Inblandade parter är enligt samma författare: Användare, nätoperatör, nätleverantör, kreditreferens, autentiseringsmyndighet och eventuella andra parter. Detta kan idag lösas genom att alla parter är certifierade genom elektroniska certifikat som delas ut av en frigående organisation. Arvidson (2006) beskriver dessa som CA-certifikat. Detta innebär dock ett problem då en mobiltelefon enligt Arvidson (2006) inte har minneskapacitet nog att lagra en lång lista av betrodda CA-certifikat. Dock kan detta lösas genom att istället lagra en pekare till en URL-adress där certifikatet ligger. På detta sätt går det att verifiera inblandade parter.

Dock finns det ett problem gällande verifiering i ett GSM-nät (S. Axelsson, personlig kommunikation, 2006). Detta är att användaren autentiserar sig mot GSM-nätverket men GSM-nätverket autentiserar sig inte mot användaren. Användaren vet i dagsläget helt enkelt inte om det är rätt nätverk han/hon är uppkopplad mot.

WAP kan därför inte uppfylla kravet om verifiering.

4.2.3 Integritet

Vid en transaktion måste parterna kunna vara säkra på att informationen som skickas emellan dem inte är ändrad av någon obehörig. Detta sker genom att lägga till elektroniska signaturer (Hu et al, 2005) eller CA-certifikat (Arvidson, 2006). Detta medför att WAP uppfyller kravet om integritet.

4.2.4 Auktorisering

Det måste enligt Hu et al (2005) även finnas processer som bekräftar att en person är behörig att genomföra en efterfrågad transaktion. Detta kan lösas genom inloggningsrutiner med användarnamn och lösenord eller användning av liknande koddosor som används vid inloggning till vissa banker via datorn i hemmet. Dock anses koddosor alltför komplext för mobila lösningar (A. Larsson, personlig kommunikation, 2005). Detta medför att auktoriseringen går att lösa lika säkert som via datorn i hemmet men denna möjlighet används inte på grund av dess komplexitet.

4.2.5 Tillgänglighet

Denna rubrik relaterar till att all nödvändig information om en tjänst respektive en tjänst alltid skall vara tillgänglig för alla inblandade parter. Hu et al (2005), Axelsson (S. Axelsson, personlig kommunikation, 2005) och Von Braun (J. Von Braun, personlig kommunikation, 2006) inser faran med framtida Dos-attacker vilket de anser kan medföra att mobiltelefonen inte går att använda eftersom den bombarderas med SMS-meddelanden. Detta är en

fara tills mobiltelefonerna får större processorkraft och mer internminne vilket medför att det går att installera olika säkerhetsprogramvara (J. Von Braun, personlig kommunikation, 2006; S. Axelsson, personlig kommunikation, 2005).

Hu et al (2005) inser också risken med att trådlösa nät påverkas lättare av störningar än fasta nät. Trådlösa nät kan även ha döda signalzoner vilket medför att mobilen inte får kontakt med GSM-nätet.

Tillgängligheten när det gäller mobiltelefoner är därför i dagsläget inte säkrad

4.2.6 Ej förnekbar

Inblandade parter i en transaktion skall heller inte kunna förneka att de har varit inblandade i transaktionen. Detta kan enligt Hu et al (2005) lösas genom digitala signaturer. Parterna måste kunna bevisa att motparterna är iblandade. Då det finns en lösning till detta anser vi att detta uppfyller säkerhetskravet för mobila transaktioner.

4.3 Virus

Virusens framtid gällande mobila enheter och störningar för deras applikationer är något alla som vi intervjuat för uppsatsen tror kommer slå till snart och bli ett problem. Enligt Willassen förekommer redan nu virus som sprids via bluetooth (S. Willassen, personlig kommunikation, 2006) men ingen av de vi har varit i kontakt med har ännu hört talas om någon större virusattack. Men enligt Axelsson är det bara en tidsfråga innan ett första virus kommer att dyka upp (S. Axelsson, personlig kommunikation, 2006). Det förekommer dock redan andra typer av hot liknande virus i form av maskar som enligt samma källa kan riktas mot en specifik användare för att komma åt dennes användarnamn och lösenord för exempelvis en banktjänst. Enligt samma källa förekommer även Phishing mot mobila enheter men inget av dessa sätt utgör idag något reellt hot mot gemene man. Dock kan ett framtida behov vara ett spamfilter även för mobiltelefonen.

När utvecklingen nu går mot mer avancerade mobila system och telefoner kommer de också bli känsligare för virus enligt Atea Security (2005), detta eftersom mer funktionalitet byggs in viken i sin tur kan manipuleras genom virusattacker. Enligt von Braun krävs det att telefonerna utrustas med mer internminne och processorkraft för att säkerhets- och antivirusprogram skall kunna göras mer avancerade (J. von Braun, personlig kommunikation, 2006). Det krävs enligt tidigare källa att sådana program tas fram i ett tidigt stadium för att stoppa en invasion av virusattacker som kan komma eftersom det enligt F-secure (2005) just nu i stort sett är öppet för virusmakare att infektera näten.

4.4 Övriga risker

Nedan diskuteras övriga brister som framkommit under intervjuer.

4.4.1 Monokultur

En risk som i framtiden föreligger enligt Axelsson är att de mobila plattformarna kommer gå samma öde till mötes som den situation som idag existerar hos öppna plattformar (S. Axelsson, Personlig kommunikation, 2006). Plattformsmarknaden idag för persondatorer domineras idag totalt av Microsoft vilket enligt tidigare källa är mycket farligt säkerhetsmässigt, dels för att säkerheten inte håller tillräckligt hög standard men framför allt för att en brist i systemet kan drabba alla användare. Detta gör att det är intressant ämne för ekono-

misk brottslighet då det finns chans komma åt en stor mängd användare och därav stora belopp. Plattformskulturen som idag finns för mobila enheter har ett bredare utbud vilket gör att samma monokultur som tidigare diskuterats inte föreligger i dagsläget.

4.4.2 Kapacitet

För att i framtiden kunna utföra säkrare mobila transaktioner krävs det enligt von Braun förbättringar i form av ökad processorkraft och internminne till de mobila enheterna (J. von Braun, personlig kommunikation, 2006). Det krävs nya administrativa program för att kontrollera de mobila plattformarna och enligt Willassen (personlig kommunikation, 2006) kommer dessa behöva ha samma teknik som dagens datorer med säkerhetsprogram, brandvägg och antivirusskydd. Det finns idag enligt von Braun (personlig kommunikation, 2006) administrativa kontrollprogram för mobila plattformar men det optimala vore ett program som sammanbinder virusskydd, personlig brandvägg, kryptering och behörighets-kontroll. Samma författare fortsätter med att diskutera behovet av program som kan kontrollera att säkerhetsprogrammen är uppdaterade.

4.4.3 Offentlig användning

En annan säkerhetsaspekt som Willassen (personlig kommunikation, 2006) tar upp som inte hör till de tekniska aspekterna är att mobiltelefonen används oftast i offentliga miljöer. Det kan därigenom vara möjligt för obehöriga att se vad en person använder för tjänster via sin mobiltelefon och då rent visuellt uppfatta t.ex. användarnamn och lösenord.

5 Övergripande analys

Denna del av analysen binder samman de olika delarna i förgående analys till respektive forskningsfråga. Motivet bakom detta är för att göra det lättare för läsaren att förstå hur vi kommit fram till våra slutsatser.

5.1 Analys – Forskningsfråga 1

Utifrån de svar som framkom på fråga 12 fick vi fram att 64 % av respondenterna inte har förtroende för säkerheten vid användandet av en finansiell tjänst i mobiltelefonen. Bara genom att titta på utfallet av denna fråga kan vi konstatera att majoriteten av mobiltelefonanvändarna ej har förtroende för säkerheten kring denna typ av tjänst. Detta styrks även av fråga 10 där respondenterna fick svara på om de anser att det är lika säkert att surfa via mobilen som via datorn i hemmet. Majoriteten svarar här att de ej anser det vara lika säkert att surfa i mobilen vilket stödjer ett negativt svar på vår forskningsfråga.

Då vi jämför frågorna 11 och 12 vilka svarar på förtroendet för säkerheten gällandes en finansiell tjänst via mobilen respektive datorn i hemmet, ser vi stora skillnader i svarsalternativen. Hela 80 % anser att de diskuterade tjänsterna är säkra att använda via datorn i hemmet medan endast 36 % anser att det är säkert via mobilen. Detta styrker vår uppfattning från de tidigare diskuterade frågorna att förtroendet för säkerheten hos mobila tjänster är lågt.

När vi kopplar ihop ovan ställda frågor med fråga 5 där vi undersöker vilka tjänster som används via mobilt Internet, kan vi se att de tjänster som används idag är tjänster som inte kräver hög säkerhet. Användarna brukar inte tjänster som betal- och banktjänster i stor utsträckning förmodligen delvis beroende på att de ej har förtroende för säkerheten. Däremot så skulle användarna gärna använda tjänster av detta slag vilket besvaras med hjälp av fråga 7 (Vilka tjänster skulle du vilja använda?) där bank- och betaltjänster ligger i samma nivå som övriga tjänster. Detta leder fram till att användarna har intresse för dessa tjänster och skulle gärna använda dem om deras förtroende för säkerheten förbättras. Då hälften av respondenterna svarar att de skulle kunna tänka sig att betala över Internet med mobiltelefonen styrker detta vårt förra påstående om att användarna har intresse för betaltjänster via mobilen.

5.2 Analys forskningsfråga 2

Ur den föreliggande analysen kan vi lyfta fram ett antal punkter som tillsammans ger underlag för slutsatser om det är ”lika säkert att utföra betalningstjänster via en mobiltelefon som med en stationär dator i hemmet”. Det finns avseenden där säkerheten är jämförbar (se tidigare avsnitt). De punkter som vi ser som skiljande ur säkerhetssynpunkt då vi jämför användandet av en betaltjänst via en mobil med att utföra denna tjänst via datorn i hemmet är:

- Trådlöshet
- Offentlig användning
- WAP-gateway
- Bristande säkerhetsprogramvara
- Bristande minneskapacitet

Var och en av dessa punkter analyseras nedan under respektive rubrik.

5.2.1 Trådlöshet

Då den mobila tekniken för att surfa alltid kommer att behöva ske trådlöst finns under alla omständigheter risken att något kan fånga upp signalerna. Detta medför att informationen enligt Hu et al (2005) är mer osäker jämfört med en stationär dator i hemmet som är fast ansluten. Utifrån vår analys om konfidentiellitet kan vi dock styrka genom Axelsson (personlig kommunikation, 2006) att någon sådan risk inte existerar för en privatperson i dagsläget. Eftersom en sådan utrustning enligt senast nämnda källa kostnadsmässigt ligger runt 1 miljon kronor finns det ingen reell risk att en privatperson inhandlar dylik utrustning och tillgriper sig den kunskapen. Detta i syfte att avlyssna och avkoda signaler för att sedan utnyttja detta i syfte att få information om privata personers betaltjänstutförande. Men eftersom risken alltid finns att fånga upp signalerna och med rätt utrustning faktiskt avkoda den anser vi att på denna punkt är inte säkerheten lika bra som vid utförandet av en betaltjänst om den utförs på en dator som är fast uppkopplad mot Internet. Skulle dock datorn vara trådlöst uppkopplad mot en router antar vi emellertid att en liknande risk som för mobiltelefonen uppkommer då signalerna någonstans i kommunikationen skickas trådlöst.

5.2.2 Offentlig användning

Då mobilen till största del används i offentliga miljöer är detta enligt Willassen (personlig kommunikation, 2006) ytterligare en aspekt att ta i beaktande för säkerheten gällande mobila betalningstjänster. Om användaren utför en betaltjänst från sin dator i hemmet är det enligt oss ingen större risk att någon obehörig visuellt kan se vad personen gör och uppfatta vilka koder och lösenord som används. Samma villkor gäller dock inte när en mobil används i offentlig miljö, eftersom det då kan finnas en risk att någon annan än användaren ser vilka lösenord och koder som används. Det kan således enligt vår uppfattning föreligga en större risk att någon visuellt observerar vad en användare utför på sin mobiltelefon än om en betaltjänst utförs på datorn i hemmet.

5.2.3 WAP-gateway

När det gäller betaltjänster som utförs via WAP finns det en svag punkt eftersom signalen måste gå via en gateway för att nå slutdestinationen (Dornan, 2001; Hu et al, 2005; Mikal 2005). Sändningen kan då kopieras när den når gatewayen om någon obehörig har tillgång till denna. Detta då det enligt ovan nämnda författare i gatewayen sker en omkryptering från WTLS till TLS. Enda sättet att försäkra sig om att detta inte sker är enligt Dornan (2001) att den som tillhandahåller tjänsten själv också äger gatewayen. Hur detta förhåller sig rörande betaltjänster kan vi inte svara på då vi inte lyckats nå aktörer och få svar på denna fråga. Därför kan endast spekulationer göras om detta föreligger eller inte men eftersom den faktiska risken finns är det enligt oss en säkerhetskillnad mot att använda en betaltjänst i hemmet.

5.2.4 Bristande säkerhetsprogramvara

Det krävs enligt von Braun (personlig kommunikation, 2006) och Willassen (personlig kommunikation, 2006) framtida förbättringar för säkerhetsprogramvara för mobiltelefoner. Detta för att förhindra exempelvis virusintrång eller DoS-attacker. Det finns enligt senast nämnda källor i dagsläget inte tillräckligt bra programvaror för detta vilket gör att en betal-

tjänst utförd via en mobil enhet jämfört med att utföra den via datorn i hemmet inte skyddas av likartad säkerhetsskydd.

Genom våra intervjuer har vi identifierat två hot som i dagsläget ses som de två största hoten. Dessa är virus och DoS-attacker.

5.2.5 Bristande minneskapacitet

Ett behov för att uppfylla en bättre säkerhetsprogramvara är enligt von Braun (personlig kommunikation, 2006) att telefonernas minneskapacitet utökas. Därför ser vi att även ett behov av en ökad prestanda hos mobiltelefoner föreligger för att kunna uppfylla säkerhetsprogramvarans krav.

5.3 Analys av övriga framkomna resultat

Genom fråga 4 så svarar respondenterna på om de använder mobilt Internet. Resultatet blev att 60 % av respondenterna använder denna tjänst. Detta innebär att flertalet mobiltelefonanvändare brukar denna tjänst men att det finns utrymme för större användning.

Surveyundersökningen innehöll även en ålderfråga vars syfte var att ge oss information om vilka det var som svarade på undersökningen. När vi kopplade denna fråga till fråga 4 så fick vi fram vilket ålderskategori som främst använder dessa tjänster. Vår uppfattning innan arbetet var att det var främst yngre människor som använde sig av mobilt Internet då de oftast anses mer teknikintresserade. Detta stämde väl då vi genom svaren fick fram att i åldrarna 10-29 är det 78 % som använder denna tjänst.

Tjänster som använts mest med hjälp av mobilt Internet är inom nyheter och underhållning. Detta får vi fram genom fråga 5 i surveyundersökningen. Detta tror vi främst bero på att dessa tjänster är lätta att använda och inte kräver hög säkerhet. Det är även dessa som marknadsförts mest i samhället. Det är även en enkel och tillgänglig sysselsättning t.ex. när respondenten väntar på bussen och behöver fördriva tiden.

Genom fråga 5 fick vi reda på vilka tjänster som är populära och används av respondenterna. De tjänster som är minst attraktiva att använda är bank- och betaltjänster. Dessa tjänster kräver hög säkerhet, vilket kan vara orsaken till att de är minst populära. Även tjänster som innebär bokningar och biljetthantering är mindre populära, vilket kan bero på att också dessa tjänster kräver något mer förtroende för att säkerheten är löst än t.ex. vad tjänster som nyheter och underhållning fordrar.

En annan intressant aspekt att diskutera som vi fick fram genom surveyundersökningen är hur ofta respondenterna använder mobilt Internet. 60 % av respondenterna använder mobilt Internet vilket vi anser relativt högt beroende på vilka tjänster det gäller. Att använda mobilt Internet till att boka en biljett 1 ggr/veckan måste anses som högt medan att surfa på en nyhetssida 1 ggr/veckan kan anses som lågt.

Genom diskussionen om förtroende för mobil säkerhet ovan så framkom det även att förtroende för säkerheten vid användandet av Internettjänster via datorn i hemmet är hög. Denna diskussion härleder vi från fråga 11 då respondenterna fick svara på om de känner förtroende för säkerheten vid användandet av en finansiell tjänst via datorn i hemmet då 80 % svarade positivt.

6 Slutsatser

Här presenterar vi våra slutsatser kopplade till de två forskningsfrågor vi ställt och övriga slutsatser uppsatsen genererat.

1. Har användarna förtroende för säkerheten hos mobila betalningstjänster?

Utifrån vår undersökning kan vi konstatera att majoriteten av respondenterna inte känner förtroende för säkerheten gällande mobila betalningstjänster. Största delen anser att det inte är lika säkert att surfa via mobilen som via datorn i hemmet. Trots detta kan hälften av populationen tänka sig att betala över Internet via mobiltelefon, och en betydande del kan även tänka sig att utföra finansiella affärer med hjälp av mobiltelefon.

2. Är det lika säkert att utföra betalningstjänster och betalningar via en mobiltelefon som hos en stationär dator med fast Internet?

Vår slutsats är att en mobiltelefon inte når upp till samma säkerhetsnivå som hos en stationär dator med fast Internet. Detta beror till stor del på grund av följande faktorer:

- Trådlöst – *Då det mobila nätet är trådlöst är det lättare att fånga upp trafiken*
- Offentlig användning – *En mobiltelefon används ofta i offentliga miljöer vilket medför behov av visuellt skydd*
- WAP-gateway – *För att kunna säkra trafiken måste den WAP-gateway som används skyddas från intrång*
- Bristande säkerhetsprogramvara – *Bättre utvecklad säkerhetsprogramvara krävs*
  - Virus – *Behov av virusskydd*
  - Dos-attack – *Behov av skydd mot Dos-attacker*
- Bristande minneskapacitet – *Behov av utökad processorkraft och interminne*

3. Övriga slutsatser

- 60 % av mobiltelefonägarna använder möjligheten att ansluta till Internet
- Det är främst yngre användare som använder möjligheten att ansluta till Internet
- De mest frekvent använda tjänsterna är nyheter och underhållning
- Tjänster som kräver hög säkerhet är mindre attraktiva än andra tjänster
- Mobila Internetanvändare använder Internet minst 1 ggr/veckan
- Förtroendet för säkerheten kring datorn i hemmet är stort

7 Avslutande diskussion

Nedan följer en diskussion om de olika erfarenheter vi fått genom arbetet med uppsatsen. Vi presenterar även några förslag för fortsatta studier.

7.1 Erfarenheter

Att lägga ut en surveyundersökning på Internet medförde att vi snabbt och enkelt fick många respondenter. Vi sparade därför mycket tid på detta moment gentemot att genomföra en pappersbaserad surveyundersökning.

7.2 Motiveringar

Valet att inkludera OSI-modellen om WAP i teorikapitlet motiverar vi med att det ger en bra grund för förståelsen om hur WAP fungerar och även att läsaren kan se var säkerheten kommer in.

De respondenter som svarat på vår surveyundersökning är främst personer som besöker forum. Detta kan ha lett till en något smal population men då vi spred undersökningen på väldigt olika forum, ämnesmässigt, anser vi att vi fått en bra spridning.

7.3 Reliabilitet

Vårt mål var att eftersträva en komparativ studie mellan vår surveyundersökning och andra forskares undersökningar för att kunna stärka vår intersubjektiva reliabilitet. Då vi ej fann undersökningar vars syfte var att studera förtroende för mobil säkerhet var detta ej möjligt.

För att undvika slumpmässiga mätfel i surveyundersökningen genomförde vi den i ett standardiserat utförande. Då samma frågor ställdes till alla respondenter i samma miljö vad avser att de tillfrågades genom forum på Internet. Dock kan vi ej påverka miljön där respondenten sitter fysiskt, men detta tror vi inte påverkat vår undersökning negativt.

7.4 Validitet

Då alla intervjuer skett via telefon kunde vi inte använda inspelningsutrustning utan istället använde vi oss av vårt alternativa genomförandesätt. Detta innebär att vi antecknade stödord under intervjun för att i efterhand sammanfatta i löptext. Vi anser att vi tack vare stödordsanteckningarna inte ändrat innebörden i respondenternas svar och därvid bibehålligt hög validitet vad gäller detta förfarande.

För att erhålla en hög validitet genomförde vi ett pilottest angående frågorna till surveyundersökningen. Detta för att säkerställa att respondenterna uppfattar frågorna på det sätt vi avser.

Då vi i efterhand upptäckt brister gällande en fråga i surveyundersökningen har det lett till funderingar kring vår metod och speciellt framställningen av frågorna. Genom att inkludera personer med stor kunskap om frågeställningar i vårt pilottest kunde eventuella brister ha framkommit i ett tidigare skede.

Den brist som framkom vid frågeutformningen till surveyundersökningen presenteras nedan:

Fråga 3 – Har du en mobiltelefon med åtkomst till Internet?

Det finns möjlighet att vissa respondenter inte vet om de har åtkomst till Internet på sin mobiltelefon därför bör de haft möjligheten att svara ”Vet ej” på denna fråga.

Vi vet genom kommentarer på forumen att vissa respondenter ej svarat på denna fråga då de inte vet om de har en mobiltelefon med åtkomst till Internet. Vi tror dock ej att detta påverkat undersökningen till stor del då vi förmodar att dessa personer ej använder denna möjlighet. Detta svar påverkar heller inte våra slutsatser då de ändå besvarat de frågor som i huvudsak hjälper oss att svara på forskningsfråga 1.

7.5 Generalisering

Den generalisering vi kan göra i vår uppsats är relaterat till vårt urval av respondenter inför surveyundersökningen. Då vi lagt ut undersökningen på olika forum är det främst människor som rör sig i forum som svarat på surveyundersökningen. Detta innebär att vi främst kan generalisera våra resultat på forskningsfråga 1 att gälla personer som rör sig i dessa forum.

7.6 Problem

7.6.1 Avgränsningar

I kapitel 1.4 – Avgränsning, informerar vi läsaren om att vi avgränsar oss till banktjänster. Detta var dock inte möjligt då de banker vi kontaktade inte var villiga att ge oss information om säkerheten kring tjänsterna vilket medförde att vi var tvungna att förändra vår avgränsning. Istället fokuserade vi på mobila tjänster som kräver hög säkerhet och intervjuade personer som inte specifikt var knutna till finansiella tjänster men hade stor kunskap inom området.

Ovan nämnda problem innebar även att våra tänkta fallstudier på olika banker fallerade. Vi kontaktade därför ett olika experter inom mobil säkerhet för att få information om ämnet. Vi hade i åtanke innan arbetet att det inte var säkert att bankerna var villiga att svara på alla frågor om deras säkerhetssystem. Dock trodde vi att vi skulle kunna få ut allmän information kring helheten hos tjänsterna.

7.6.2 Surveyundersökningen

Då en miss i kommunikationen med vår webbkonstruktör innebar att vi inte sparade vad varje enskild respondent svarade på fråga 5 kunde vi inte i efterhand få fram vilken person (kön och ålder) som använde en viss typ av tjänster. Vi kunde heller inte koppla ihop fråga 5 med fråga 6 (Hur ofta använder du dessa tjänster?). Detta hade kunnat ge ytterliggare intressanta aspekter kring användningen av mobila Internettjänster.

På grund av bankernas ovilja att svara på våra frågor blev arbetet kraftigt försenat. Detta resulterade i att arbetet med fokusgruppen blev lidande då det ej fanns utrymme för att använda fokusgruppen i alla planerade moment då detta ej inrymdes inom ramen för uppsatsarbetet.

7.7 Förslag till fortsatta studier

Då mobiltelefonutvecklingen går snabbt framåt och mobilerna mer och mer liknar permanenta datorer kan detta vara ett intressant framtida studieämne. Kraftfullare mobiltelefoner

gör det möjligt att använda fler och mer avancerade program. Detta medför även att säkerhetsluckorna blir fler. Hur säkra blir mobiltelefoner i framtiden? Det är även av intresse att studera framtida säkerhetsprogram till mobiltelefoner för att se hur effektiva de blir.

Vidare presenterar vi ett antal frågeställningar som kan vara intressanta att studera vidare i framtiden:

- Hur kan en säkerhetslösning teoretiskt sett se ut som säkrar en specifik mobil Internettjänst optimalt?
- Vilka nya tekniska säkerhetsfunktioner är framtidens lösningar?
- Vilka säkerhetsfunktioner är smidigast för användaren?
- Skall säkerhetsprogramvara ingå vid köp av mobiltelefonen?
- Hur löses uppdateringar för säkerhetsprogramvaran för mobiltelefoner? Prenumeration?
- Hur övertygas allmänheten om att använda finansiella tjänster via sin mobiltelefon? Marknadsföring?

Litteraturförteckning

Andersen, H., (1994). *Vetenskapsteori och metodlära.* Lund: Studentlittertur

Bell, J., (1995). *Introduktion till forskningsmetodik. (2:a upplagan).* Lund: Studentlitteratur

Dillman, D, (1997). *The Role of Behavioral Survey Methodologists in National Statistical Agencies.* Washington State University, Social and Economic Research Center.

Dornan, A, (2001). *The Essential Guide to Wireless Communications.* NJ, Prentice Hall PTR.

Goldkuhl, G. (1998). *Kunskapande.* Jönköping

Gruvö, P. & Rimming, T., (20004). *Säkerhet i mobila nät.* Erhållen från Tomas Rimming, Teleca Sweden East AB

Hardjono, Thomas. (2005). *Security in Wireless LANs and Mans.* Artech House: Norwood.

Hu, W.C., Lee, C-W. & Kou, W. (2005). *Advances in Security and Payment Methods for Mobile Commerce.* Idea Group: Hershey

Lundahl, U. & Skärvad, P-H., (1999). *Utredningsmetodik för samhällsvetare och ekonomer.* Lund: Studentlitteratur

Patel, R. & Davidson, B. (2003). *Forskningsmetodikens grunder: Att planera, genomföra och rapportera en undersökning.* Lund: Studentlitteratur.

Richie, J. & Lewis, J (2003). *Qualitative research practise.* London: SAGE publications

Rubin, Jeffrey (1994). *Handbook of usability testing: how to plan, design and conduct effective tests.* New York: Wiley, cop

Seal, C., Gobo, G., Gubrium, J & Silverman, D. (2004). *Qualitativ Research Practise.* London: SAGE publications

Internetkällor

Aspiro, (2005). *Marknad.* Hämtad 2005-10-24 från http://www.aspiro.com/templates/Page.aspx?id=64

Arvidsson, S., (2006*). Mobiltelefonen blir säkerhetskanal genom trådlös PKI*. Hämtad 2006-04-24 från: http://www.wpki.net/files/WPKI_Historia.pdf

Atea security, (2005). *Kort om virus för mobiltelefoner.* Hämtad 2005-12-06 från http://www.atremo.se/informationscentrum/security-info/sakerhetsartiklar/326.html

Cesam, (2005). Cesam - Stiftelsen Centrum för Samhällsarbete och Mobilisering. *Mötestekniker.* Hämtad 2005-10-11 från http://www.cesam.se/motestekniker_1_10.asp

Computer Sweden, (2005). *Sverige bäst på mobil säkerhet.* Hämtad 2005-10-25 från http://computersweden.idg.se/ArticlePages/200506/17/20050617104610_CS036/20050617104610_CS036.dbp.asp

Ericsson, (2001). Ericsson press releases. *Ericsson in cooperation with Eurocard AB in Sweden to test Bluetoothtm based wireless payment.* Hämtad 2005-10-25 från http://www.ericsson.com/press/archive/2001Q2/20010404-0103.html

ERS. (2005). *ERS – WAP*. Hämtad 2005-12-04 från: http://www.esr.se/WAP/

F-secure, (2005). Hämtad 2005-12-06 från http://www.f-secure.se/

Jarneving, Bo (2005). Bibliotekshögskolan i Borås. *Kvantitativa metoder inom LIS*. Hämtad 2005-10-25 från: www.hb.se/bhs/personal/bojar/bibliometri_%20IR_VETSKP.ppt

Mikal P. (2005). *WTLS – The Good and Bad of WAP Security*. Hämtad 2005-12-04 från: http://wirelessadvisor.net/doc/08980

National Encyklopedin, (2005). *Mobiltelefoni*. Hämtad 2005-10-25 från http://www.ne.se.bibl.proxy.hj.se/jsp/search/article.jsp?i_art_id=257445

Nokia, (2003). Press releases. *Nokia Introduces Dallas to a New Wallet*. Hämtad 2005-10-25 från http://press.nokia.com/PR/200305/903588_5.html

Nordea, (2005). *Mobil*. Hämtad 2005-10-25 från http://www.aspiro.com/templates/Page.aspx?id=64

Onyszko, T. (2005). *Secure Socket Layer*. Hämtad 2005-12-04 från: http://www.windowsecurity.com/articles/Secure_Socket_Layer.html

Stelacon, (2003). *Användningen av mobila tjänster och intresse av 3G och 3G-tjänster på konsument-marknaden*. Hämtad 2005-10-24 från http://www.pts.se/Archive/Documents/SE/Stelacons%20rapport%20om%20anvandningen%20av%20mobila%20tjanster%20och%20intresse%20av%203G%20och%203G-tjanster%20pa%20konsumentmarknaden.pdf

Svenska Bankföreningen, (2004). Press & media. *Rekordmånga använder bank på Internet*. Hämtad 2005-10-25 från http://www.bankforeningen.se/Press%20,-a-,%20Media/Rekordm%C3%A5nga%20anv%C3%A4nder%20bank%20p%C3%A5%20internet%20%E2%80%93%205,2%20miljoner.aspx

Telenormobile. (2005). *GPRS, WAP, Data, SMS & MMS*. Hämtad 2005-12-04 från: https://www.telenormobile.se/foretag/support/gprsWAPmmssms.jsp?id=6

Wapforum (2002). *WAP Wireless Communication*. Hämtad 2005-12-10 från: http://www.protocols.com/pbook/wap.htm

Bilaga 1 – Telefonintervju Anders Larsson

Telefonintervju med Anders Larsson 21 november 2005, WIP Karlskrona

Säkerhetssystem som idag används på Internet kallas SSL och TLS. Det system som WIP idag använder för säkerhet i de mobila applikationer de tillhandahåller är WTLS vilket är en vidareutveckling av TLS. Det är samma krypteringsgrad, 128 bitar, som används för både fast Internet som mobilt. Det som gör att fast Internet kan göras säkrare är att där används koddosor vid exempelvis inloggning till banktjänster. Denna teknik skulle vara möjlig att använda även för mobiltelefoner men anses idag vara för komplex för att den ska implementeras i de mobila lösningarna.

Ett betalningssystem för mobiltrafik som är mycket vanligt idag är att via sms erlägga en likvid. Även mms används för att betala någon form av tjänst. Kunden skickar ett sms eller mms till ett nummer som kostar en viss summa vilket är det som motsvarar avgiften.

Bilaga 2 – Mailintervju Joakim von Braun

Mailintervju med Joakim von Braun 14 April 2006, von Braun Security Consultants

Joakim von Braun specialitet är hotbilder och riskfaktorer och hur dessa kan komma att hota ett företags eller myndighets säkerhet. Gällande mobiler har han betraktat dessa utifrån tre olika aspekter. Dessa är:

1. Fientlig kods utnyttjande av mobila plattformar
2. Åtkomst av konfidentiell information på mobila plattformar
3. Utnyttjande av mobila plattformar för att ta sig vidare in i lokala nätverk

Joakim von Braun besvarade följande frågor:

- **Hur fungerar säkerheten för mobilt Internet - t.ex. WAP?**
  Joakim ansåg sig inte själv ha tillräcklig kunskap för att besvara denna fråga men hänvisade oss till att ta kontakt med Nokia samt SonyEricsson.

- **Var ligger bristerna i mobila lösningar? Var är systemen mest mottagliga för attacker? T.ex. en WAP-gateway**
  Problemen ökar idag i och med att man rör sig bort från proprietära, nedstängda operativsystem över till generella, öppna.

  Med möjligheten att installera script och program ökar riskerna avsevärt. En brist är här att det finns få bra och integrerade säkerhetsverktyg och att man har begränsat med processorkraft och internminne att leka med. Det optimala vore en enda applikation som kan sköta virusskydd, personliga brandvägg, kryptering och behörighetskontroll.

- **Finns det några större skillnader mellan att surfa på mobilen jämfört med att surfa i hemmet via datorn säkerhetsmässigt?**
  Mycket stora. Se ovan avgivna svar + plus att en mobil kan vara både telefon och dator i ett. När den inte utgör en del av det lokala nätverket eller Internet kan vi inte kontrollera den på samma sätt som en vanlig dator. Dels krävs det då ett särskilt kontrollsystem för mobilerna, dels måste man bygga upp ett särskilt system för distribution av säkerhetsprogram och uppdateringar. Det är mycket lättare att greppa de telefoner som alltid har en egen IP-adress och alltid är en del av Internet.

- **Har det funnits några problem med säkerheten för mobilt Internet?**
  Se ovan avgivna svar.

- **Finns det någon specifik hotbild vad gäller mobil säkerhet?**
  Se mitten svar " Problemen ökar idag i...."

- **Tycker du att säkerheten för mobiltelefoner som det är idag är tillräcklig eller krävs det förbättringar?**
  Bl.a. förbättringar i form av ökad processorkraft och internminne som medför att säkerhetsprogrammen kan göras mer avancerade. Nya administrativa program för att kontrollera de mobila plattformarna så att man vet om de har rätt program och är tillräckligt uppdaterade och patchade. Sådana kan ju ha dykt upp som jag missat men det jag sett imponerar inte än så länge.

- **Vet du om några större händelser där mobila system påverkats av attacker?**
  Nej, inte än så länge. Men det finns olika möjligheter som ännu inte utnyttjats. DoS-attacker skulle kunna bli ett hot och jag kan i alla fall se minst två olika scenarier:

  Mängder med SMS eller MMS skickas till en eller ett fåtal mobiler så att minnet blir helt fult och att de blir upptagna att ta emot meddelanden. Detta har hänt i verkligen här i Sverige.

  Särskilt konstruerat SMS som skickas till en mobil men som är skrivet så att den sändande servern inte känner av att SMS:et kommit fram och därför återsänder det igen och igen och igen.

  Detta hände mig två gånger under samma dag vid jultid 2004. Ett SMS dundrade i cirka 2.30 på morgonen och som återsändes till mig minst en gång per sekund. Det var bara att stänga av mobilen och under kontorstid ringa leverantören som då manuellt fick ta bort SMS-meddelande från sin server.

Bilaga 3 – Telefonintervju Svein Willassen

Telefonintervju med Svein Willassen 20 april 2006, Simcon Norge

Det som i stort skiljer mellan mobilt Internet och att använda Internet från en fast anslutning är att signalerna går via en gateway som operatören tillhandahåller. Detta är inte någon dålig lösning säkerhetsmässigt då det är mycket svårt att nå de gateways som distribuerar systemen.

Möjligheterna finns att avlyssna trafiken i luften men detta är mycket svårt vilket inte gör att det utgör något reellt hot mot mobil Internetanvändning.

De problem som finns idag säkerhetsmässigt och som kan utvidgas i framtiden är virus. Dessa virus sprids till största del via bluetooth. Virus skulle även kunna spridas via mobilt Internet användande men detta finns det inga uppgifter om idag att det hänt.

Övriga säkerhetsaspekter som idag kan vara väl så farliga är att mobilen är ett medium användaren bär med sig och använder mer öppet än t.ex. Internetanvändning på en dator. Det kan vara lättare att se vad någon gör och använder för program och tjänster på sin mobil och dessutom rent visuellt se vad för koder som används och var de används.

Det finns nu även nya kreditkortstjänster via mobiltelefoner vilka i stort sett har samma säkerhet som ett kreditkort innehar.

Däremot gällande säkerheten när betalningar via mobiltelefonen eller andra finansiella tjänster och applikationer används är det inte alls speciellt säkert. Möjligheterna att belasta dessa tjänster är stort och enkelt. Exempelvis kan textmeddelande skickas till en mobil utan att mottagaren bett om detta vilka i sin tur kan generera problem.

Det som kan lösa säkerhetsproblemen med mobilt Internet är att mobiltelefonerna mer och mer blir fulländade datorer. Det som då kommer att behövas är samma teknik som på dagens datorer med säkerhetsprogram, brandvägg och antivirusskydd. När detta finns kan säkerheten vara som den idag är då finansiella tjänster utförs från en stationär dator.

Bilaga 4 – Telefonintervju Stefan Axelsson

Telefonintervju Stefan Axelsson, System Manager Ericsson AB, Sverige 2 maj 2006

En öppen intervju hölls med Stefan Axelsson den 2 maj. Stefan pratade runt säkerhetsaspekterna om mobila applikationer.

Den stora skillnaden idag är plattformssäkerheten. Men egentligen är mobilen mer sårbar eftersom den sänder radiovågor som hypotetiskt sett kan fångas upp av någon obehörig. Men där är vi inte idag någon sådan hotbild finns inte. En utrustning för att klara av att ta emot signaler och avkoda dem ligger kostnadsmässigt på runt 1 miljon och det springer inte någon vanlig ”Svensson” runt med.

Framtida bekymmer kan bli virus vilket alla just nu egentligen sitter å väntar på att det ska komma ett första virus. Än har inget större virus uppträtt. Det som kommit är riktade maskar som riktas mot en användare, känner igen om denne är kund på exempelvis en specifik bank och laddar då ner lösenordet då det används.

Även Phising förekommer och detta är helt plattformsoberoende.

Kritiskt mot 3G vissa tidigare säkerhetsbrister är åtgärdade men samtidigt var GSM säkrare sett till helheten. En storsvaghet som GSM har är att systemet inte autentiserar sig själv det är bara användaren som autentiserar sig in vilket gör att det är lätt att sätta upp en egen basstation. Samtidigt är all trafik och överföring tunnlad vilket gör att det är mycket svårt att komma åt paket och om man gör det är det extremt svårt att få ut dem därifrån.

Större brister är WLAN där utvecklarna helt glömde att speca krypton.

Inget större tryck från någon att bedriva brottslighet mot användarna av banktjänster de går oftast mot själva banken eller andra delar där det finns info om många kunder på en gång. Brottsligheten riktas mot där de kan göra stora pengar genom en överträdelse.

Saker går aldrig att få helt säkra det är alltid en fråga om hur mycket pengar ett företag vill lägga kontra säkerhetsnivån. I USA finns ett mycket större svinn än i Europa eftersom företagen där accepterar visst intrång så länge helheten inte påverkas nämnvärt vilket den ofta inte gör.

Anser att säkerheten är högre på telefonen än vid datorn hemma. Eftersom telefonen har bredare utbud av plattformar som bortsett från Microsoft produkterna håller en högre standard säkerhetsmässigt är det svårare att komma åt något där.

Det finns fler riktiga plattformar från början eftersom UNIX och Linux ändvänds i högre grad och dessa inte är lika intressanta att angripa.

Det gäller att inte den mobila utvecklingen av plattformar hamnar i samma monokultur som Microsoft har gällande ordinära plattformar. Det är en mycket farlig kultur sett säkerhetsmässigt.

Bilaga 5 – Pappersversion surveyundersökning

Enkät Mobila Tjänster Och Dess Förtroende

En enkätundersökning rörande allmänhetens användande och förtroende för mobila tjänster

Besvara varje fråga genom att kryssa i det alternativ som du tycker överstämmer bäst med frågan	Kön?	Ålder?		
	Man ☐	**10-19**	☐	**20-29** ☐
	Kvinna ☐	**30-39**	☐	**40-49** ☐
		50-59	☐	**60+** ☐

Har du en mobiltelefon med åtkomst till Internet? *(WAP…..)*

Ja ☐

Nej ☐

Använder du denna möjlighet till åtkomst av Internet?

Ja ☐

Nej ☐

Om ja vad använder du?

Nyheter	**Betaltjänster**	**Banktjänster**	**Underhållning**	**Biljetter**	**Bokningar**
☐	☐	☐	☐	☐	☐

Hur ofta använder du dessa tjänster?

Dagligen	**3 dagar i veckan eller mer**	**1 dag i veckan eller mer**	**Mer sällan**
☐	☐	☐	☐

Vilka tjänster skulle du vilja använda?

Nyheter	**Betaltjänster**	**Banktjänster**	**Underhållning**	**Biljetter**	**Bokningar**
☐	☐	☐	☐	☐	☐

Skulle du kunna tänka dig att betala över Internet med mobiltelefonen?

Ja ☐

Nej ☐

Skulle du kunna tänka dig att sköta dina finansiella affärer via mobiltelefonen? *(Såsom bankärenden, aktiehandel, köp av varor m.fl.)*

Ja ☐ **Nej** ☐

Anser du att det är lika säkert att surfa i mobilen som via datorn i hemmet?

Ja ☐

Nej ☐

Känner du förtroende för säkerheten vid användandet av en finansiell tjänst via datorn i hemmet? *(Såsom överföringar av pengar, betala räkningar o andra banktjänster)*

Ja ☐ **Nej** ☐

Känner du förtroende för säkerheten vid användandet av en finansiell tjänst i din mobiltelefon? *(Såsom överföringar av pengar, betala räkningar osv.)*

Ja ☐ **Nej** ☐

Tror du att säkerheten ligger på samma nivå vad gäller mobilt Internet och via datorn i hemmet?

Ja ☐

Nej ☐

Tack för att du har besvarat enkäten och därmed hjälpt oss i vårt magisteruppsatsarbete.

Linus, Mattias

Bilaga 6 – Välkomstsida surveyundersökning

Hej,

Vi är två studenter vid Internationella Handelshögskolan i Jönköping som nu skriver vår magisteruppsats. Temat för uppsatsen rör användarnas säkerhetsförtroende kring mobiltelefonen och dess tjänster.

Vi önskar nu Er hjälp gällande en undersökning vi ämnar genomföra hos mobiltelefonanvändare. Målet med undersökning är att få svar på vilka mobila tjänster som generellt används och förtroendet kring säkerheten för mobila tjänster.

Undersökningen genomförs i form av en enkät som finns på nästkommande sida och tar max ett par minuter att genomföra. Vi hoppas att Ni är villiga att ge oss denna hjälp!

Tack på förhand!

Mvh
Linus Andersson
Mattias Johansson

Till undersökningen

Bilaga 7 – Surveyundersökning

Kön?

☐ Man | ☐ Kvinna

Ålder?

☐ 10 - 19 | ☐ 20 - 29 | ☐ 30 - 39

☐ 40 - 49 | ☐ 50 - 59 | ☐ 60+

Har du en mobiltelefon med åtkomst till Internet? (WAP)

☐ Ja | ☐ Nej

Använder du denna möjlighet till åtkomst av Internet?

☐ Ja | ☐ Nej

Om ja, vad använder du? (Du kan välja mer än ett alternativ)

Nyheter	Betaltjänster	Banktjänster	Underhållning	Biljetter	Bokningar	Annat
☐	☐	☐	☐	☐	☐	☐

Hur ofta använder du dessa tjänster?

☐ Dagligen

☐ 3 dagar i veckan eller mer

☐ 1 dag i veckan eller mer

☐ Mer sällan

Vilka tjänster skulle du vilja använda? (Du kan välja mer än ett alternativ)

Nyheter	Betaltjänster	Banktjänster	Underhållning	Biljetter	Bokningar	Annat
☐	☐	☐	☐	☐	☐	☐

Skulle du kunna tänka dig att betala över Internet med mobiltelefonen?

☐ Ja | ☐ Nej

Skulle du kunna tänka dig att sköta dina finansiella affärer via mobiltelefonen? *(Såsom bankärenden, aktiehandel, köp av varor etc.)*

☐ Ja | ☐ Nej

Anser du att det är lika säkert att surfa via mobilen som via datorn i hemmet?

☐ Ja | ☐ Nej

Känner du förtroende för säkerheten vid användandet av en finansiell tjänst via datorn i hemmet? *(Såsom överföringar av pengar, betala räkningar och andra banktjänster)*

☐ Ja | ☐ Nej

Känner du förtroende för säkerheten vid användandet av en finansiell tjänst i din mobiltelefon? *(Såsom överföringar av pengar, betala räkningar och andra banktjänster)*

☐ Ja | ☐ Nej

Svara

Bilaga 8 – WPKI projektet

WPKI-föreningen är en sammanslutning av olika företag vars syfte är att möjliggöra en väl fungerande infrastruktur för mobila e-legitimationer.

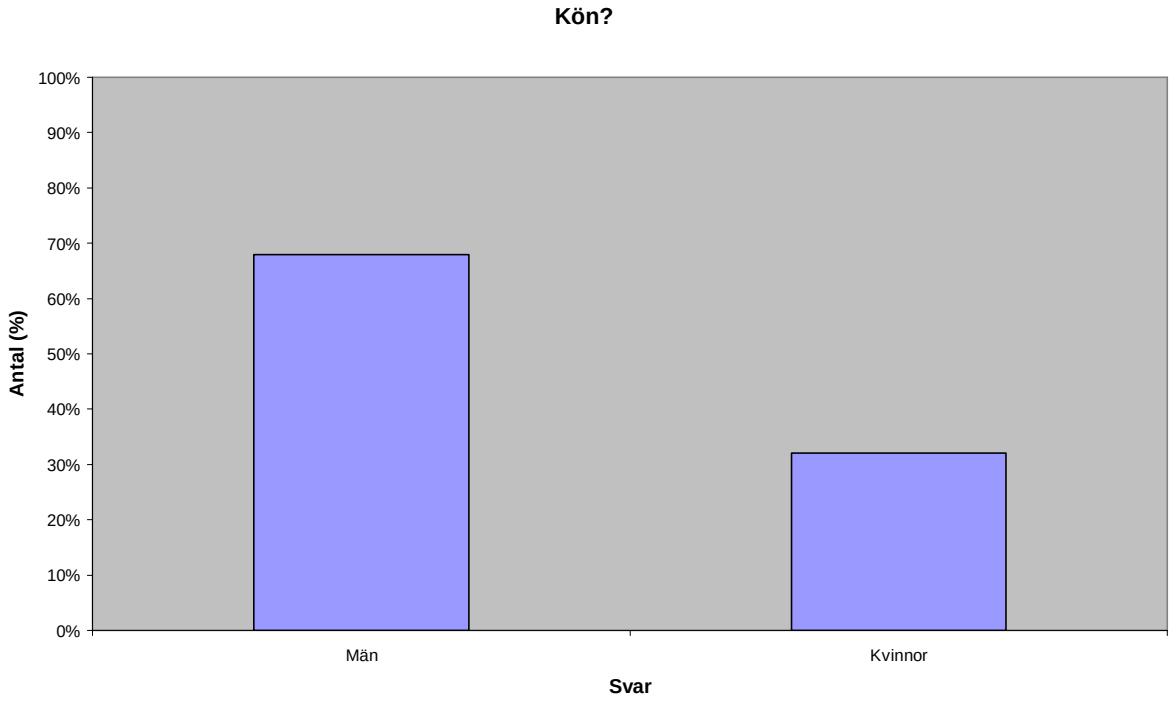
Föreningen arbetar mot att förvalta och vidareutveckla ett antal tekniska och administrativa specifikationer som:

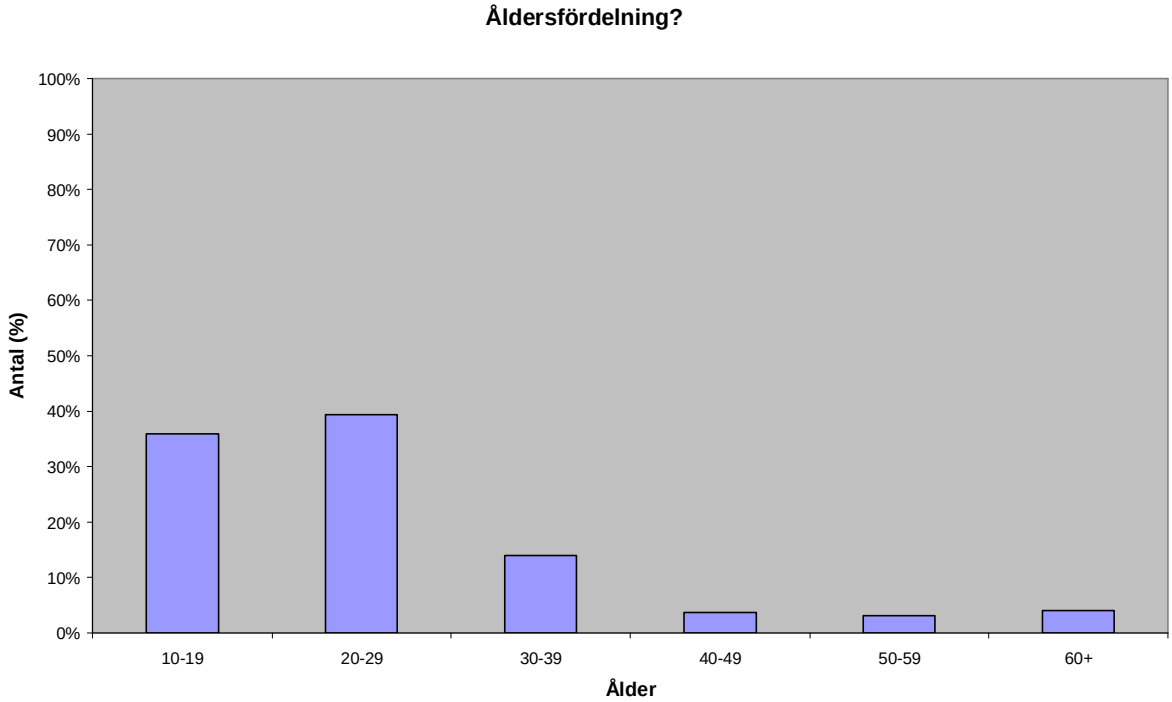
- Anger hur SIM-kort i mobiltelefoner ska vara utformade för att kunna inhysa den mobila e-legitimationen
- Specificerar gränssnitten mellan de inblandade aktörerna:
  Mobiloperatör, e-legitimationsutgivare (RA/CA), och förlitande part
- Beskriver de åtaganden som finns emellan ovan nämnda aktörer

WKPI-föreningen strävar mot att skapa en globalt accepterad specifikation av WPKI genom att:

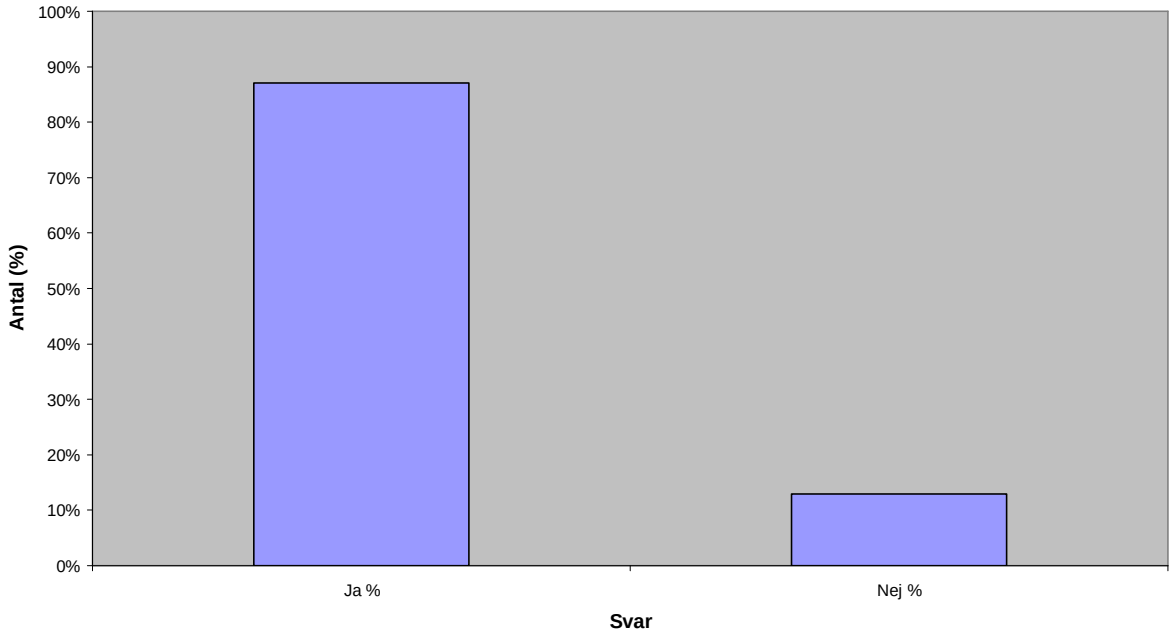
- Publicera de tekniska och administrativa specifikationerna
- Säkerhetsställa att de tekniska specifikationerna för WPKI baserar sig på globalt accepterade standarder
- Genom de medlemmar som är aktiva i standardiseringsorganisationer lämna in bidrag i linje med specifikationerna

Bilaga 9 – Resultat Surveyundersökning

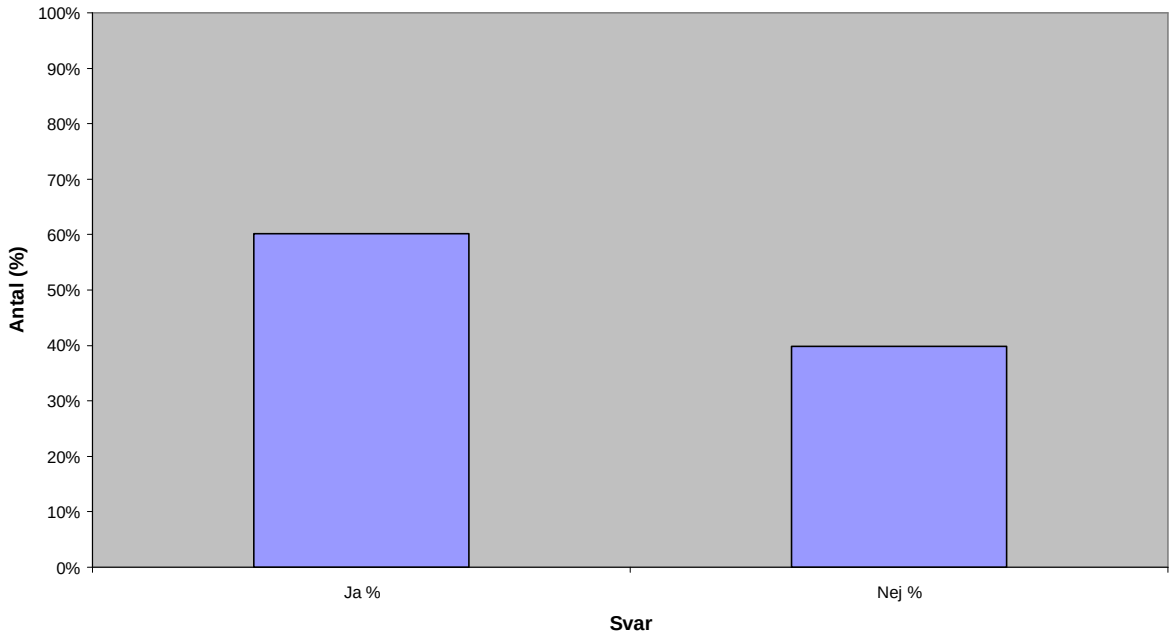




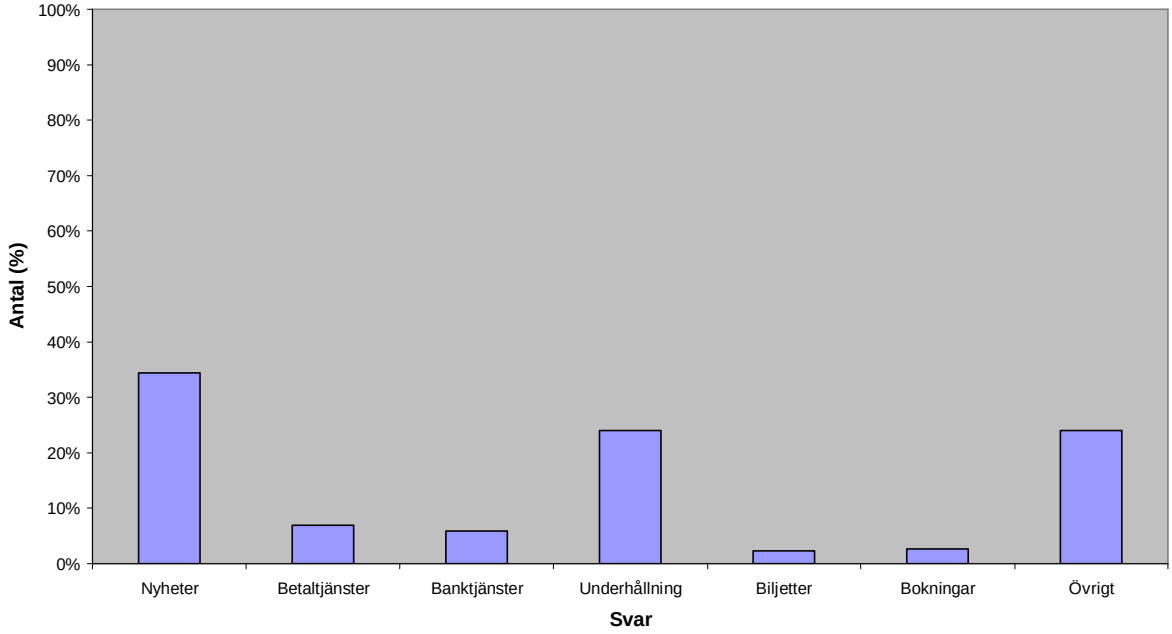
Har du en mobiltelefon med åtkomst till wap?



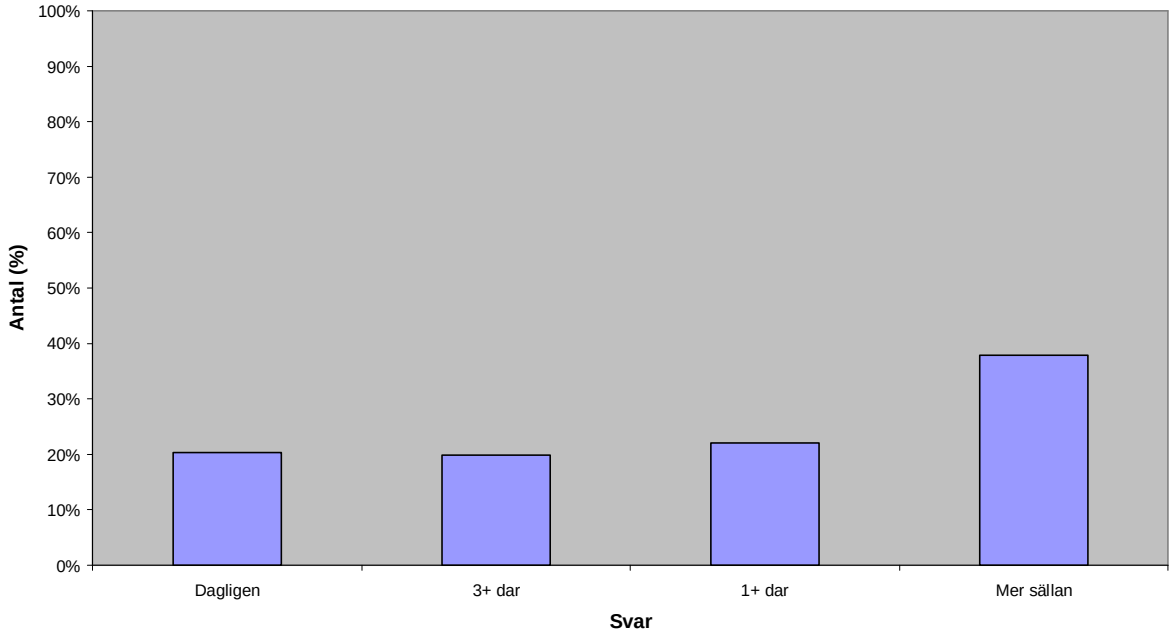
Använder du denna möjlighet till åtkomst av Internet?



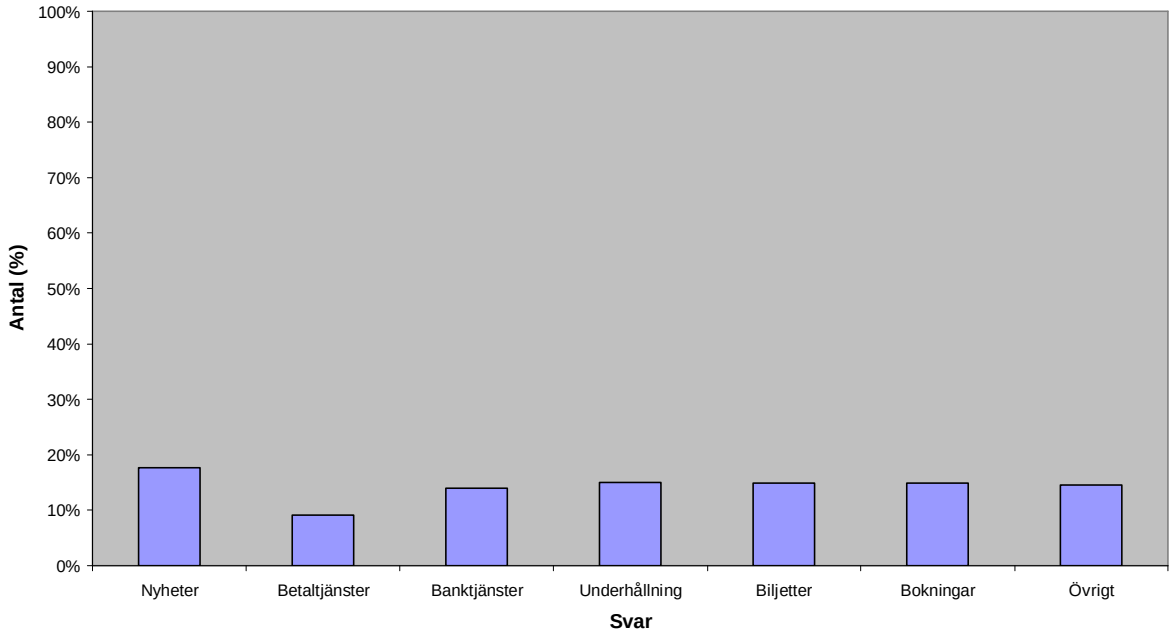
Om ja vad använder du?



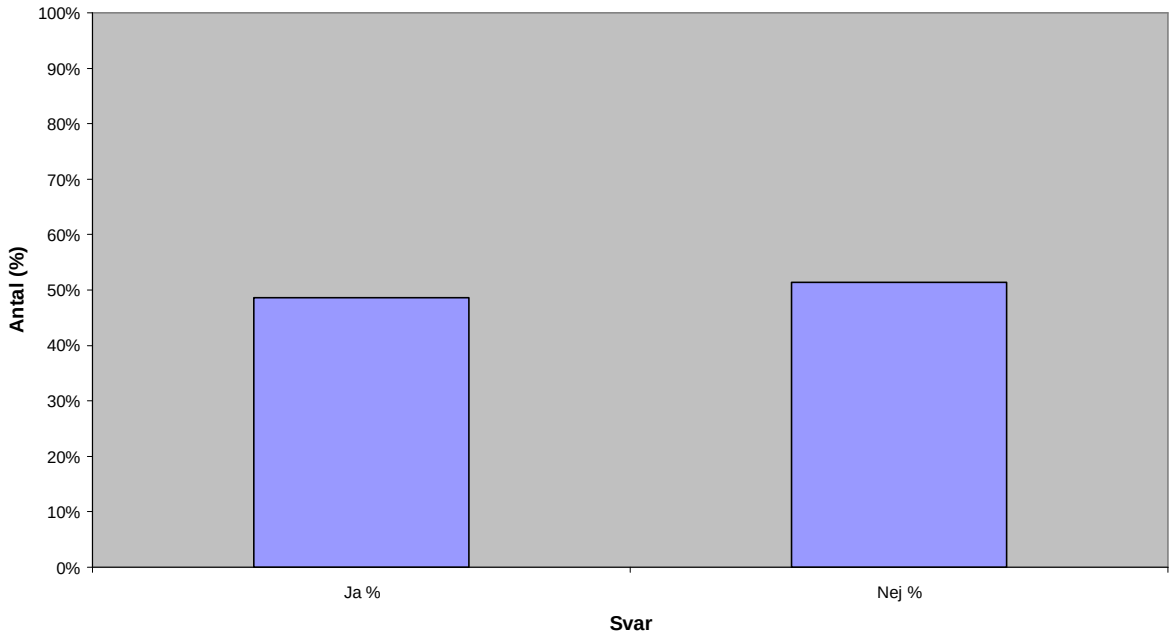
Hur ofta använder du dessa tjänster?



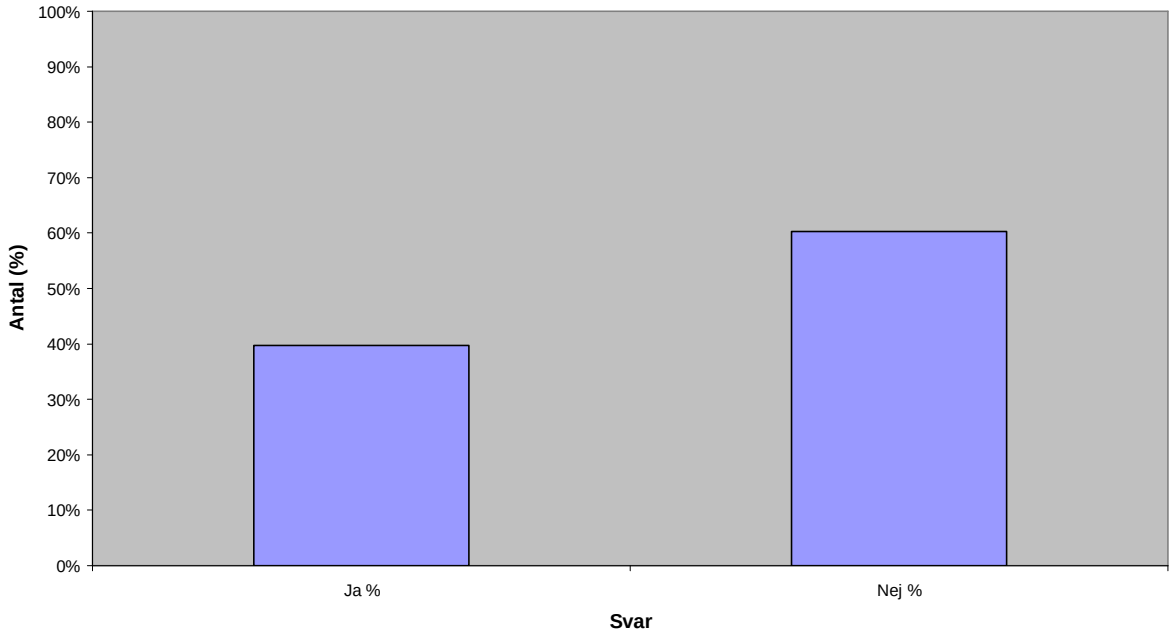
Vilka tjänster skulle du vilja använda?



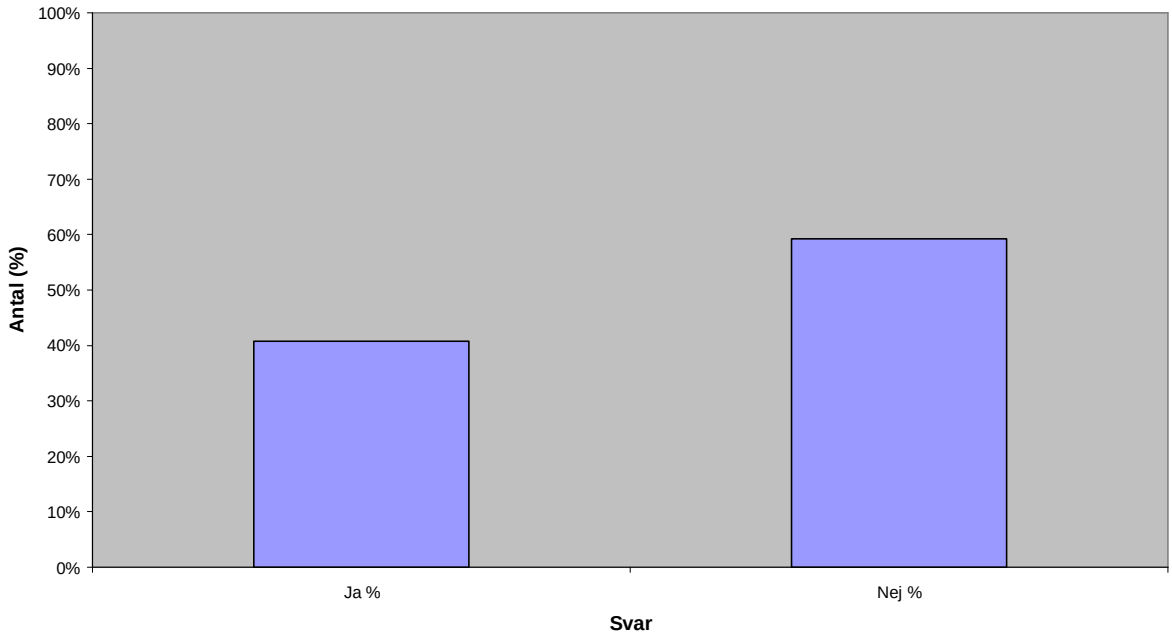
Skulle du kunna tänka dig att betala över Internet med mobiltelefonen?



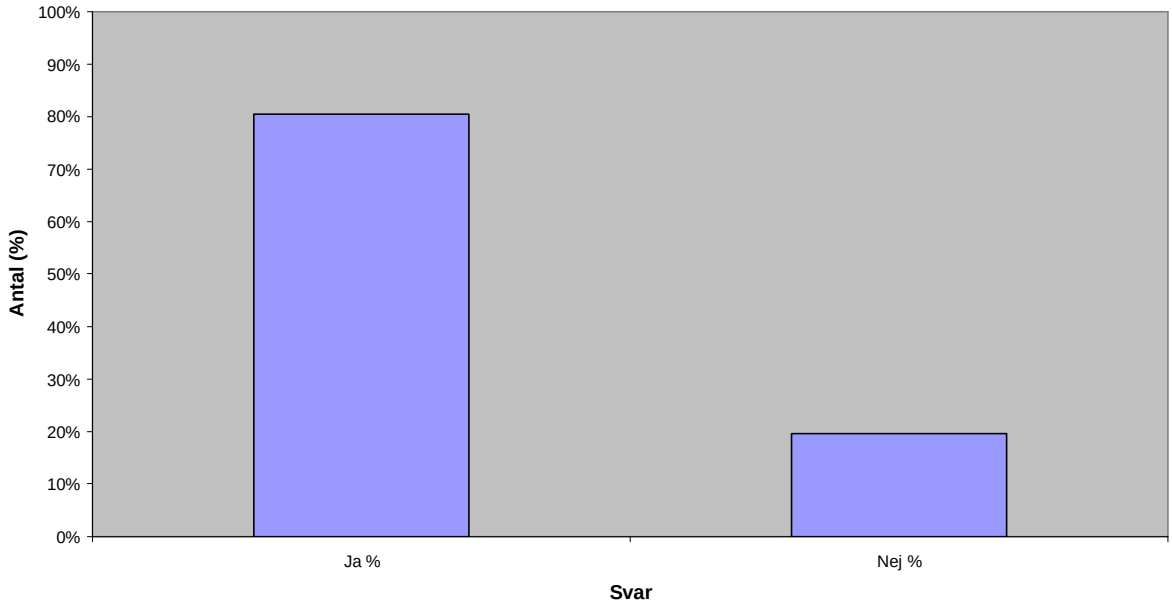
Skulle du kunna tänka dig att sköta dina finansiella affärer via mobiltelefonen?



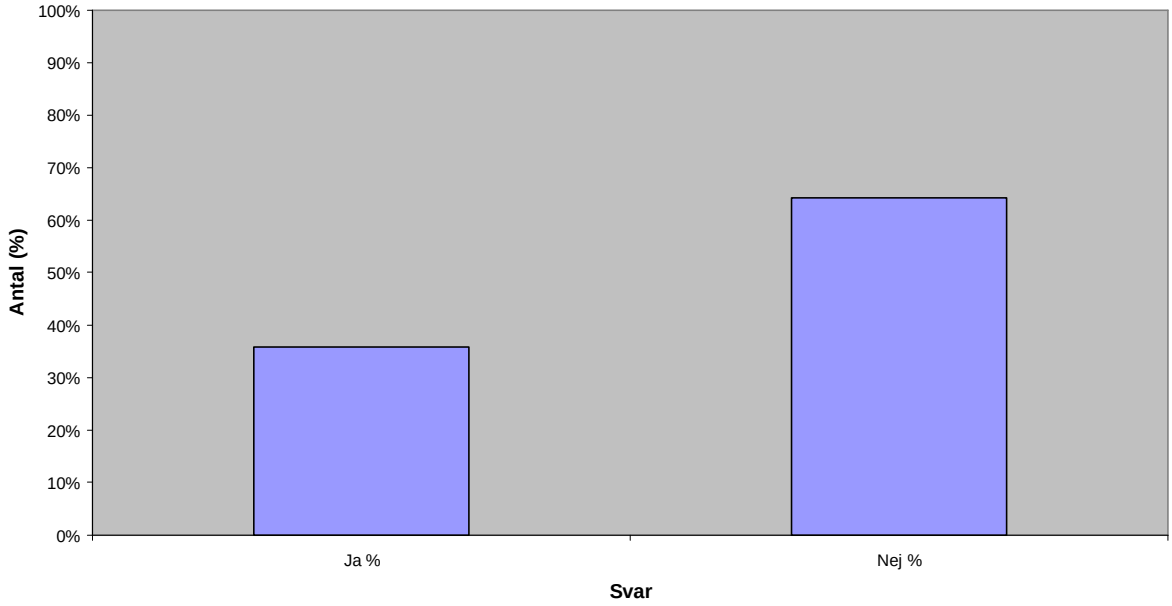
Anser du att det är lika säkert att surfa i mobilen som via datorn i hemmet?



Känner du förtroende för säkerheten vid användandet av en finansiell tjänst via datorn i hemmet?



Känner du förtroende för säkerheten vid användandet av edn finansiell tjänst i din mobiltelefon?



Bilaga 10 – Adresser till undersökningens forum

Internetadress	Tema
www.Internetstart.se -	Internet
www.pricerunner.se -	Konsumentrådgivning
www.brollopstorget.se -	Bröllop
www.fuska.se -	Spel
www.passagen.se -	Blandat
www.fz.se -	Datorer
www.64bits.se -	Datorer
www.itforum.se -	IT
www.wlan-forum.se -	WLAN
www.puls.se -	Träning
www.grafisktforum.se -	Grafik
www.sweclockers.com -	Datorer
www.webforum.nu -	Datorer
www.aftonbladet.se -	Nyheter
utbytet.skolutveckling.se -	Skola
www.hype.se -	Spel
www.idg.se -	IT-nyheter
www.monster.se -	Jobbsökande
www.99mac.com -	Macintosh
www.sportgamers.se -	Sportspel
www.datormagazin,se -	Datorer
www.sporthoj.se -	Motorcyklar
www.pokerforum.nu -	Poker
www.bendro.se -	Vikt & hälsa
www.ss.se -	Svenska Spårvagnssällskapet
www.voodoofilm.org -	Film

Bilaga 11 – Fokusgrupp

Fokusgruppsmöte 2005-12-06

Mötets mål var att diskutera fram frågor till vår surveyundersökning. Gruppen bestod av 6 personer i vår omgivning utöver oss själva.

Mötet inleddes med att vi som mötesledare presenterade mötets mål och innebörden av en fokusgrupp. Därefter fick deltagarna fritt diskutera möjliga frågor, med utgångspunkt från de två huvudfrågorna i vår uppsats, som de ansåg värda att ställa i en surveyundersökning vars mål var att få fram information om vad mobilanvändare anser om säkerheten kring WAP-tjänster.

Nedan följer informationen som mötet resulterade i:

Första delen av undersökningen skulle bestå av information om respondenten. Detta för att få lite vetskap om vilka det är som svarat på surveyundersökningen. Dessa frågor var:

Kön?

Ålder?

Nästa del bestod i att få vetskap om respondenten har WAP och i så fall använder det. Frågor

gällande vad för tjänster respondenten använde var också av intresse. Dessa frågor var:

Har du en mobiltelefon med åtkomst till Internet? (WAP)

Använder du denna möjlighet till åtkomst av Internet?

Om ja vad använder du?

Alternativ:
Nyheter Betaltjänster Banktjänster Underhållning Biljetter Bokningar

Hur ofta använder du dessa tjänster?

Alternativ:
Dagligen 3 dagar i veckan eller mer 1 dag i veckan eller mer Mer sällan

Tredje delen av surveyundersökningen var att få fram information om vilka olika tjänster respondenten skulle vilja använda. Dessa frågor var:

Vilka tjänster skulle du vilja använda?

Alternativ:
Nyheter Betaltjänster Banktjänster Underhållning Biljetter Bokningar

Skulle du kunna tänka dig att betala över Internet med mobiltelefonen?

Skulle du kunna tänka dig att sköta dina finansiella affärer via mobiltelefonen? (Såsom bankärenden, aktiehandel, köp av varor m.fl.?)

Sista delens syfte var att få fram vad användarna anser om säkerheten gällande dessa tjänster kontra när dessa tjänster används genom datorn i hemmet. Dessa frågor var:

Anser du att det är lika säkert att surfa i mobilen som via datorn i hemmet?

Känner du förtroende för säkerheten vid användandet av en finansiell tjänst via datorn i hemmet? (Såsom överföring av pengar, betala räkningar o andra banktjänster)

Känner du förtroende för säkerheten vid användandet av en finansiell tjänst i din mobiltelefon? (Såsom överföring av pengar, betala räkningar o andra banktjänster)

Tror du att säkerheten ligger på samma nivå vad gäller mobilt Internet och via datorn i hemmet?

Bilaga 12 – Pilottest

Efter att vi genomfört fokusgrupp mötet tog vi fram en pappersvariant av undersökningen vi planerade att ha Internetbaserad. Detta för att ha möjlighet att innan vi konstruerade enkäten på webben kunna enkelt genomföra ett pilottest för att se om de frågor vi tagit fram förstods och besvarades rätt av gemene man.

Pilottestet genomfördes på 20 slumpvisutvalda personer i vår omgivning från båda könen i åldrarna 15-60 år.

Från de svar och diskussioner pilottestet genererade beslöt vi att ta bort frågan ”Tror du att säkerheten ligger på samma nivå vad gäller mobilt Internet och via datorn i hemmet?” eftersom den i stort svarar på samma sak som frågan ”Anser du att det är lika säkert att surfa i mobilen som via datorn i hemmet?”. Vi lade även till texten ”du kan välja mer än ett alternativ” på de frågor vi förväntade att respondenterna skulle markera mer än ett alternativ då detta inte var självklart i pilottestet.

Bilaga 13 – Ordlista

256-bit kryptering (24) – Hör till AES (Advanced Encryption Standard) som är en standardiserad krypteringsalgoritm.

3G (8) – Tredje generationens mobila nät vars teknik möjliggör bandbredd upp till 2 Mbit/s.

Applikation (11) – Ett dataprogram som hjälper användaren att utföra en viss tillämpning, t.ex. ordbehandling, kalkylering, bokföring och bildbehandling.

Asymmetrisk kryptering (29) – En publik nyckel används vid kryptering medan en privat nyckel används vid dekryptering.

Autentisera (25) – En kontroll av uppgiven identitet vid exempelvis kommunikation mellan två system eller vid utväxling av meddelande mellan olika användare.

Bluetooth (30) – En trådlös kortdistanskommunikation som använder radioteknik för att kommunicera mellan mobiltelefoner, datorer, skrivare, kameror m.fl.

Brandvägg (42) – En mjukvaru- eller hårdvarulösning som agerar hinder mot oönskad kommunikation mellan olika datornät, främst mot intrång.

CA-certifikat (31) – Ett digitalt certifikat som är certifierat av en oberoende certifieringsorganisation (Certification Authoriy).

Digitala certifikat (28) – Ett dokument som innehåller information om vad som är certifierat, t.ex. en epostadress, en krypteringsnyckel för samma epostadress samt en krypterad signatur av informationen.

Digitala signaturer (23) – En kod som följer med ett elektroniskt meddelande och på så sätt identifierar avsändaren.

DoS-attacker (23) - DoS uttyds Denial-of-Service, är en form av datasabotage som på svenska ofta kallas för överbelastningsattack. Ett exempel är när en mailserver bombarderas med epost vilket kan medföra överbelastning. .

Elektroniska signaturer (23) – Se Digitala Signaturer

Phishing (41) – En metod riktad mot Internetanvändare som luras att lämna ut känslig information vilket ofta används i syfte för bedrägeri.

Flyttbara lagringsmedia (30) – En enhet som kan lagra datainformation t.ex. portabla hårddiskar, laptop, mobiltelefon.

Gateway (27) - En sorts nätsluss som skickar trafik mellan olika typer av datornät.

GPRS (30) – (General Packet Radio System) En uppgradering av 2G-nätet som ofta kallas 2.5G. Denna förbättring medförde ökad bandbredd och fokuserar på ett mobilt Internet.

GSM (30) – (Global Service for Mobile Transmission) Det europeiska mobiltelefonsystemet.

HTML (25) – (HyperText Markup Language) Är ett märkspråk och en standard för strukturering av text, hypertext, media och inbyggda objekt i exempelvis webbsidor och i e-brev.

https (28) - Ett protokoll för krypterad transport av data.

LINUX (52) - Ett fritt operativsystem vilket härstammar från UNIX.

m-commerce (23) – (Mobile commerce) En tjänst som kan användas med hjälp av en mobiltelefon, exempel banktjänster.

Mobila plattformar (42) – Ett operativsystem för en mobiltelefon.

Öppna plattformar (41) – Ett operativsystem som kan köras oberoende av hårdvaran.

Pda (24) – (Personal Digital Assistant). En handdator som ryms i en ficka.

PKI (30) – (Public Key infrastructure). Standard för att hantera publika krypteringsnycklar.

RSA-algoritm (28) - En asymmetrisk krypteringsalgoritm.

Scriptspråk (27) - Ett programmeringsspråk, t.ex. java.

SMS (8) – (Short Message Service) Är en tjänst för korta textmeddelanden som sänds till och från mobiltelefon.

SSL-tekniken (27) – (Secure Socket Layer) Är en standard för kryptering av bland annat webbtrafik.

Symmetrisk kryptering (29) - Använder samma nyckel för att både kryptera och dekryptera.

TCP/IP (27) - TCP/IP är en arkitektur för datakommunikation över nätverk.

UMTS (8) – (Universal Mobile Telecommunications System) En 3G-standard som bland annat används i Sverige.

UNIX (52) - En grupp operativsystem.

URL-adress (40) – (Uniform Resource Locator) Benämningen för en webbadress som till exempel http://www.ihh.hj.se

VPN-tunnel (40) – (Virtual Private Network) En teknik som gör det möjligt att sammankoppla olika nätverk samt enskilda enheter på ett säkert sätt. T.ex. säkrar trafiken mellan en distansarbetare och företagets nät.

WAP (25) – (Wireless Application Protocol) Kommunikationsprotokoll som ger åtkomst till Internet från en mobiltelefon.

WML (26) – (Wireless Markup Language) Ett XML-språk som används vid skapandet av WAP-sidor för mobiltelefoner.

Källanvisningar

Svenska Språknämnden, (2006). Svenska Datatermgruppen. Hämtad 2006-05-15 från http://www.nada.kth.se/dataterm

National Encyklopedin, (2006). *Mobiltelefoni.* Hämtad 2006-05-16 från http://www.ne.se.bibl.proxy.hj.se/jsp/search/article.jsp?i_art_id=257445