NORGES HANDELSHØYSKOLE
Bergen, Vår 2018

# Mobilbetaling

*Holdninger til sikkerhet og bekvemmelighet blant norske millennials*

**Mathilde Plo-Sørensen og Margrethe Shields Rasmussen**

**Veileder: Jon Iden**

Masterutredning i Økonomisk Styring og Strategi og Ledelse

NORGES HANDELSHØYSKOLE

# Sammendrag

Det norske markedet for digitale mobilbetalingsløsninger har hittil vært begrenset til hovedsakelig vennebetalinger. Endringer i lovverk og nytt datadirektiv legger nå til rette for at tredjepartsaktører kan tre inn i markedet for mobilbetaling som tidligere har vært forbeholdt banker. Mobilbetaling i butikk har så langt ikke vært tilbudt norske forbrukere i særlig stor grad, men medieoppslag tilsier at dette nå blir en realitet. Vipps er blant aktørene som har sagt at de snart vil tilby kundene sine mobilbetaling i butikk, men at dagens løsninger ikke er bekvemmelig nok for norske forbrukere. Med utgangspunkt i eksisterende teori og egen datainnsamling studerer vi hvilke holdninger norske millennials har til henholdsvis sikkerhet og bekvemmelighet i mobilbetalingsapplikasjoner. Med utgangspunkt i uttalelser fra fagfolk og i medieoppslag var vår antakelse da vi startet arbeidet at forbrukernes holdninger til bekvemmelighet var av større betydning enn deres holdninger til sikkerhet.

Gjennom arbeidet har vi gjennomført to fokusgrupper med representanter fra milleniumsgenerasjonen. Denne datainnsamlingen ble utført for å skape klare definisjoner rundt begrepene sikkerhet og bekvemmelighet i mobilbetalingsapplikasjoner. Dette var en del av forarbeidet til et større spørreskjema, hvor respondentene besto av studenter fra Norges Handelshøyskole og Handelshøyskolen BI Campus Bergen. Spørreskjemaets hensikt var å gi deskriptive, statistiske data som målte respondentenes holdninger til sikkerhet og bekvemmelighet i mobiletalingsapplikasjoner. Denne datainnsamlingen har avdekket funn som både bekrefter og avkrefter en rekke antakelser som er presentert i oppgaven. Utredningen har funnet at millennial-forbrukeren verdsetter sikkerhet og bekvemmelighet høyt. Kanskje ikke overraskende er bekvemmelighet det viktigste for millennial-forbrukeren, men vi ser også at sikkerhet er en prioritet. Det viktigste hva angår sikkerhet er dog de sikkerhetsmekanismer som tilbys forbrukeren fra det offentlige og fra tjenestetilbyderene. Sikkerhetstiltak som påvirker forbrukerens bekvemmelighet, eksempelvis oppdateringer og variasjon av passord, nedprioriteres av millennial-forbrukeren. Dette legger visse føringer for tilbyderne, ettersom de må investere i sikre og enkle løsninger for å kunne tiltrekke og beholde brukere innenfor denne generasjonen. Studiet vårt bidrar derfor med innsikt på de akademiske områdene som omhandler forbrukerholdninger til sikkerhet og bekvemmelighet i mobilbetalingsapplikasjoner, samt at det kan gi innsikt for kommersielle aktører som ønsker å entre markedet for mobilbetaling i butikk.

# Forord

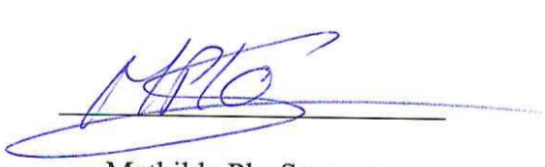
Denne utredningen er det avsluttende arbeidet i vår mastergrad i økonomi og administrasjon ved Norges Handelshøyskole. Oppgaven er skrevet innenfor henholdsvis hovedprofilene Økonomisk Styring og Strategi og Ledelse og tilsvarer 30 studiepoeng. Arbeidet ble påbegynt desember 2017 og avsluttet i juni 2018. Det har vært en lærerik prosess hvor vi har skrevet om et tema som har vært av høy aktualitet, og hvor endringer i markedet har oppstått underveis. Gjennom arbeidet har vi tilegnet oss dybdekunnskap om teoretiske emner og om et hittil ukjent marked i Norge.

Vi ønsker å rette en stor takk til vår dyktige veileder, professor Jon Iden, som fra start til slutt har motivert, støttet og bidratt med sin faglige kompetanse. Idens entusiasme og interesse for oppgavens tema har ført til mange gode diskusjoner som har styrt oss i riktig retning.

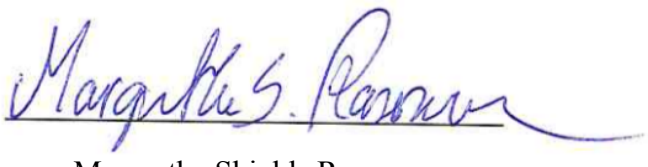
Videre vil vi takke deltakerne som bidro i fokusgruppene for sine gode innspill og meninger. Alle deltakerne er lovet anonymitet, men vi setter stor pris på at de tok seg tid i en travel hverdag til å tilføre utredningen den informasjonen vi hadde behov for.

God lesning!

Norges Handelshøyskole
Bergen, 8. juni 2018



Mathilde Plo-Sørensen



Margrethe Shields Rasmussen

# INNHOLDSFORTEGNELSE

# 1.0 Introduksjon

Det norske betalingsmarkedet karakteriseres i hovedsak av korttransaksjoner. Likevel har det de siste årene vært en fremvekst av nye, kortløse betalingstjenester som Vipps, mCash og MobilePay. Sistnevnte muliggjorde mobilbetaling i fysiske butikker, men tjenesten ble trukket fra det norske markedet på grunn av lav adopsjon blant norske forbrukere (Hoemsnes og Trumpy, 2017).

Utviklingen fra tradisjonelle banktjenester til mobile løsninger har de siste årene vært sterk, men antas å bli enda sterkere i årene som kommer. Nelly S. Maske (2017, s. 16) beskriver i SpareBank1 SMNs årsrapport for 2016 at utviklingen i banknæringen stadig går raskere og påpeker at bankenes utvikling må baseres på et samarbeid med potensielle partnere. Dette utsagnet støttes av Øyvind Aass (Stefanovic og Ribe, 2017, s. 55) som mener at "*Kunsten er å gjøre disse* [teknologiaktørene] *til samarbeidspartnere og ikke konkurrenter."* I april 2018 tillot Konkurransetilsynet en fusjon mellom Vipps, BankID og BankAxept, med forbehold om at de ga konkurrerende aktører tilgang til BankID og BankAxept (Seljehaug, 2018). Med nytt EU-direktiv, PSD2, som er forventet å tre i kraft i 2018, åpnes det for en endring av konkurransesituasjonen i betalingstjenestemarkedet som hittil har vært monopolisert av finansielle institusjoner. Tredjepartsaktørene kan basere sine løsninger på lettvekts-IT som mobilapplikasjoner og bygge sine tjenester på toppen av bankenes tyngre infrastruktur (Finans Norge, u.å).

Med de nye mulighetene i betalingstjenestemarkedet vil flere aktører kunne tilby mobilbetaling i butikk til norske forbrukere. Selv om dagens marked i stor grad baserest på korttransaksjoner er det, med tanke på den store utbredelsen til Vipps, naturlig å anta at mobilbetaling i butikk vil bli godt mottatt av norske forbrukere. Den yngre generasjonen, *millennials,* har levd et liv hvor bruken av digitale tjenester har vært tilnærmet en selvfølge. Det kan derfor igjen antas at denne forbrukergruppen vil være først ute med å adoptere denne typen tjenester. Forbrukere kan ha asymmetriske behov når de skal ta i en bruk en mobilbetalingstjeneste. Mobilapplikasjoners livssyklus kan bli relativt kort dersom de ikke tilfredsstiller forbrukernes krav og behov. Litteraturen viser at det i digitale tjenester ofte er et forbrukerfokus på sikkerhet, i tillegg til at forbrukerne har forventninger om at slike tjenester skal være tids- og innsatsbesparende. I forbindelse med forbrukerperspektivet hva angår mobilbetalingsapplikasjoner, er det følgelig to hovedaspekter som vi mener bør

undersøkes nærmere: sikkerhet og bekvemmelighet. Vår initielle antakelse var at millennialforbrukere anser bekvemmelighet som viktigere enn sikkerhet i mobilbetalingsapplikasjoner. Denne utredningens hensikt er derfor å undersøke følgende problemstilling:

*Hvilke holdninger har norske millennials til sikkerhet og bekvemmelighet i mobilbetalingsapplikasjoner?*

For å besvare denne problemstillingen valgte vi først å gjennomføre to fokusgrupper. Dette ble gjort fordi vi, basert på litteratursøket, ikke fant tilstrekkelig gode begreper for bekvemmelighet i mobilbetalingsapplikasjoner og for sikkerhet sett fra et millennial-forbrukerperspektiv. Deretter utviklet vi og sendte et spørreskjema til et utvalg millennials hvor vi samlet data om deres holdninger til sikkerhet og bekvemmelighet i mobilbetalingsapplikasjoner. For å styrke kvaliteten i spørreskjemaet var påstandene basert på utsagn fra fokusgruppene i tillegg til den eksisterende litteraturen.

Målet med denne utredningen er å styrke forskningen innenfor sikkerhet og bekvemmelighet i mobilbetaling. Et annet mål er å øke forståelsen for millenniumgenerasjonens holdninger til sikkerhet og bekvemmelighet i digitale betalingstjenester. Videre ønsker vi å gi et bidrag til kommersielle aktører som allerede er, eller planlegger en inntreden, i markedet. Vi håper at utredningens funn vil være til nytte for både akademikere og praktikere.

# 2.0 Litteratur

I dette kapittelet skal vi først gi et overblikk av digitalisering i dagens samfunn. Videre definerer vi hva mobilbetaling er, hvordan det fungerer og sikkerhetsproblematikk knyttet til dette. Deretter redegjør vi for definisjoner og tidligere forskning gjort på bekvemmelighet i tjenester. Til slutt presenteres potensielle avveininger mellom sikkerhet og bekvemmelighet i mobilbetalingsapplikasjoner.

## 2.1 Digitalisering i samfunnet

Det  råder ingen tvil om at digitalisering har vært et trendord de siste årene, og kanskje spesielt i 2017. Christoffer Hærnes, Fintech-ekspert og CDO i Sbanken, trekker i sin DN-artikkel "Digitalåret 2018" frem fire trender som vil være spesielt relevant i forbindelse med digitaliseringen i Norge: tingenes internett (IoT), blokkjedeteknologi, kunstig intelligens (AI), samt personvern og datasikkerhet (Hærnes, 2017).

Det stilles høye krav til digitale tjenestetilbyderes sikkerhet, kanskje spesielt når løsningene befinner seg i brukernes smarttelefoner. Store deler av "brukernes liv" samles på ett sted, og personvern og sikkerhet kan kompromitteres dersom smarttelefonen kommer på avveie, blir utsatt for ondsinnede angrep. I 2018 blir EUs forordning for personvern, The General Data Protection Regulation (GDPR), norsk lov. Dette medfører en skjerping av kravene til behandling og lagring av personopplysninger. I tillegg innføres EU-direktivet Payments Services Directive 2 (PSD2), et rammeverk som regulerer betalingstjenester i EUs indre marked. Hensikten med PSD2 er å ytterligere harmonisere regelverket i EU på dette området, fremme innovasjon, styrke sikkerheten for nettbetalinger og legge til rette for økt konkurranse i betalingstjenestemarkedet. Direktivet medfører at tredjepartsaktører, det vil si ikke-banker, kan utføre betalingstjenester på vegne av kunder, innhente kundenes kontiopplysninger, samt sammenstille opplysningene på tvers av banker dersom en kunde er tilknyttet mer enn én bank (Finans Norge, u.å.).

Det har dukket opp nye digitale innovasjoner som hittil ikke er utbredt eller tilgjengelig i Norge. Blant annet har Amazon nylig utviklet et nytt butikkonsept, Amazon Go, hvor hensikten er at kundene skal slippe å stå i kø for å betale. Det eneste kundene trenger for å handle er Amazon Go-applikasjonen, en Amazon-konto og å registrere smarttelefonen sin

når de ankommer butikken. Teknologien som Amazon benytter gjør at varer registreres når de plukkes fra hyllen og avregistreres dersom kunden ombestemmer seg og setter varen tilbake i hyllen. Når kunden er ferdig og har forlatt butikken vil den motta en kvittering fra Amazon og vedkommendes konto belastes (Amazon, u.å.).

Utviklingen av mobilbetalingsapplikasjoner har vært fremtredende i store deler Asia. WeChat og AliPay er to av de største tredjepartsaktørene for mobilbetalingstjenester i Kina, til sammen dekker de 92% av mobilbetalingene på de kinesiske markedet (Chen, 2017). WeChat er den mest brukte meldingsapplikasjonen i Kina, og tilleggstjenesten WeChat Pay fungerer som en digital lommebok. WeChat Pay er tatt i bruk over hele Kina og kan brukes til overføringer mellom forbrukere, til forhandlere og andre organisasjoner (WeChat Pay, u.å.). AliPay ble lansert i Norge i September 2017, men er foreløpig kun tilgjengelig for kinesiske turister. AliPay har omtrent 520 millioner brukere, hovedsakelig i Kina. I tillegg til å kunne betale med smarttelefonen får brukere blant annet push-varsler fra forhandlere i nærheten som godtar betalinger via applikasjonen. Kunden kan motta rabatter, samt se andre brukeres vurderinger av produkter og tjenester (Lindvoll, 2017). Alipay er derfor ikke bare en mobilbetalingsapplikasjon, men en livsstilsapplikasjon.

### 2.1.1 Digitale forbrukere og millenniumsgenerasjonen

Forbrukere kan plasseres i fem ulike kategorier når det kommer til hvor tidlig de tar i bruk en ny innovasjon, disse er: innovatører, tidlige brukere, tidlig majoritet, sen majoritet og etternølere. I praksis kan det være vanskelig å trekke et klart skille mellom de fem kategoriene. På grunn av dette har flere forskere (Gatignon og Robertson, 1985; Shankar, Carpenter, og Krishnamurthi, 1999, referert til i Lam og Shankar, 2014, s. 30) vurdert det dit hen at innovatører og tidlige brukere for praktiske formål kan vurderes som én kategori: tidlige brukere. Tidlige brukere defineres i litteraturen som forbrukere som adopterer et nytt produkt i introduksjons- og vekstfasen av produktet. Tidlige brukeres rolle er svært viktig når det kommer til mobile enheter ettersom produktets livssyklus er relativt kort (Lam og Shankar, 2014, s. 28).

Tidlige brukere anses for å bestå av en stor andel opinionsledere som kan bidra til å påvirke andre forbrukere. Lee (2014, s. 308) konkluderer i sin studie med at studenter på høyskoler

og universiteter inngår i gruppen av tidlige brukere når det kommer til bruken av smarttelefoner.

Denne utredningen skal studere millennials på grunn av karakteristikker som skiller dem fra tidligere generasjoner. Den konkrete definisjonen av intervallet som millennials er født i varierer noe i litteraturen, men det er relativt bred enighet om at millennials er født mellom starten av 1980-tallet og slutten av 1990-tallet. Pew Research Center (Dimock, 2018) introduserer gruppen post-millennials, det vil si individer født etter 1997, men trekker frem at det fremdeles er for tidlig å definere hva som skiller dem fra millennials og at avskjæringspunkt i generasjonssammenheng ikke er en eksakt vitenskap.

I denne utredningen benytter vi et spørreundersøkelsesutvalg bestående av studenter fra Norges Handelshøyskole og Handelshøyskolen BI - Campus Bergen, samt et utvalg i to fokusgrupper bestående av deltakere født fra sent 1980-tall til tidlig 1990-tall.

Millennials er generasjonen som gikk fra barn og ungdom til voksne i det nye millenniet. Dette medfører at de er en gruppe forbrukere som fra tidlig alder er tilvendt en tilværelse med internett og smarttelefoner tilgjengelig og Bull (2010, s. 28) omtaler dem som den første "always connected"-generasjonen. Millennials har også blitt identifisert som den drivende kraften bak netthandel (Smith, 2011, s. 490) og er den største forbrukergruppen av internett, mobilteknologi og sosiale medier (Taylor, 2014). På bakgrunn av disse karakteristikkene anser vi millennials som et passende utvalg til studiet ettersom dette er forbrukere som både er tilvendt, komfortable og erfarne med mobilteknologi og internetthandel.

## 2.2 Mobilbetaling

Au og Kauffman (2008, s. 141) definerer mobilbetaling som enhver betaling hvor en mobil enhet er benyttet for å initiere, autorisere og bekrefte en overføring av en finansiell verdi i bytte mot et produkt eller en tjeneste. Foreløpig er det utfordringer som gjenstår å løse før mobilbetaling blir normen i det norske samfunnet. Vipps utsatte blant annet lansering av mobilbetaling i butikk, og hevder at dette er fordi forbrukerne så langt foretrekker å betale med bankkort med chip (Trumpy, 2018). Tim Cook, direktør for Apple, uttalte også i mai at de ønsket å lansere Apple Pay i Norge innen kort tid. Apple Pay gjør det mulig for iPhone-brukere å betale med mobil i butikk (Baugerød Stokke, 2018).

Mobilbetalinger er definert av Mallat (2007, s. 415) som bruken av mobile enheter for å utføre en betalingstransaksjon hvor penger eller midler er overført fra betaler til mottaker via en tredjepart, eller direkte uten en tredjepart. Mallat (2007, s. 414) trekker også frem flere karakteristikker ved smarttelefoner som gjør dem egnet for betalingsformål. For det første har spredningen av mobil telekommunikasjonsteknologi gjort smarttelefoner stadig mer vanlig og tilgjengelig for brukere. For det andre, sammenlignet med ikke-trådløse datamaskiner og telefoner, er smarttelefoner nærmere brukeren, noe som muliggjør oppbevaring av personlig informasjon og fasiliterer bruken av dem som et betalingsmiddel.

Finansielle institusjoner har ønsket å dra nytte av smarttelefonens utbredelse og tilbyr som følge av dette nye banktjenester via mobile enheter. Denne prosessen startet med overføring av penger fra mobiltelefoner, og var hovedsakelig beregnet for utviklingsland hvor innbyggere ikke har hatt bankkonto med tilknyttet debit- eller kredittkort. De store aktørene i banknæringen, spesielt Visa, anslår at smarttelefonen vil erstatte bankkortet i løpet av de kommende årene. særlig gjelder dette utviklingsland (Jaouad og Wadii, 2014, s. 44).

Forrester Research (henvist til i eMarketer, 2017) hevder at mobilbetaling vil bli mer vanlig på grunn av følgende faktorer:

- Spredning av smarttelefoner og andre mobile enheter som er i stand til å gjøre personlige mobilbetalinger
- Større bevissthet og fortrolighet overfor mobilbetalingsalternativer blant forbrukere
- Bekvemmeligheten ved mobilbetaling
- Lansering av flere mobilbetalingsløsninger
- Forhandlerinteresse og investeringer i mobilbetalingsløsninger

I følge Güngör (2017, s. 956) finnes det to metoder for å gjennomføre en betaling gjennom en mobil enhet:

(1) *Bruk av Bluetooth, RFID-aktivert eller Near Field Communication (NFC)-aktivert mobilenhet*. Her kreves det at forbrukeren åpner en applikasjon som er aktivert med en av de ovennevnte funksjonene, og deretter beveger sin mobile enhet over en betalingsterminal hos forhandleren. I slike tilfeller vil den mobile enheten fungere på samme måte som et kontaktløst kredittkort.

(2) *Bruk av en applikasjon som er lastet ned på enheten på forhånd for å gjennomføre betalingsprosessen.* En applikasjon lastes ned på enheten, og ved et tastetrykk kan penger overføres fra kundens konto til forhandlerens konto, for eksempel gjennom Paypal. I dette tilfellet blir pengene overført gjennom elektronisk datautveksling (EDI – electronic data interchange), og det er ikke behov for en fysisk terminal. Denne metoden er relativt ny sammenlignet med den første.

## 2.3 Digital sikkerhet

Når nye digitale tjenester lanseres spres de raskt, på få dager vil tjenestene være tilgjengelig internasjonalt. I Telenors rapport *Status Digital Sikkerhet 2017* (2017) understrekes det at utbredelsen også i stor grad vil påvirke sikkerhetsbildet. Norge er et av de mest digitaliserte landene i verden og de digitale tjenestene benyttes på alle områder i samfunnet. Privatpersoner, næringslivet og myndighetene er i stor grad digitalisert. Det faktum at digitaliseringen er kommet langt i Norge gjør at kommunikasjon, kunnskap, arbeidsprosesser og tilgang på informasjon forenkles. Baksiden av medaljen er at digitale verktøy og infrastruktur kan bli potensielle ofre for ondsinnede angrep.

Effektiv sikkerhetsinfrastruktur for digitale verktøy krever en helhetlig tilnærming, ettersom sikkerhetstrusler rettes mer mot den digitale sfæren og kan ramme alle industrier. De fleste ondsinnede angrep forekommer i form av datainntrengning og skadelig programvare. Slike former for angrep skjer faretruende ofte i finanssektoren, detaljhandelen, teknologi og i offentlig sektor. Risikoen øker ved hver sensor, lagringsenhet og applikasjon som er tilkoblet et nettverk. Digitale tilkoblinger gjør nettverket "smartere", men samtidig mer utsatt for angrep (Accenture, u.å.).

Med så mye som er avhengig av nettverkssikkerhet er det behov for at verktøy utvikles for å beskytte nettverket mot useriøse aktører. Dette kreves for å forebygge mot angrep, og for at nettverket raskt kan gjenopprettes etter et fysisk eller digitalt angrep. Jim Guinn (u.å.), managing director hos Accenture, fremmer behovet for mer omfattende verktøy for å redusere risikoen for angrep, men understreker at det vil være umulig å sikre digitale operasjoner mot alle trusler. Samtidig peker Guinn på at de organisasjoner som fokuserer på forebygging av eventuelle angrep vil være de organisasjonene som raskest henter seg inn

igjen etter at et angrep har skjedd og på den måten best beskytter sine ressurser og kritiske data.

## 2.4 Sikkerhet i mobilbetaling

I artikkelen *Security in mobile payments* beskriver Vizzarri, Vatalaro og Vari (2013, s. 2) to hovedkriterier for klassifisering av mobilbetalingssystemer: offline- og onlinebetalinger, samt fjern- og nærbetalinger:

**Offline- og onlinebetalinger**

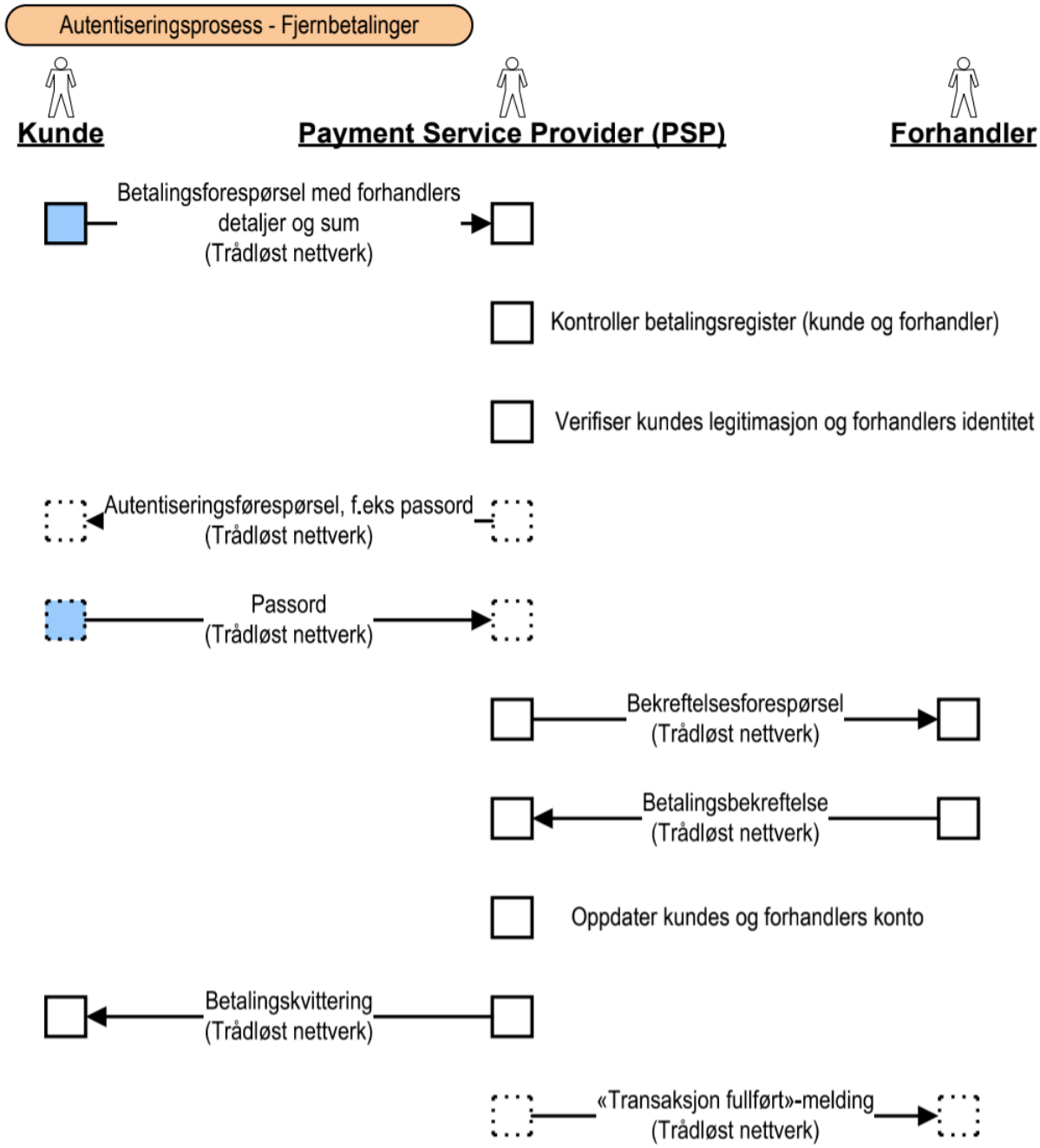
WeChat Pay er et eksempel på en mobilbetalingsapplikasjon som håndterer offline-betalinger (Boden, 2017). Ved offline-betalinger mellom kunde og forhandler er transaksjonen direkte, det vil si at datautvekslingen foregår utelukkende mellom deres respektive enheter. Slik sett er det unødvendig å involvere en tredjepart, og styring av sikkerhets- og krypteringsprosesser vil være mindre komplekse. Denne betalingsmetoden krever likevel at kjøperens enhet inneholder en digital lommebok som må belastet i forkant av transaksjonen. Digitale protokoller etablerer reglene for sikker utveksling av informasjon mellom de enheter som betalingen involverer. I motsetning til offline-betalinger vil online-betalinger involvere andre enheter, som mobile nettverksoperatører (MNO) og selskaper, som i forkant godkjenner transaksjonen og deretter verifiserer statusen til den totale betalingsprosessen. Online-transaksjoner fordrer ikke at brukeren har forhåndsbetalt kreditt lagret på telefonen siden vedkommende kan få direkte kontakt til egen bankkonto via internett og således bruke smarttelefonen som et bankkort.

**Fjern- og nærbetalinger**

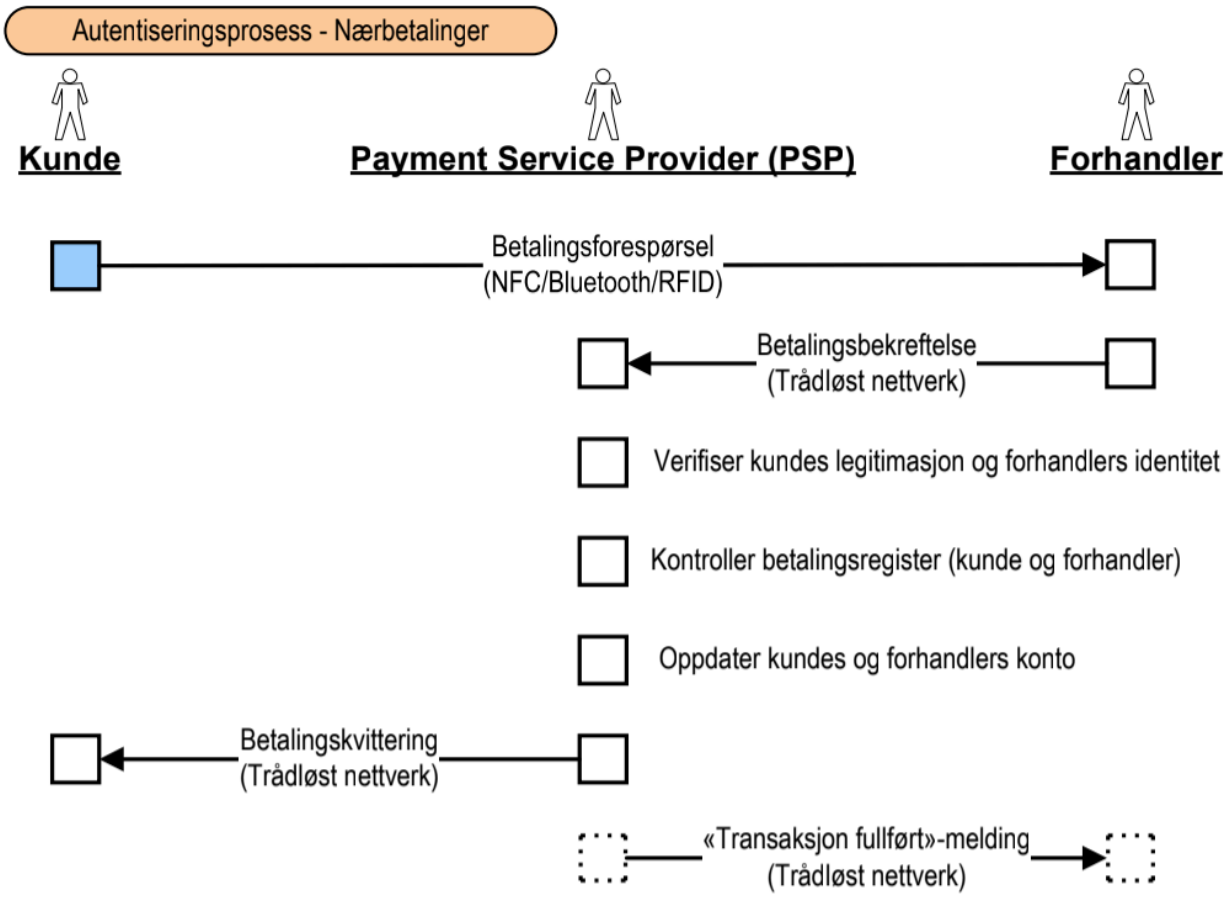
Nærbetalinger (Proximity Mobile Payment, PMP) inkluderer de transaksjoner hvor kjøper og selger er i fysisk nærhet til hverandre. Slike transaksjoner er basert på protokoller, eksempelvis RFID, NFC eller Bluetooth. Mobilbetaling i butikk, som Vipps har planer om å lansere, er et eksempel på en slik nærbetaling (Trumpy, 2018). Fjernbetalinger (Remote Mobile Payments, RMP) inkluderer de betalinger som utføres i tilfeller hvor avstanden mellom selgers og kjøpers enheter ikke påvirker transaksjonen. I slike betalingssituasjoner vil en MNO gi en dataforbindelse, for eksempel mobilapplikasjon.

### 2.4.1 Autentisering og prosedyrer i mobilbetaling

Agarwal, Khapra, Menezes og Uchat (2007, 143) beskriver prosedyrene for mobile betalingssystemer, noe som kan benyttes til å forstå forskjellene i autentiseringsprosesser for henholdsvis fjern- og nærbetalinger. For fjern- og nærbetalinger er hovedprosedyrene som følger (Se Appendiks for nærmere beskrivelse av prosessene):




***Figur 1:*** *Prosedyre for fjernbetalinger*




***Figur:*** *Prosedyre for nærbetalinger*

### 2.4.2 Former for angrep på nærbetalinger

Over har vi forklart hvordan de ulike betalingsformene fungerer med tanke på autentiseringsprosessen. Vipps har offentliggjort at deres planlagte mobilbetaling i butikk-løsning skal lanseres som en type nærbetaling. Vi velger derfor å fokusere på de typene angrep som kan forekomme under nærbetalinger, ettersom det med stor sannsynlighet er denne typen risiko norske forbrukere vil stå overfor. Videre følger en beskrivelse av ulike angrep som kan ramme nærbetalinger som benytter NFC-teknologi (Vizzarri, Vatalaro og Vari, 2013, s. 4):

- *Avlytting*: avlytting av overførte radiosignaler gjort av en mulig angriper. For at angriperen skal kunne avlytte må angriperen besitte det nødvendige utstyret for å motta signaler, samt inneha spesifikk kunnskap for å kunne tolke dataene.
- *Datakorrupsjon*: målet til angriperen er ikke bare å avlytte dataene som overføres, men også omdirigere overføringen. I de enkleste tilfellene er angriperens hensikt å

forstyrre kommunikasjonen slik at mottakeren ikke er i stand til å tolke dataene. Det er ikke særlig vanskelig å gjennomføre et slikt angrep, men det kan resultere i en forstyrring av kommunikasjon.

- *Datainnsetting*: Ved datainnsetting setter angriperen inn en melding mellom de to kommunikasjonsenhetene. Et slikt angrep er mulig dersom enheten som reagerer på meldingen bruker lang tid på å svare. I slike tilfeller kan angriperen sende sin data før den legitime mottakeren. Angrepet er en suksess kun i de tilfeller hvor oppgitt data overføres før den legitime mottakeren begynner å svare.
- *Man in the Middle:* Ved denne typen angrep vil de to partene som ønsker å kommunisere med hverandre bli lurt av en tredjepart. De to partene vil kommunisere uten å vite at kommunikasjonen faktisk foregår mellom tre parter. Av natur har NFC-systemer en iboende beskyttelse mot denne typen angrep, slik at det er lettere å etablere en sikker kommunikasjonskanal.

### 2.4.3 Teknikker for å garantere sikkerhet

Det eksisterer ulike teknikker for å sørge for sikkerheten i mobilbetalingssystemer. Klassiske metoder er *end-to-end*-kryptering og *tokenisering*. Ved *end-to-end*-kryptering blir kontonummer og magnetstripe på kortet fanget og kryptert første gang man benytter kortet i en betalingsprosess. Det gjøres gjennom en ikkemanipulerbar sikkerhetsmodul eller i en uavhenging krypteringsprogramvare. Med *tokenisering* vil en kryptert eller tilfeldig verdi, kalt et *token*, erstatte kortnummeret eller magnetstripen i en elektronisk transaksjon. *Tokenet* blir da referansenummeret som representerer kortnummeret slik at alle *tokens* kan spores tilbake til det opprinnelige kortnummeret (Vizzarri, Vatalaro og Vari, 2013, s. 5). Elefant (2011) fremhever viktigheten av at *end-to-end*-kryptering og *tokenisering* går raskest mulig. Når en kunde bruker sitt betalingsmiddel hos en forhandler vil kortinformasjonen være ubeskyttet inntil den enten blir *tokenisert* i en gateway eller kryptert på en prosesseringsplattform. Dersom dette tar for lang tid kan kundenes sensitive informasjon bli utsatt for ondsinnede angrep.

I løpet av de siste årene har autentiseringsteknikker blitt forbedret for å forhindre slike angrep. Den beste løsningen vil være å benytte en flerfaktorautentisering og dynamisk autentisering, som gir best beskyttelse mot uautoriserte individer som kompromitterer betalingstransaksjonen (Vizzarri, Vatalaro og Vari, 2013, s. 5).

### 2.4.4 Autentisering

*Flerfaktorautentisering* relaterer til kundens ulike autentiseringsalternativer. Weir, Douglas, Carruthers og Jack (2009, s. 47) beskriver tofaktorautentisering som en sikkerhetsløsning hvor det kreves verifikasjon av to forskjellige komponenter. Typiske komponenter er: Kunnskap (passord), eiendel (bankkort) og fysiske attributter (fingeravtrykk). Tofaktorautentisering bidrar til å hindre bedrageri ved å ha en ekstra barriere i tillegg til for eksempel et passord. Debit-kort har alltid hatt to komponenter: selve bankkortet (eiendel) og en hemmelig PIN (kunnskap). Nettbanker har for eksempel hatt passord (kunnskap) pluss kodebrikke (eiendel), og i Norge har man utvidet med bankID og bankID på mobil. Løsninger på autentisering kan være enten statiske eller dynamiske, hvor dynamiske er vesentlig sikrere (Vizzarri, Vatalaro og Vari, 2013, s. 5). Ved statisk autentisering vil de samme persondataene bli brukt for validering. Ved dynamisk autentisering brukes forskjellige persondata for hver autentisering, og dataene som benyttes er ofte spesifikke for transaksjonen som gjennomføres.

Behovet for dynamisk transaksjonsautentisering har oppstått fordi *end-to-end*-kryptering ikke kan beskytte forhandlere fullt og helt fra datatyveri og ondsinnede angrep . Bruken av dynamisk transaksjonsautentisering gir forhandlere en flerlagsløsning for å sikre hvert element av betalingen. Den benytter en kombinasjon av kraftig kryptering, sikker tokenisering, forfalsknings- og manipulasjonsgjenkjenning, datarelevans og integritet, samt dynamiske, digitale transaksjonssignaturer. Sammen vil disse faktorene validere og beskytte hele transaksjonen og hvert element som er involvert.

## 2.5 Bekvemmelighet

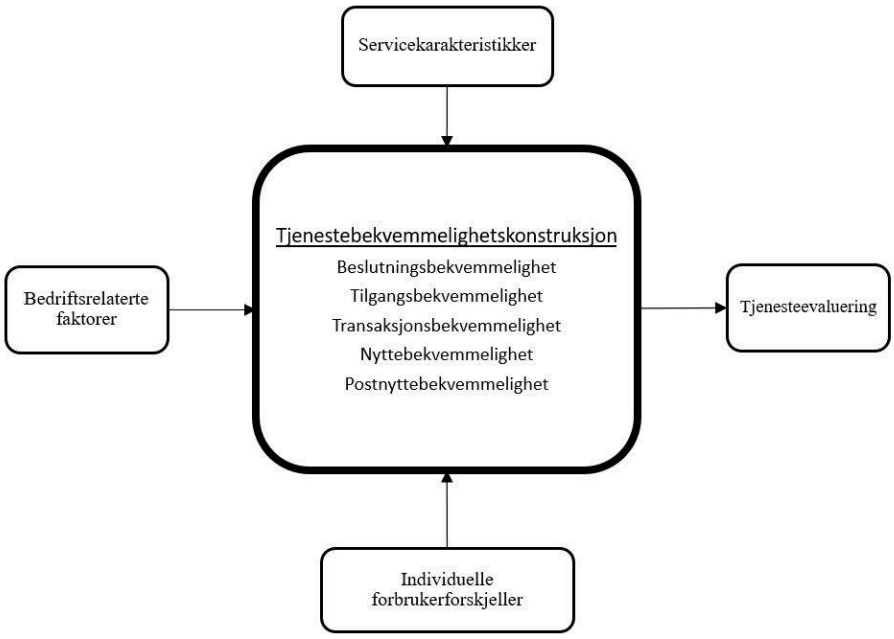
Konseptet bekvemmelighet dukket først opp i markedsføringslitteraturen med en henvisning til forskjellige produktkategorier. Copeland (1923, henvist til i Berry, Seiders og Grewal, 2002, s. 1) sin klassifisering av forbrukerprodukter inkluderte *bekvemmelighetsprodukter*. Dette gjaldt intensivt distribuerte produkter hvor anskaffelse krevde minimalt med tid, samt minimal fysisk og kognitiv innsats. I den tidlige markedsføringslitteraturen betegnet derfor bekvemmelighet den tiden og innsatsen som forbrukerne brukte på å kjøpe et produkt, fremfor å betegne en karakteristikk eller en egenskap ved produktet (Brown, 1990, s. 54). Senere begynte forskere å fokusere på tid, innsats og alternativer som ressurser, og anså

bekvemmelighet som et attributt som reduserte de ikke-monetære kostnadene for kunden (Berry, Seiders and Grewal, 2002, s. 2).

Litteraturen om tid er substansiell og forsket på i flere fagfelt. Litteraturen om innsats er derimot mindre og begrenser seg hovedsakelig til kognitiv innsats. Berry, Seiders og Grewal (2002, s. 3) trekker frem to spesifikke litteraturstrømmer i sin studie av tjenestebekvemmelighet. Den ene strømmen fokuserer på forbrukernes bekvemmelighetsorientering, og undersøker hvorfor noen forbrukere er mer tilbøyelige til å kjøpe bekvemmelighetsrelaterte produkter og tjenester enn andre. Den andre strømmen er litteraturen om forbrukerventing, som undersøker hvordan forbrukere responderer på å måtte vente, og hvordan bedrifter styrer venteprosessen.

Fordi bekvemmelighetslitteraturen har konsentrert seg nesten utelukkende om å spare tid, har karakteristikker som sparer innsats blitt regnet som tidsbesparende attributter (Brown, 1990, s. 54). Innsats har blitt ansett som en relevant og positiv input i en byttehandel. I en rettferdig byttehandel vil en eventuell høyere innsats som den ene parten yter øke denne partens forventning om motytelse (Berry, Seiders og Grewal, 2002, s. 2).

### 2.5.1 Tjenestebekvemmelighet




***Figur 3:*** *Tjenestebekvemmelighetskonstruksjonen (Berry, Seiders og Grewal, 2002, s. 4)*

Berry, Seiders og Grewals (2002, s. 4) konseptuelle modell av tjenestebekvemmelighet er presentert i figur 1. Den viser at visse karakteristikker har sterk innflytelse på forbrukernes oppfatning av bekvemmelighet. De bedriftsrelaterte faktorene til tjenesteleverandøren, altså hvordan en bedrift tilrettelegger for bekvemmelighet gjennom distraksjoner, forbedringer, informasjon, design og merkevare, og forbrukernes individuelle forskjeller knyttet til demografi, erfaring eller kultur, påvirker også forbrukernes oppfatning.

Sentralt i modellen er selve tjenestebekvemmelighets-konstruksjonen, konseptualisert som forbrukernes oppfatninger av tid og innsats knyttet til å kjøpe eller å bruke en tjeneste. Disse oppfatningene favner om fem definerende typer for bekvemmelighet - *beslutning, tilgang, transaksjon, nytte og postnytte.* Disse formene for bekvemmelighet speiler aktivitetene i prosessen som forbrukerne gjennomgår for å kjøpe eller bruke en tjeneste.

*Beslutningsbekvemmelighet:* Forbrukere som ønsker en spesiell tjeneste bruker tid og innsats på å beslutte hvordan de skal anskaffe den. Den første beslutningen forbrukeren må fatte er hvorvidt den skal utføre ytelsen selv eller kjøpe en tjeneste. En kjøpsbeslutningen krever igjen beslutninger knyttet til hvilken leverandør som skal brukes og hvilken spesifikk tjeneste som ønskes kjøpt. Beslutningsbekvemmelighet defineres av forbrukernes oppfattede bruk av tid og innsats på å gjøre en kjøp- eller bruksbeslutning.

Forbrukere har lært å forvente variabilitet i arbeidskrevende tjenester og vier derfor tid og innsats i å finne tjenester som de har tillit til. Dette gjelder spesielt tjenester som er involverende, komplekse, gjentakende og medfører konsekvenser for forbrukeren. Forbrukere av denne typen tjenester søker ofte varige relasjoner med en leverandør de kan stole på, dels på grunn av tids- og innsatskostnader knyttet til et gjenkjøp. Gwinner, Gremler og Bitner (1998, s. 104) hevder at forbrukerselvtillit, altså redusert angst og sterk troverdighet overfor tjenesteleverandøren, er den viktigste fordelen for forbrukere når de skal opprettholde en relasjon med en tjenestebedrift. Tidligere forskning har adressert hvordan forbrukere reduserer tids- og innsatskostnader ved å søke råd fra andre, for eksempel opinionsledere (Montgomery og Silk, 1971, referert til i Berry, Seiders og Grewal, 2002, s. 6). Etterspørsel etter støtte fra en tredjepart har stimulert veksten av nye online-tjenester. Visse forbrukere benytter shopping-roboter til å finne de laveste prisene i markedet, som for

eksempel prisjakt.no. Noen applikasjoner gjør forbrukerne i stand til å innhente meninger fra andre, for eksempel gjennom TripAdvisor.

*Tilgangsbekvemmelighet:* Tilgangsbekvemmelighet omhandler forbrukernes oppfattede bruk av tid og innsats som kreves for å initiere en tjenesteleveranse. Dette omfatter aktivitetene en forbruker må utføre for å forespørre tjenesten, og i noen tilfeller aktiviteter som kreves for å motta den. Forbrukere kan initiere tjenester personlig (dra til en restaurant), eksternt (ringe inn en takeout-bestilling), eller gjennom begge metoder (ringe inn en reservasjon, deretter dra til restauranten). Tilgangsbekvemmelighet er hovedgrunnen til at forbrukere velger selvbetjening i visse tjenester. Minibanker ble blant annet populære dels fordi de var tilgjengelige utenfor bankenes åpningstider.

*Transaksjonsbekvemmelighet:* Transaksjonsbekvemmelighet knytter seg til forbrukernes oppfattede bruk av tid og innsats for å effektivisere en transaksjon. Transaksjonsbekvemmelighet fokuserer kun på handlingen forbrukeren må utføre for å sikre seg retten til en tjeneste. Når forbrukeren har bestemt seg for å kjøpe en tjeneste og skaffet seg tilgang til selve tjenesten, må forbrukeren også delta i en transaksjon. Transaksjonen involverer vanligvis penger i bytte mot et løfte for å få utført tjeneste.

I følge en Forrester Research-rapport vil to tredjedeler av internetthandlere forlate sine "handlekurver" før de faktisk kjøper noe (Tedeschi, 2000). En annen studie har funnet at netthandlere forlater sine handlekurver på trege sider etter så lite som åtte sekunder (Berry, Seiders and Grewal, 2002, s. 7). Transaksjonsubekvemmelighet, for eksempel det å fullføre et detaljert registreringskjema, er en medvirkende faktor for høy fluktfrekvens.

*Nyttebekvemmelighet:* Nyttebekvemmelighet er forbrukernes oppfattede bruk av tid og innsats på å oppleve, eller dra nytte av, en tjenestes kjernefordel. For eksempel det å bli transportert av en drosje fra A til B. Å manøvrere en forbruker effektivt til nyttestadiet i en tjenesteprosess, for så å gi dem en ubekvemmelighet på dette stadiet kan har sterke negative effekter, fordi persepsjon av en byrde forstyrrer persepsjonen av nytten.

*Postnyttebekvemmelighet:* Postnyttebekvemmelighet involverer forbrukernes oppfatning av bruk av tid og innsats når de på ny initierer kontakt med en bedrift etter selve nyttestadiet.

Postnyttebekvemmelighet kan oppstå ved behov for reparasjon av et produkt, vedlikehold eller bytting. Noen ganger initierer forbrukere ny kontakt på grunn av en tjenestefeil som ikke er gjenkjent eller løst under selve møtet med tjenesten. Et eksempel er når en forbruker kontakter kundeservice for assistanse knyttet til bruk av tjenesten. Noen aktiviteter relatert til postnyttebekvemmelighet initieres av tjenestebedriften. Dette kan gjelde en pasient som returnerer til en kirurg for en postoperasjonsevaluering. Viktigheten ved postnyttebekvemmelighet har blitt understreket de siste årene på grunn av vanskeligheter som forbrukere har møtt når de ønsker å returnere produkter kjøpt over internett.

Forbrukere vil foretrekke å ikke forholde seg til postnyttestadiet, med mindre dette tilfører merverdi til tjenesten. Forbrukere må bruke av sin egen tid og innsats for å motta slike ekstrafordeler. Postkirurgipasienter vil sannsynligvis ønske å returnere til kirurgen fordi kirurgen kan betrygge pasienten, gi råd eller vurdere nye behandlingstiltak.

## 2.6 Avveininger mellom sikkerhet og bekvemmelighet i mobilbetaling

Mobilbetaling vil gi konsumentene anledning til å håndtere sin økonomi gjennom én applikasjon ved at forhåndsbetalte kort, lojalitetskort og debit-/kredittkort er integrert i applikasjonen. Gjennom en mobil lommebok vil konsumenter også kunne betale regninger, se kontooversikt og overføre penger med mer fra mobilen. Geetha og Sujatha (2017, s. 193) hevder at bekvemmeligheten dette medfører for konsumentene vil drive konsumenter mot bruken av mobile lommebøker og vekk fra tradisjonelle betalingsmetoder.

Hasham, Vancauwenberge, Weiner og Rezek (2016) beskriver et eksempel på hvordan ulike forbrukere avveier sikkerhet og bekvemmelighet i digitale tjenester ulikt. Det vises til et gitt scenario hvor to brukere av en nettside skal logge inn samtidig. Den første brukeren har vansker med å huske passordet sitt og må gjennom en resettingprosess. Vedkommende kjenner på frustrasjon knyttet til å gå gjennom disse stegene og tenker “Hvorfor kan ikke bare siden huske passordet mitt?” Den andre brukeren oppgir passordet sitt og kommer direkte inn på sin konto. Denne brukeren bekymrer seg over at siden ikke virker veldig sikker. Vedkommende hadde satt pris på en form for flerfaktorautentisering, for eksempel ved å få tilsendt et sikkert engangspassord på en annen enhet før tilgangen ble gitt. Her har vi to forbrukere med veldig forskjellige forventninger til digital sikkerhet. Den ene prioriterer

bekvemmelighet, og den andre sikkerhet. Utfordringen i dette eksempelet, og i øvrige problemstillinger knyttet til sikkerhets- og bekvemmelighetsavveininger, handler derfor om hvordan man skal tilfredsstille forbrukere med asymmetriske behov.

Når forbrukerne skal veie sikkerhet og bekvemmelighet opp mot hverandre, har tidligere forskning vist at det ofte dreier seg om hvordan forbrukere forholder seg til autentisering i flere faser (Weir et al., 2009, s. 48; Crosman, 2016). Vil norske forbrukerne sette pris på en bekvemmelig og enkel autentiseringsprosess med ett trinn, eller vil de ønske å gå gjennom et eller flere ekstra trinn? Og; finnes det øvrige forbrukeravveininger mellom sikkerhet og bekvemmelighet som kan påvirke deres valg av betalingstjeneste? Gjennom datainnsamling blant norske millennials skal vi søke å finne svar på disse spørsmålene. Dette vil bli presentert under *5.0 Funn* og *6.0 Diskusjon*.

# 3.0 Utvikling av spørreskjema

For å få svar på hvilke holdninger millennials har til sikkerhet og bekvemmelighet i mobilbetalingsapplikasjoner har vi gjennomført datainnsamling gjennom et spørreskjema. I litteraturgjennomgangen har vi funnet gode definisjoner på tjenestebekvemmelighet generelt og forklart de ulike sikkerhetsmekanismene og -truslene som eksisterer i mobilbetalingsapplikasjoner. For å lage egnede påstander til spørreskjemaet fant vi det nødvendig å konkretisere tjenestebekvemmelighet og sikkerhet fra et mobilbetalingsperspektiv. I eksisterende litteratur fant vi ikke tilstrekkelig teori eller forskning som tidligere har definert dette fra forbrukernes ståsted. For å få klare definisjoner som gjenspeiler forbrukernes holdninger fant vi det hensiktsmessig å gjennomføre fokusgrupper hvor de to begrepene var tema.

## 3.1 Fokusgrupper

I denne utredningen har vi benyttet fokusgrupper blant annet for å operasjonalisere og generalisere begrepene i problemstillingen gjennom en samtale med en gruppe *tidlige brukere* av mobilapplikasjoner. Gjennomføringen av fokusgruppene ble gjort tidlig i forskningsprosjektet, med hensikt om å følge dem opp med en en bredere, mer kvantitativ metode på et større utvalg (Stewart, Shamdasani og Rook, 2007, s. 41). Utsagnene fra de transkriberte versjonene av fokusgruppene ble benyttet til å formulere påstander til spørreskjemaet, samt hensyntatt i diskusjonskapittelet. Fokusgrupper har som alle teknikker sine fordeler og begrensninger. I vårt tilfelle var det fordeler ved at vi på en effektiv måte fikk samlet store mengder utsagn knyttet til begrepene sikkerhet og bekvemmelighet i mobilbetalingsapplikasjoner. Vi fikk også muligheten til å stille deltakerne oppfølgningsspørsmål dersom det var uklarheter, og gjennomføringen var tilnærmet kostnadsfri. Av begrensninger kan blant annet det at en eller flere av deltakerne er dominante i samtalen påvirke de andre deltakerne (Stewart, Shamdasani og Rook, 2007, s. 43), men vi oppfattet ikke at dette var tilfelle blant våre deltakere. En begrensning var at det lave antallet deltakere gjorde utsagnene lite generaliserbare (Stewart, Shamdasani og Rook, 2007, s. 43), men vi så mange likheter i hvordan deltakerne definerte sikkerhet og bekvemmelighet på tvers av de to fokusgruppene.

### 3.1.1 Design av fokusgrupper

Vi startet med å definere hva vi ønsket å få svar på i fokusgruppene og laget en intervjuguide som inneholdt spørsmål knyttet til både sikkerhet og bekvemmelighet. Deretter identifiserte vi hvilke typer deltakere vi hadde behov for, i tillegg til moderator og assisterende moderator. Da det var gjort rekrutterte vi deltakere innenfor kriteriene vi hadde satt og gjennomførte selve fokusgruppene. Til slutt ble samtalene transkribert og analysert.

**Intervjuguide**

Hovedpunktene som vi ønsket å få svar på i fokusgruppene var som følger:

- Hvordan definerer deltakerne mobilbetalingsapplikasjoner
- Hvordan definerer deltakerne sikkerhet i mobilbetalingsapplikasjoner
- Hvordan definerer deltakerne bekvemmelighet i mobilbetalingsapplikasjoner

Intervjuguiden startet med et par spørsmål som dreide seg om generell bruk av mobilapplikasjoner. Dette ble gjort fordi Liamputtong (2011, s. 76) anbefaler å starte med et par introduksjonsspørsmål, og dette ga deltakerne anledning til å bli komfortabel i situasjonen. Videre stilte moderator et overgangsspørsmål, som her dreide seg om bruken av mobilbetalingsapplikasjoner blant deltakerne. Deretter ble selve fokuset for samtalen introdusert i form av spørsmål knyttet til hva deltakerne oppfattet som bekvemmelighet og sikkerhet i forbindelse med alt fra valg av til bruk av mobilbetalingsapplikasjoner. Da samtlige hovedpunkter var dekket tilstrekkelig, ble deltakerne stilt noen oppsummerende spørsmål for å sikre at alle oppfatninger var forstått og kommet frem i samtalen. Se Appendiks for utfyllende intervjuguide.

**Identifisering og rekruttering**

Hovedkriteriene for deltakerne var at de var innenfor millenniumsgenerasjonen og *tidlige brukere* av mobilteknologi. Ut ifra disse kriteriene anså vi at det ville være mulig å rekruttere deltakere gjennom eget nettverk. Etter gjennomføring av den første fokusgruppen oppdaget vi at det ville være behjelpelig å ha med deltakerne som hadde utvidet kompetanse om bekvemmelighet og sikkerhet. De hittil identifiserte deltakerne hadde forbrukeroppfatninger om bekvemmelighet og sikkerhet i mobilbetalingsapplikasjoner, men ikke mye kunnskap om de bakenforliggende mekanismene. Ved å ta inn deltakere med en slik teknisk kompetanse, kunne de øvrige deltakerne bli opplyst uten at vi som moderatorer påvirket dem ved å delta i

stor grad.  Vi valgte derfor å rekruttere to deltakere som hadde henholdsvis følgende tilleggskriterier: Kunnskap om sikkerhet og bekvemmelighet i mobilbetalingsapplikasjoner. Den ene nye deltakeren jobber med *fremtiden innen autentisering* i et kjent teknologiselskap og har derfor mye innsikt hva angår sikkerhet i mobilbetalingsapplikasjoner. Den andre nye deltakeren er en *user experience designer* og jobber som konsulent i en stor, norsk bank, og har derfor mye kunnskap om bekvemmelighet i mobilbetalingsapplikasjoner. Ved å ha med de to deltakerne som hadde en form for ekspertkompetanse, fikk både de øvrige deltakerne, og vi som forskere, bedre innsikt i temaene, hvilket påvirket bredden i samtalen.

Deltakerne ble lovet konfidensialitet i forbindelse med sin deltakelse og ble kompensert med en enkel gave.

Vi valgte å benytte oss selv som forskningspersonell til de to rollene, moderator og assisterende moderator, som kreves for å gjennomføre en fokusgruppe (Liamputtong, 2011, s. 60-64). Den assisterende moderatoren hadde tilgang til moderator via chat-funksjonen i et google-dokument og ga beskjed underveis dersom samtalen eller tidsskjemaet begynte å flyte ut. Moderator fulgte intervjuguiden og avbrøt samtalen dersom den ble gjentakende, samt stilte spørsmål dersom samtalen stoppet opp. Moderator var påpasselig med ikke å påvirke eller lede deltakernes samtale i en bestemt retning, men opptrådte som en navigatør for å sikre at alle punkter ble dekket.

### 3.1.2 Praktisk gjennomføring

Med utgangspunkt i anbefalinger fra Liamputtong (2011, s. 84) og Stewart, Shamdasani og Rook (2007, s. 93) ble samtalene spilt inn, fremfor å notere underveis. Vi arrangerte også bord og stoler i en sirkel for å fasilitere interaksjonen mellom deltakerne. På denne måten kunne de se hverandre i øynene fremfor å henvende seg til moderator, noe som skapte samspill og dynamikk i samtalen. Deltakerne ble også plassert slik at de som vi på forhånd visste at gjerne snakker mye satt litt fra hverandre. Assisterende moderator satt utenfor sirkelen, men på en slik måte at øyekontakt med moderator kunne oppnås og tegn kunne sendes uten at deltakerne la merke til dette. Samtalen startet med at alle introduserte seg selv, og på denne måten sikret vi at samtlige hadde fått bidratt fra starten av. Deretter fulgte samtalen i tråd med intervjuguiden og varte frem til alle punktene var dekket.

### 3.1.3 Bearbeidelse og analyse av fokusgruppesamtale

**Transkribering**

Før samtalen kunne analyseres måtte den transkriberes. Transkriberingen forenklet den videre analysen og sikret skriftlig dokumentasjon fra fokusgruppene. Transkriberingen skulle korrespondere mest mulig med deltakernes uttalelser, og redigering av deres formuleringer ble brukt i minst mulig grad. Hovedårsaken til at vi ikke ønsket å redigere ufullstendige setninger og svake formuleringer var for å gi et mest mulig korrekt bilde av hvordan deltakerne forholdt seg til temaene som det ble snakket om.

Vi benyttet programmet Transcriber 1.5.1.

**Innholdsanalyse**

Vi anså det fordelaktig å gjennomføre en innholdsanalyse ettersom det kan benyttes for å sette elementer fra en tekst i en sammenheng som gjør dem forståelig (Sæter og Sterri, 2015). Ved anvendelse av innholdsanalyse produserte vi en systematisk og omfattende oppsummering av datainnhentingen.

Det finnes flere ulike måter å gjennomføre en innholdsanalyse på, men hovedkonseptene har flere fellestrekk. Vi benyttet Bengtssons (2016, s. 11-12) fire steg for gjennomføring av innholdsanalysen.

**Dekontekstualisere**

I den første fasen gjorde vi oss kjent med dataene som var samlet inn ved å lese gjennom transkriberingen og få et helhetlig bilde av innholdet. Deretter brøt vi ned dataene i mindre, meningsfulle enheter. Hver av enhetene som var identifisert blir merket med en kode som skulle gi mening ut ifra sammenhengen. Kodene forenklet identifiseringen av konsepter slik at dataene lettere kunne samles i kategorier. Kodelisten ble utviklet under bearbeidelsen av den transkriberte versjonen av den første fokusgruppen, og kan sees i sin helhet i Appendikset.

**Rekontekstualisere**

I rekontekstualiseringsfasen, etter at meningsenhetene var identifisert, forsikret vi oss om at alle aspektene i innholdet var dekket i tråd med forskningsformålet. Vi leste originalteksten

på nytt sammen med kodelisten. Deretter fargela vi de ulike meningsenhetene i den originale transkriberingen for å få et tydelig skille mellom disse. De delene av teksten som ikke var markert med farger kunne anses som unødvendige dersom de ikke var relevant for selve problemstillingen. Vi vurderte likevel om slike utsagn var relevant informasjon som kunne belyse oppgaven og bli inkludert i videre arbeid.

**Kategorisere**

Før kategoriseringen startet måtte de identifiserte meningselementene komprimeres. Dette innebar at setninger ble forkortet uten at de mistet innhold og mening. Å komprimere elementene kan være helt nødvendig når de innhentede dataene er basert på intervjuer. Vi kategoriserte på bakgrunn av tjenestebekvemmelighetskonstruksjonen (Berry, Seiders og Grewal, 2002, s. 4), og utviklet fire sikkerhetskategorier ut ifra hovedelementene som oppsto i diskusjonen. De fire kategoriene ble organisert som følger; Generell oppfatning av sikkerhet; Sikkerhet knyttet til offentlige regulering og lovverk; Sikkerhetstiltak fra leverandørs side; Sikkerhetstiltak som forbrukeren selv kan utføre. Det var viktig at de ulike kategoriene skulle være internt homogene og eksternt heterogene, hvilket betyr at ingen data skulle falle mellom to kategorier, ei heller kunne plasseres i to eller flere kategorier.

**Samle**

For å sikre stabilitet og reliabilitet anså vi det som gunstig å gjøre analysearbeidet og kodingen hver for oss og deretter sammenligne våre respektive notater samt forslag til koder og kategorier. På det jevne hadde vi tolket samtalene relativt likt, men kom i samarbeid frem til at vi kunne kategorisere på bakgrunn av de fem formene for bekvemmelighet, samt de fire ovennevnte kategorier for sikkerhet. Deretter samlet vi de utvalgte utsagnene og plasserte dem i tabeller under sine respektive kategorier. Transkriberingen og analysen av samtalen i den første fokusgruppen ble gjennomført induktivt, og gjorde det vesentlig enklere å analysere samtalen i den andre fokusgruppen ettersom at vi da hadde klarhet i hvilke koder og kategorier som skulle benyttes.

### 3.1.4 Funn fra fokusgruppene

Det var tydelig i fokusgruppene at deltakerne prioriterte bekvemmelighet fremfor sikkerhet i mobilbetalingsapplikasjoner. Samtlige deltakere hadde benyttet seg av Vipps, og de fleste var kjent med øvrige tjenester slik som mCash, Mobile Pay, Payr og Paypal. Under følger et utvalg av utsagn som er direkte knyttet til de fire sikkerhetskategoriene som ble utviklet i

innholdsanalysen og de fem formene for bekvemmelighet fra tjenestebekvemmelighetskonstruksjonen (Berry, Seiders og Grewal, 2002, s. 4).

**Generell oppfatning av sikkerhet**

Deltakerne diskuterte hvilken betydning sikkerhet i mobilapplikasjoner og mobilbetalingsapplikasjoner hadde for dem. Mange av deltakerne ytret at sikkerhet var noe de ikke tok så mye hensyn til i det daglige, og at de anså det som lite sannsynlig at de selv skulle bli utsatt for ondsinnede angrep.

*"Det er ikke noe jeg forholder meg til, at det skal gå galt."*

*"[...] og jeg tror at sannsynligheten er liten."*

*"[...] inntil jeg blir rammet selv så, så bare lukker jeg øynene for den risikoen."*

**Sikkerhet knyttet til offentlig regulering og lovverk**

Det var bred konsensus i gruppene om at de følte seg trygge på at det fantes eksterne sikkerhetsmekanismer (f.eks. regelverk og forsikringer) som forebygget ondsinnede angrep og beskyttet dem dersom slike det oppsto.

*"[...] da er det helt sikkert noe regelverk som tar oss i vare."*

*"Jeg er ikke helt sikker på hvordan det fungerer, jeg bare antar at det fungerer sånn, som forbruker, at ja, hvis det skjer noe så skal det ordne seg."*

Det var likevel én av deltakerne i den første fokusgruppen som viste noe usikkerhet og stilte spørsmål ved dette ettersom at mobilbetalingstjenester er et relativt nytt område.

*"Er det det? For dette er så nytt."*

I den andre fokusgruppen hadde en av deltakerne i løpet av de siste seks månedene blitt utsatt for et angrep på sin ebay-konto og opplevd å ikke få refundert tapet på 10.000 kroner.

*"Uten PayPal, så det er ingen som dekker noe som helst. Banken gir meg skylden for at jeg har opptrådt uten forsiktighet."*

**Sikkerhetstiltak fra leverandørs side**

I forbindelse med leverandører av mobilbetalingsapplikasjoner diskuterte deltakerne blant annet tillit til leverandør og hvordan mobilbetalingsapplikasjonen hentet informasjon fra andre applikasjoner på brukerens enhet, for eksempel slik Vipps benytter mobilenhetens kontaktliste.

*"[…] hvis du lover vekk all informasjonen din og om alle vennene dine i prosessen så skal jeg nok stole litt mer på utgiver."*

Utgivers renommé ble også trukket frem som en viktig faktor.

*"Godt rykte er viktig. Veldig viktig. Det er ikke aktuelt å bruke noe som ikke har det."*

*"[...] når den der DnB-skandalen var i forfjor, [...] Da hadde ikke jeg Vipps en stund. Og da var jeg ganske megaskeptisk."*

Deltakerne snakket også om tillit til utenlandske aktører, og de var skeptiske til å benytte seg av en tjeneste levert av eksempelvis Facebook.

*"Ville kanskje stolt mer på en norsk eller en lokal utgiver."*

For mange av deltakerne var det viktig at en bank var involvert på eiersiden.

*"Jeg syns kanskje en bankinstitusjon, må si, må være i hvert fall involvert her […] En objektiv part! […] En finansinstitusjon."*

*"Banker og sånn forventer jeg at har alt på stell."*

At en leverandør kunne tilby sikre innloggingsmetoder var et sterkt kriterium.

*"For å bare slenge på flere sånne [autentiserings]faktorer det, det er ikke godt nok."*

Da deltakerne ble spurt om de ønsket påminnelser fra leverandør om endre innloggingsinformasjon mente de at det i varierende grad var praktisk.

*"Men det syns jeg er ganske faktisk bekvemmelig, selv om du må gjøre en endring. Da sier de: nå anbefaler vi alle å endre alle passordene sine på alle Google-kontoene."*

*"[...] takk for påminnelsen, eller så hadde jeg ikke husket det."*

**Sikkerhetstiltak som forbrukeren selv kan utføre**

Da deltakerne ble spurt om hva de selv kunne gjøre for å håndtere sikkerhetsproblematikk ble i hovedsak to emner diskutert. Disse var å sette seg inn i leverandørens vilkår og hvordan de selv kunne styrke robustheten i passord og PIN-koder de benyttet seg av. Deltakerne ble av moderator spurt direkte om de hadde for vane å lese vilkårene før de tok i bruk en applikasjon.

*"Det kommer an på hva slags type ting det er"*

*"Nei! Aldri. Jeg tror aldri at jeg har gjort det."*

*"Av og til."*

*"Men altså jeg har ikke tid til å, jeg har IKKE tid til å sette meg ned i åtte minutter og lese vilkårene for å laste ned Vipps."*

Kompleksitet og variasjon i bruk av passord og PIN-koder varierte litt blant deltakerne, men mange oppga at de av bekvemmelighetsårsaker foretrakk å bruke samme eller lignende passord og PIN-koder.

*"Jeg bruker samme kode på alt."*

*"Alle har bare sånn to passord de bruker."*

*"Men hvis noen fant min personlige kode, så kunne de endret ALT om meg. Altså, AltInn, nettbanken, altså alt, for BankID har jo samme kode på alle flater, sant."*

En av deltakerne i fokusgruppen, som per i dag jobber med fremtiden innen autentisering, opplyste de andre deltakerne om hvor enkelt et passord eller en PIN-kode kunne knekkes.

*"[...]det er veldig stor forskjell på hvor lang tid det tar å knekke åtte siffer og ti."*

En annen deltaker kunne fortelle om hvordan det å benytte seg av muligheten for å lagre innloggingsinformasjon og passord hadde ført til tap av finansielle eiendeler.

*"[…] jeg har bestilt noe én gang, og så trykket "husk min betalingsinformasjon". Sånn at når jeg da ble hacket så lå informasjonen tilgjengelig der. Så ingen stjal min kontoinformasjon, jeg ga den til dem […]."*

Dette skapte noe uro blant øvrige deltakere.

*"Jeg må hjem og skifte alle passord!"*

**Beslutningsbekvemmelighet**

Da deltakerne ble spurt om hvordan de tok tids- og innsatsbesparende beslutninger knyttet til hvilken mobilbetalingsapplikasjon de skulle laste ned, ble det snakket mye om pris, samt hvilke kundeomtaler eller vurderinger applikasjonen hadde fått.

*"Jeg vet hva jeg skal ha, så trykker jeg på den med finest bilde. Den som er gratis."*

*"[…] er det dårlig review så laster jeg det ikke ned."*

*"Jeg liker å sjekke vurderinger."*

**Tilgangsbekvemmelighet**

Deltakerne diskuterte om det ville være mer bekvemmelig å ha én mobilbetalingsapplikasjon som fungerte i alle, eller i de fleste, utsalgssteder fremfor å benytte seg av flere ulike.

*"[…] hvorfor skal du ha liksom tre forskjellige?"*

*"Hvorfor skal du bruke flere?"*

En av deltakerne ga uttrykk for at det å ha flere apper, som dog fungerte i de samme utsalgsstedene, var å foretrekke.

*"Ja, det er det igjen, for da står alt og faller på én, så hvis den krasjer den ene appen, eller det er ett eller annet problem med den appen, så er du litt sånn rådvill, mens hvis du har flere så; ja, okei, da bare bruker jeg denne."*

En annen deltaker fremmet viktigheten av at mobilbetalingsløsningen måtte være helintegrert i en tjenestevirksomhet.

*[…] du kan betale visse ting i Bergen Kommune med Vipps, men sånn som parkeringsbøter og sånn kan du ikke betale med Vipps, […] veldig vanskelig for forbrukeren å ta det imot når det er så mye forskjellig."*

En av deltakerne bekymret seg blant annet over at det på sikt kunne bli slik at noen leverandører av mobilbetalingsapplikasjoner ville få såpass stor markedsmakt at de kunne få monopol på visse utsalgssteder, slik at man ble tvunget til å laste ned deres alternativ for å kunne handle.

*"[…] etter hvert så vil det jo kunne være ting som jeg har lyst til å kjøpe noe av som bare aksepterer betaling gjennom for eksempel Facebook."*

**Transaksjonsbekvemmelighet**

Deltakerne hadde mange synspunkt knyttet til autentisering. Det kom tydelig frem at det på tross av sikkerhetsproblematikk var mange bekvemmelighetsfordeler knyttet til blant annet å ha få passord eller PIN-koder. Dette gjaldt også muligheten til å benytte seg av "husk min innloggingsinformasjon".

*"Jeg foretrekker de appene som husker påloggingsinformasjonen min."*

*"Du vil ikke trykke inn bankkortinformasjonen din hver eneste gang."*

*"Jeg ender veldig ofte i den der "glemt passord". Der jeg har måttet lage noe nytt, og det ikke er noen av de kombinasjonene jeg vanligvis har, så husker jeg ikke."*

*"Ja, det er jo derfor jeg har endt opp med å ha så mange like passord. Fordi at det er akkurat det der som skjer. Det er så mange plattformer jeg skal inn på, og det er derfor jeg setter på pris på sånn Vipps med en, med tommelen min der."*

**Nyttebekvemmelighet**

Deltakerne ble bedt om å beskrive hvordan selve betalingen i en mobilbetalingsapplikasjon burde bli utført på mest mulig bekvemmelig måte. De diskuterte en del rundt selve designet og hvordan grensesnittet burde være utformet, for eksempel at applikasjonen minnet om andre applikasjoner de hadde benyttet. Noe annet som var viktig for dem var at selve betalingen krevde få handlinger og var rask gjennomførbar. De snakket også om at det var gunstig at mobilbetalingsapplikasjonen kunne registrere kjøp hos forhandlere hvor de hadde kundefordeler eller lojalitetsprogram.

*"Enkelt design"*

*"At det minner om andre apper man bruker"*

*"Få klikk!"*

*"Alt samlet på en dings."*

*"Alle medlemsskapene du er med i for eksempel, som er, man er jo gjerne medlem av ulike klesbutikker og så videre. Å ha det i den appen, at du har kontroll over alt."*

**Postnyttebekvemmelighet**

Da deltakerne diskuterte om hvorvidt de mente at det var bekvemmelig at en mobilbetalingsapplikasjon sendte dem forslag til andre tjenester, basert på deres forbrukermønster eller geografiske lokasjon, kom det frem at det var store individuelle forskjeller.

*"Jeg hadde blitt helt forstyrret i livet mitt altså. […] det er nok forstyrrelser som det er. Så det hadde blitt veldig invaderende, at jeg ikke kunne tusle en runde i byen uten å liksom få 40 varsler."*

*"Jeg syns det er ubehagelig mye, sånn personalisert reklame."*

*"Hvis jeg melder meg på ting og gir fra meg informasjonen så forventer jeg nesten at noen skal bruke den dataen til om det er remarketing eller hva det skal være, så jeg blir ikke irritert."*

*"Det er det jeg egentlig setter pris på. Altså jeg godtar bevisst med at jeg vet det, så får jeg reklame som jeg vet at passer til meg. Og da kanskje det dukker opp noe jeg har lyst til å kjøpe, hvis jeg ikke gjorde det ville jeg gått glipp av."*

## 3.2 Måling av begrepet sikkerhet

Funnene fra fokusgruppene ga oss en oversikt over hvordan deltakerne opplevde sikkerhet i mobilbetalingsapplikasjonene de allerede hadde testet, hva de oppfattet som viktig for at en mobilbetalingsapplikasjon skulle være sikker og hvordan de forholdt seg til å oppgi personopplysninger. Det ble avdekket fire former for sikkerhet (Generell oppfatning av sikkerhet, Offentlig regulering og lovverk, Sikkerhetstiltak fra leverandørs side, Sikkerhetstiltak som forbrukeren selv kan utføre) basert på samtalene, men vi har valgt å ikke måle Generell oppfatning av sikkerhet i spørreskjemaet. Grunnen til dette er at det er vanskelig å direkte knytte utsagnene opp mot mobilbetalingsapplikasjoner, og fordi vi anser det som lite konkret. Utsagn fra deltakerne som ble plassert under hver kategori ble benyttet til å formulere ulike påstander til spørreskjemaet, og på denne måten operasjonalisere de tre kategoriene basert på fokusgruppene.

**Sikkerhet knyttet til offentlig regulering og lovverk**

I fokusgruppene kom det frem at mange av deltakerne satt med antakelser om at det fantes regelverk som tok dem i vare dersom de skulle bli utsatt for ondsinnede angrep. Svindel ble presentert som den største bekymringen blant deltakerne. Det ble også avdekket at det var et skille i oppfatningen av regelverk som forhindret slike angrep, og regelverk som beskyttet dem etter et potensielt angrep. I spørreskjemaet ble derfor betydningen av sikkerhet knyttet til offentlig regulering og lovverk målt med to påstander, henholdsvis hvor viktig det var med et offentlig regelverk som forebygget, og hvor viktig det var med et offentlig regelverk som beskyttet mot svindel i mobilbetalingsapplikasjoner.

- Det er viktig for meg at det eksisterer et offentlig regelverk som forebygger ondsinnede angrep i en mobilbetaling
- Det er viktig for meg at det eksisterer et offentlig regelverk som beskytter meg dersom jeg blir utsatt for ondsinnede angrep i en mobilbetaling

**Sikkerhetstiltak fra leverandørens side**

Fokusgruppene diskuterte forskjellige kriterier for opplevd sikkerhet med hensyn til hva leverandøren av en mobilbetalingsapplikasjoner kunne tilby dem, og hva som skulle til for at de hadde tillit til leverandøren. Temaet skapte stort engasjement og det ble samlet mange utsagn. Hovedpunktene som gjentok seg ble formulert som seks påstander knyttet til forskjellige aspekter ved temaet. Sikkerhetstiltak fra leverandørs side ble operasjonalisert med følgende faktorer; sikker innlogging; at applikasjonen ikke får tilgang til andre applikasjoner på mobilenheten; at applikasjonen var utgitt av en norsk aktør; at applikasjonen var helt eller delvis eid av en bank; at leverandør sendte påminnelser om å endre innloggingsinformasjon; at applikasjonen viste kjøpsdetaljer før transaksjonen ble gjennomført.

- Det er viktig for meg at det finnes en sikker innloggingsmetode, som hindrer andre i å få tilgang til min mobilbetalingsapplikasjon (f. eks. PIN-kode, Passord, Bank ID på mobil)
- Det er viktig for meg at mobilbetalingsapplikasjonen ikke får tilgang til andre applikasjoner på min smarttelefon

- Det er viktig for meg at leverandøren av en mobilbetalingsapplikasjon er helt eller delvis eid av en bank
- Det er viktig for meg at en mobilbetalingsapplikasjon er utgitt av en norsk leverandør
- Det er viktig for meg å få en oversikt over varene/tjenestene jeg skal kjøpe, samt sum, før jeg gjennomfører en betaling i en mobilbetalingsapplikasjon
- Det er viktig for meg at en mobilbetalingsapplikasjon sender meg regelmessige påminnelser om å endre innloggingsinformasjon.

**Sikkerhetstiltak som forbrukeren selv kan utføre**

Deltakerne i fokusgruppene ble spurt om hva de selv kunne gjøre for å øke sikkerheten i en mobilbetalingsapplikasjon. Hovedtemaene i samtalen her dreide seg om å lese vilkårene til leverandøren før nedlasting eller bruk av en mobilbetalingsapplikasjon, samt kompleksiteten i innloggingsinformasjonen og hvor ofte den ble endret. Det ble på bakgrunn av dette formulert tre påstander som kunne måle hvor viktig respondentene av spørreskjemaet anså egne sikkerhetstiltak; hvor viktig det var å lese vilkår; hvor viktig det var å endre PIN-koder ofte; hvor viktig det var å benytte ulike PIN-koder.

- Det er viktig for meg å lese vilkår før jeg tar i bruk en mobilbetalingsapplikasjon
- Det er viktig for meg å benytte ulike PIN-koder i ulike mobilbetalingsapplikasjoner
- Det viktig for meg å endre PIN-koder ofte (med ofte menes 2 eller flere ganger i året)

## 3.3 Måling av begrepet bekvemmelighet

Utsagnene fra samtalene i fokusgruppene ble kategorisert med hensyn til de fem formene for bekvemmelighet i tjenestebekvemmelighetskonstruksjonen (Berry, Seiders og Grewal, 2002, s. 6-8). På lik linje som under sikkerhet ble utsagn som minnet om andre, eller gjentok seg, benyttet til å operasjonalisere de fem formene for bekvemmelighet og formulere påstander til spørreskjemaet.

**Beslutningsbekvemmelighet**

Forbrukernes oppfatninger av hva som er beslutningsbekvemmelighet og hvor viktig det er for dem ble i fokusgruppene undersøkt ved å spørre deltakerne om hvordan de gjorde kjøps- eller nedlastningsbeslutninger, og hvilke faktorer som var viktigst for dem og krevde minst tid og kognitiv innsats når de skulle anskaffe en mobilbetalingsapplikasjon. Deltakerne delte

flere synspunkt, men mest fremtredende var at de fattet beslutninger basert på gode eller dårlige omtaler av applikasjonen. I spørreskjemaet ble derfor begrepet beslutningsbekvemmelighet målt ved en påstand om hvor viktig det var at en mobilbetalingsapplikasjon hadde gode kundeomtaler.

- Det er viktig for meg at en mobilbetalingsapplikasjon har gode kundeomtaler

**Tilgangsbekvemmelighet**

I fokusgruppene ble tilgangsbekvemmelighet undersøkt gjennom åpne og generelle spørsmål om hva som definerer bekvemmelighet i mobilbetalingsapplikasjoner. På bakgrunn av litteraturen og utsagnene i fokusgruppen ble det ansett mest hensiktsmessig å måle tilgangsbekvemmelighet gjennom spørreskjemaet ved en påstand om hvor viktig det var at en mobilbetalingsapplikasjon kunne benyttes i mange utsalgssteder.

- Det er viktig for meg at en mobilbetalingsapplikasjon kan benyttes i mange utsalgssteder

**Transaksjonsbekvemmelighet**

Ettersom mobilbetalingsapplikasjoner så langt tilbys gratis til forbrukere, er tiden og innsatsen knyttet til autentisering blitt benyttet for å måle transaksjonsbekvemmelighet. I fokusgruppene ble deltakerne spurt om deres oppfatninger rundt bruk av tid og innsats knyttet til forskjellige autentiseringsmetoder, samt oppfatninger av bekvemmelighet i tjenester som tilbyr å huske forbrukerens betalings- eller innloggingsinformasjon. De førstnevnte tema ble vurdert som mer relevant for å måle forbrukerens egne sikkerhetstiltak. I spørreskjemaet ble transaksjonsbekvemmelighet målt ved en påstand som omhandlet muligheten til å benytte seg av "husk min innloggingsinformasjon"-tjenester, ettersom at dette vil kunne spare forbrukerens bruk av tid og kognitiv innsats på å memorere denne typen informasjon.

- Det er viktig for meg å benytte meg av "husk min innloggingsinformasjon" i mobilbetalingsapplikasjoner

**Nyttebekvemmelighet**

For å definere nyttebekvemmelighet ble fokusgruppene blant annet bedt om å beskrive hvordan en mobilbetaling kunne gjennomføres på mest mulig bekvemmelig måte. I spørreskjemaet ble det benyttet to påstander for å måle nyttebekvemmelighet, hvor den ene dreide seg om hvor viktig det var at en mobilbetaling kan gjennomføres med få klikk, og den andre målte viktigheten av at mobilbetalingsapplikasjonen kunne kommunisere med andre applikasjoner på smarttelefonen.

- Det er viktig for meg at en mobilbetalingsapplikasjon krever få klikk for å gjennomføre en betaling
- Det er viktig for meg at en mobilbetalingsapplikasjon kan kommunisere med andre applikasjoner på min smarttelefon (f. eks. applikasjoner med lojalitetsprogram)

**Postnyttebekvemmelighet**

Postnyttebekvemmelighet ble i fokusgruppene undersøkt ved å stille deltakerne spørsmål om hvordan de opplevde aktiviteter initiert av leverandøren basert på deres bruk av mobilbetalingsapplikasjonen. På bakgrunn av utsagnene ble det i spørreskjemaet benyttet to påstander for å måle dette. En av påstandene dreide seg om at mobilbetalingsapplikasjonen sendte push-varsler om for eksempel gode tilbud basert på stedtjenester, og den andre handlet om at mobilbetalingsapplikasjonen benyttet brukerens forbrukermønster til å gi dem personalisert reklame.

- Det er viktig for meg at en mobilbetalingsapplikasjon sender meg push-varsler (f. eks. gode tilbud basert på stedtjenester)
- Det er viktig for meg at en mobilbetalingsapplikasjon sender meg reklame basert på mitt forbrukermønster

## 3.4 Antakelsene som spørreskjemaet skal teste

Basert på litteraturgjennomgang og fokusgruppene har vi formulert seks antakelser som spørreskjemaet tar sikte på å bekrefte eller avkrefte i *5.0 Funn*. Hvorvidt antakelsene kan bekreftes eller avkreftes skal så benyttes for å diskutere utredningens problemstilling.

**A1: For millennials er offentlige reguleringer og lovverk viktigere enn sikkerhetstiltak fra leverandørs side.**
På bakgrunn av utsagnene i fokusgruppene vil vi anta at millennials forventer at det offentlige tar dem i vare, og at dette vil være viktigere enn at tjenesteleverandørene har høy sikkerhet.

**A2: For millennials er offentlige reguleringer og lovverk viktigere enn sikkerhetstiltak som forbruker selv kan utføre.**
På bakgrunn av utsagnene i fokusgruppene vil vi anta at millennials forventer at det offentlige tar dem i vare, og at dette vil være viktigere enn det å utføre sikkerhetstiltak selv.

**A3: Sikkerhetstiltak fra leverandørs side er viktigere enn sikkerhetstiltak som forbruker selv kan utføre.**
Tillit til leverandør var viktig i fokusgruppene, og vi antar at dette vil være viktigere for millennials enn å selv utføre sikkerhetstiltak.

**A4: Bekvemmelighet er like viktig i alle faser.**
Ettersom at bekvemmelighet i fokusgruppene var viktigere enn sikkerhet for millennials vil vi fremme antakelsen om at det er like viktig fra beslutning til postnytte.

**A5: Pushvarsler basert på tjenester og personalisert reklame vil for millennials oppleves som en postnyttebekvemmelighet.**

I bekvemmelighetslitteraturen er postnyttestadiet noe som forbrukere vil foretrekke å ikke forholde seg til med mindre det tilfører merverdi til tjenesten. I fokusgruppene var deltakerne splittet i meningene om hvorvidt push-varsler og personalisert reklame basert på deres kjøp var bekvemmelig, altså tilførte en merverdi. Vi ønsker derfor å teste dette gjennom spørreskjemaet.

**A6: For millennials er bekvemmelighet viktigere enn sikkerhet**
På bakgrunn av tidligere forskning, uttalelser fra individer i bransjen (Stefanovic og Ribe, 2017, s. 44) og utsagnene i fokusgruppene antar vi herved at millennials vekter bekvemmelighet høyere enn sikkerhet i mobilbetalingsapplikasjoner.

# 4.0 Metode

I dette kapittelet vil vi presentere vårt forskningsdesign og vår strategi. Deretter vil vi begrunne fremgangsmåten i spørreskjemaet, herunder utvalg og populasjon, samt kvalitet, reliabilitet og validitet i skjemaet.

## 4.1 Forskningsdesign og strategi

Utredningens problemstilling har som mål å undersøke forbrukerholdninger knyttet til sikkerhet og bekvemmelighet i en hittil tilnærmet ikke-eksisterende tjeneste og hvor det finnes lite eksisterende forskning. Den overordnede planen for hvordan denne problemstillingen skulle undersøkes og besvares, selve forskningsdesignet (Saunders, Lewis og Thornhill, 2016, s. 163), måtte derfor vurderes på bakgrunn av hva som var tilgjengelig av litteratur. For begrepet bekvemmelighet eksisterte det et rammeverk som kunne benyttes som et utgangspunkt for å kvantitativt, gjennom et spørreskjema, samle inn data om målgruppens holdninger. Dette var derimot ikke tilfellet for det andre begrepet, sikkerhet, men dette løste vi gjennom samtaler i fokusgrupper, hvor representanter for målgruppen bidro til å definere ulike former for opplevd sikkerhet. Utredningens forskningsmetode er derfor å gjøre datainnsamling gjennom et spørreskjema, hvor respondenter rangerer ulike utsagn knyttet til de to begrepene basert på eksisterende litteratur og bidraget fra fokusgruppene. Således benyttes en deduktiv forskningsstrategi (Saunders, Lewis og Thornhill, 2016, s. 145), hvor vi søker å verifisere antakelser basert på eksisterende litteratur og fokusgruppesamtaler.

## 4.2 Spørreskjema

Spørreskjemaet ble utviklet i Qualtrics og distribuert gjennom sosiale medier og NHH sin studentportal Canvas. Under følger begrunnelse for og gjennomføring av valg knyttet til utvalg, datainnsamling og vurdering av reliabilitet og validitet.

### 4.2.1 Utvalg og populasjon

Det vil i en masterutredning være vanskelig, med tanke på tidsbruk og midler, å skaffe et utvalg som er stort nok til å representere samtlige millennials. Utvalget som ble brukt i spørreskjemaet var studenter ved Norges Handelshøyskole og Handelshøyskolen BI Campus

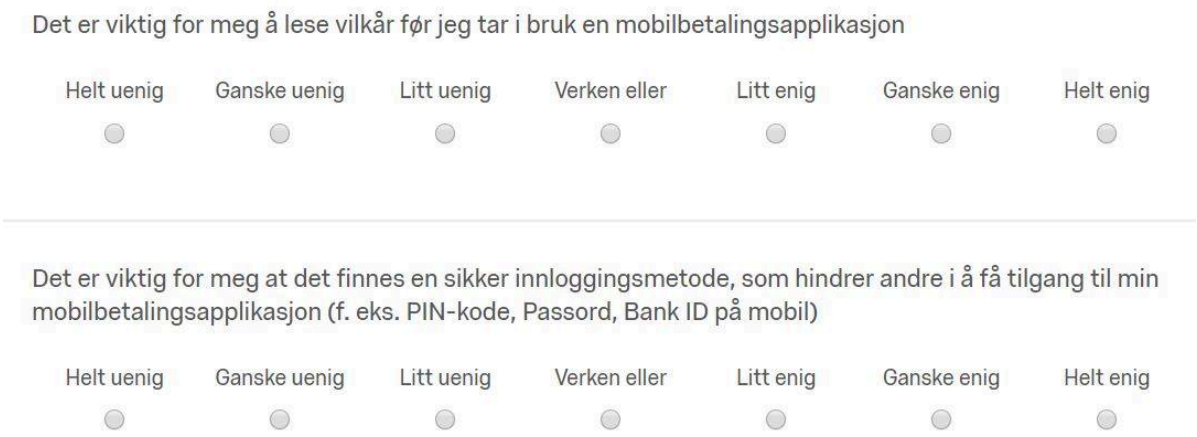
Bergen. Vi vurderer det dit hen at dette er en gruppe mennesker som kan representere en populasjon bestående av millennials i Norge. Vi antar at mobilbetalingsapplikasjoner yter den samme formen for tjeneste til forbrukere uavhengig av akademisk bakgrunn. Økonomistudenter antas også å i stor grad kunne representere en gjennomsnittsforbruker som ikke har tung innsikt i verken bekvemmelighet eller det tekniske sikkerhetsaspektet, slik som eksempelvis en IT- eller grafisk design-student vil ha.

Det er dog en forskjell mellom studenter ved de to utdanningsinstitusjonene og øvrige studenter i Norge hva angår kjønn. Andelen kvinner som ble tatt opp ved Norges Handelshøyskole i 2017 var 38,7% (Norges Handelshøyskole, 2018) og 47,5% ved Handelshøyskolen BI Campus Bergen (Handelshøyskolen BI, u.å). Den totale andelen kvinnelige studenter i Norge i 2017 var 59% (Statistisk Sentralbyrå, 2018). Vi vil imidlertid hevde at denne forskjellen ikke vil påvirke generaliserbarheten mellom utvalget og populasjonen i stor grad. Tidligere forskning har vist at forskjellen mellom kvinner og menn i milleniumsgenerasjonen ikke nødvendigvis er så stor som man tidligere har antatt. Venkatesh, Thong og Xu (2012, s. 162) påpeker at forskjellen mellom kjønnene vil være av større betydning jo eldre respondentene er. Masrom (2007, s. 6) hevder at variabelen kjønn ikke har en signifikant betydning for forbrukeres holdninger og intensjoner om å ta i bruk ny teknologi. Videre viser Lenhart, Purcell, Smith og Zickuhr (2010, s. 23) at det ikke er store forskjeller mellom hva menn og kvinner deler på internett, herunder personlig informasjon.

### 4.2.2 Spørreundersøkelsens design og kvalitet

For å sikre validitet og reliabilitet i dataene som ble samlet inn ble spørreskjemaets design pretestet, og utformingen av påstandene revidert gjennom ytterligere pretesting og diskusjon med veileder.

I pretesten av spørreundersøkelsen ble det benyttet et matrise-design. Noen av tilbakemeldingene på dette designet var negative, hvilket samstemmer med hva Dillman et al. (referert til i Saunders, Lewis og Thornhill, 2016, s. 460) bemerker om at respondenter kan ha vanskeligheter med å forstå slike typer design. Det ble derfor vurdert mest hensiktsmessig å designe undersøkelsen på en mer adskilt, horisontal måte, som vist i figuren under.




***Figur 4:*** *Design i Qualtrics*

I spørreskjemaet ble det benyttet en Likert-skala ettersom det er hensiktsmessig å bruke rangering når man skal innhente data om holdninger (Saunders, Lewis og Thornhill, 2016, s. 457). Det ble valgt syv punkter for å fange opp flest mulige nyanser i svarene. Vi valgte å benytte oddetall for å gjøre det mulig for respondentene å velge et nøytralt punkt dersom de verken var enig eller uenig i utsagnene. Vi formulerte alternativene slik at rangeringen var balansert, altså at de mulige svaralternativene ble reflektert i like stor grad på hver side av det nøytrale punktet.

Spørreskjemaet ble innledet med de demografiske variablene kjønn og alder. Alder ble spurt om for å sikre at vi utelukket eventuelle respondenter som ikke tilhørte kategorien millennials. Det ble også stilt et spørsmål til respondentene om de hadde benyttet seg av tjenester som Vipps eller Paypal den siste måneden for å skille mellom respondenter som er hyppige brukere og de som ikke er det. Deretter ble påstandene som omhandlet sikkerhet og bekvemmelighet introdusert.  En fullstendig oversikt påstander kan finnes i Appendikset.

Respondentene ble bedt om å vurdere 18 påstander og vi antok at det var en mengde som gjorde at det var liten sannsynlighet for at respondentene ikke fullførte undersøkelsen. I Qualtrics la vi inn en binding slik alle påstandene måtte krysses av før respondenten kunne gå videre, dette kan ha vært en faktor som økte sannsynligheten for at respondentene "hoppet av". For at respondentene skulle forstå påstandene i henhold til vår intensjon ble definisjonene av bekvemmelighet og sikkerhet lagt inn i skjemaet. Dette bidro til at vi sikret

oss de data som vi trengte ved at respondentene fikk tilstrekkelig informasjon om temaene (Saunders, Lewis og Thornhill, 2016, s. 450).

### 4.2.3 Reliabilitet og validitet i spørreskjemaet

For å vurdere reliabiliteten i spørreskjemaet har vi valgt å teste den interne konsistensen ved å anvende Cronbachs alfa (Saunders, Lewis og Thornhill, 2016, s. 451). Resultatene fra testen vil bli presentert i *5.0 Funn* og tatt hensyn til i *6.0 Diskusjon*.

For å sikre høyest mulig validitet i vårt studie har vi benyttet samtalene i fokusgruppene til å operasjonalisere begreper som kan måle hvor viktig henholdsvis sikkerhets- og bekvemmelighetsaspektetene er for forbrukerne. Ved å kombinere dette med litteraturgjennomgangen anser vi innholdsvaliditen som god ettersom påstandene i spørreskjemaet i tilstrekkelig grad dekker problemstillingen. Utsagnene fra fokusgruppene ble gjennomgått flere ganger i forkant av påstandsformulering og utsendelsen av spørreskjemaet. Disse er utførlig drøftet i *3.4 Måling av begrepet sikkerhet* og *3.5 Måling av begrepet bekvemmelighet.* I tillegg til dette har formuleringen av påstandene blitt nøye gjennomgått med veileder for masterutredningen.

# 5.0 Funn

I dette kapittelet vil vi presentere en oversikt over funnene fra spørreskjemaet og deretter vurdert opp mot antakelsene som er presentert under *3.5 Antakelsene som spørreskjemaet skal teste.*

## 5.1 Spørreskjema

Av 138 respondenter var det 104 som fullførte undersøkelsen. Vi valgte å eliminere de ufullførte svarene fra analysen. Kjønnsfordelingen var henholdsvis 68 kvinner og 36 menn, men som presisert under *4.2.5 Utvalg og populasjon* skal dette ikke ha påvirkningskraft på generaliserbarheten. På tross av at Likert-data i noen tilfeller kan analyseres som nominaldata, er det bred enighet om at de stort sett bør tolkes som ordinaldata (Wadgave og Khairnar, 2016, s. 67). Vi valgte å studere medianene ettersom det vil være vanskelig å gi en tolkning av gjennomsnitt ut ifra gradene av enig eller uenig. Under følger en oversikt over den deskriptive statistikken, som deretter presenteres som funn i forbindelse med antakelsene. En full oversikt over fordelingen av svar fra spørreskjema kan finnes i Appendikset.

| Helt uenig | Ganske uenig | Litt uenig | Verken eller | Litt enig | Ganske enig | Helt enig |
|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |

***Figur 5:*** *Likertskala*

| *Sikkerhet* | Gjennomsnitt | Median | Minimum | Maksimum |
|---|---|---|---|---|
| **Offentlig regulering** | 6,62 | | | |
| Forebygging | 6,57 | 7 | 4 | 7 |
| Beskytter | 6,67 | 7 | 4 | 7 |
| **Leverandør** | 5,17 | | | |
| Sikker innlogging | 6,68 | 7 | 1 | 7 |
| Applikasjonstilgang | 5,45 | 6 | 1 | 7 |
| Eierskap: Bank | 5,08 | 5 | 1 | 7 |
| Eierskap: Norsk | 4,64 | 5 | 1 | 7 |
| Påminnelser | 4 | 4 | 1 | 7 |
| Oversikt | 6,45 | 7 | 2 | 7 |
| **Forbruker** | 3,38 | | | |
| Lese vilkår | 3,15 | 3 | 1 | 7 |
| Ulik PIN-kode | 4,3 | 4 | 1 | 7 |
| Endre PIN-kode | 2,68 | 2 | 1 | 7 |

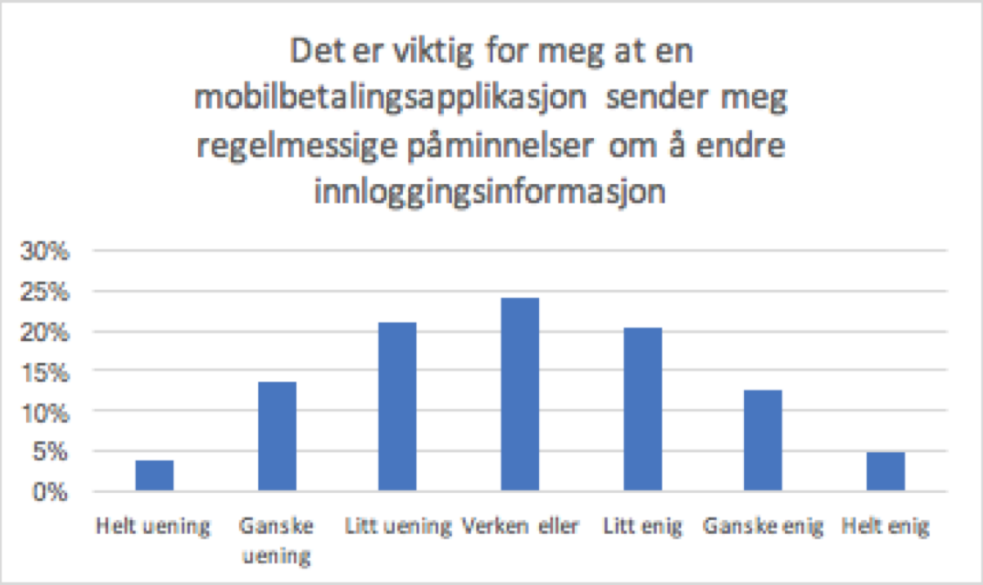
***Figur 6:*** *Funn – Sikkerhet*

| *Bekvemmelighet* | Gjennomsnitt | Median | Minimum | Maksimum |
|---|---|---|---|---|
| **Beslutningsbekvemmelighet** | 5,85 | | | |
| Kundeomtaler | 5,85 | 5 | 2 | 7 |
| **Tilgangsbekvemmelighet** | 6,21 | | | |
| Utsalgssteder | 6,21 | 6,5 | 2 | 7 |
| **Transaksjonsbekvemmelighet** | 4,79 | | | |
| Husk min innloggingsinfo. | 4,79 | 5 | 1 | 7 |
| **Nyttebekvemmelighet** | 5,335 | | | |
| Få klikk | 6,11 | 6 | 2 | 7 |
| App-kommunikasjon | 4,56 | 5 | 1 | 7 |
| **Post-nyttebekvemmelighet** | 2,555 | | | |
| Push-varlser | 2,86 | 3 | 1 | 7 |
| Personalisert reklame | 2,25 | 2 | 1 | 7 |

***Figur 7:*** *Funn – Bekvemmelighet*

**A1: For millennials er offentlige reguleringer og lovverk viktigere enn sikkerhetstiltak fra leverandørs side**

Under påstanden om hvorvidt det var viktig at et det eksisterer et offentlig regelverk som henholdsvis forebygger og beskytter forbrukere fra ondsinnede angrep i mobilbetaling var 69 % og 76 % av respondentene *helt enig*. Det var to respondenter som svarte *verken eller* under begge faktorene, og ingen var noen grad uenig. Under påstandene om leverandørs sikkerhet var det større variasjon, fra *helt uenig* til *helt enig*, og en samlet lavere median som er noe høyere enn *litt enig*. Det er dog en forskjell i variablene, og vi ser at påstanden som dreier seg om at leverandøren tilbyr en sikker form for innlogging har et høyere gjennomsnitt enn begge påstandene som måler hvor viktig offentlig regulering og lovverk er.  77 % av respondentene var *helt enig* hva angår viktigheten av sikker innlogging. Medianen til faktoren som dreier seg om at applikasjonen gir brukeren en oversikt over kjøpet før betaling gjennomføres, måles også til *helt enig*. De øvrige faktorene under leverandørs sikkerhet har medianer fra *verken eller* til *ganske enig*, som trekker gjennomsnittet ned. Faktoren som målte hvor viktig det var at applikasjonen sendte dem påminnelser om å endre innloggingsinformasjon var tilnærmet normalfordelt.




**Figur 8:** Funn "Regelmessige påminnelser"

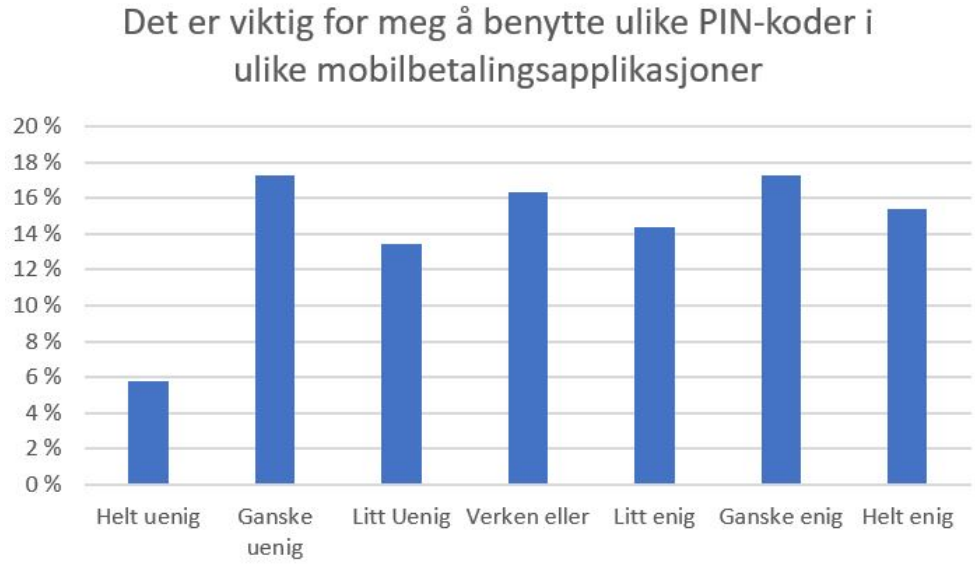
Ut ifra variasjonen i de forskjellige enhetene er det ikke grunnlag for å bastant hevde at antakelsen stemmer, men den kan heller ikke avkreftes.

**A2: For millennials er offentlige reguleringer og lovverk viktigere enn sikkerhetstiltak som forbrukerne selv kan utføre.**

| | |
|---|---|
| Helt uening | 5,77 % |
| Ganske uening | 17,31 % |
| Litt uening | 13,46 % |
| Verken eller | 16,35 % |
| Litt enig | 14,42 % |
| Ganske enig | 17,31 % |
| Helt enig | 15,38 % |

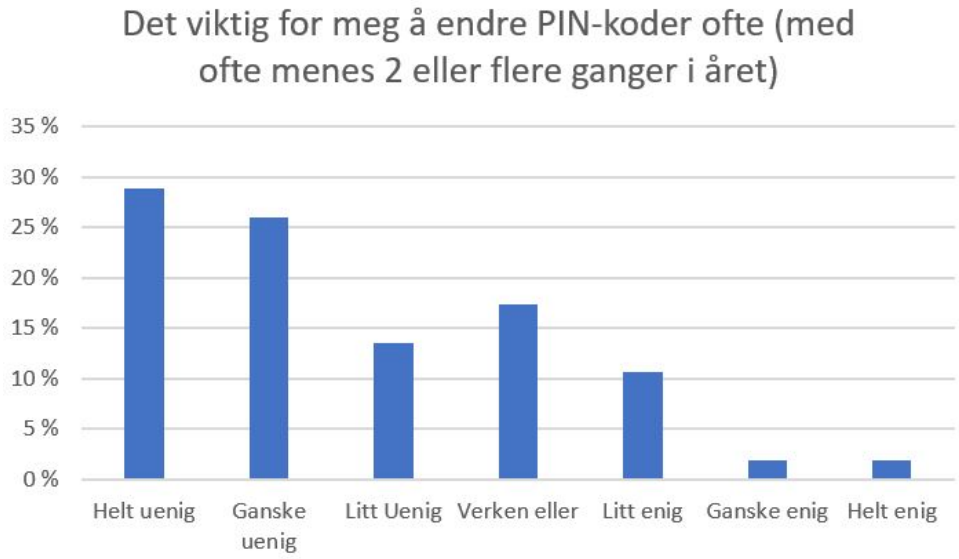
**Figur 9:** Funn - Prosentvis fordeling "endre PIN-koder"

På spørsmålet om det er viktig for respondentene å endre sine PIN-koder ofte er svarene meget sprikende. Hvert av svaralternativene fra *ganske uenig* til *helt enig* har en svarprosent på mellom 13 og 17. Det er kun i underkant av 6% av respondentene som mener at det ikke er viktig å skifte PIN-koder ofte.




***Figur 10:*** *Funn "Ulike PIN-koder"*

Under påstanden som handler om hvor viktig det er å lese vilkårene før man tar i bruk en mobilbetalingsapplikasjon var 60 % av respondentene innenfor uenig-området. Hva angår å endre PIN-koder var andelen innenfor enig-området på knappe 14 %, med en tydelig tendens mot å være uenig i påstanden.




***Figur 11:*** *Funn "Endre PIN-koder"*

Antakelsen om at offentlig regulering og lovverk er viktigere enn sikkerhetstiltak forbrukerne selv kan utføre kan ut ifra funnene i undersøkelsen bekreftes.

**A3: Sikkerhetstiltak fra leverandørs side er viktigere enn sikkerhetstiltak som forbruker selv kan utføre**

Faktorene som dreier seg om leverandørs sikkerhet scorer nesten utelukkende høyere i viktighet enn faktorene som dreier seg om tiltak forbrukerne selv kan utføre. Det er likevel ett unntak. Faktoren som dreier seg om at leverandør sender påminnelser om å bytte innloggingsinformasjon og faktoren som dreier seg om å benytte seg av ulike passord har begge medianer på *verken eller*. På tross av dette anser vi antakelsen som gyldig ettersom at det er vesensforskjeller i de øvrige variablene. Antakelsen kan derfor ut ifra funnene i spørreundersøkelsen bekreftes.

**A4: Bekvemmelighet er like viktig i alle faser**

Svarene fra spørreundersøkelsen viser at postnyttebekvemmelighet ikke er viktig for respondentene. Om lag 50% av respondentene svarte at de var *helt* eller *ganske uenig* i påstanden om hvorvidt det er viktig for dem å motta push-varsler med gode tilbud basert på stedtjenester. Den samme tendensen viser seg i svarene til påstanden om respondentene ønsker å motta personalisert reklame, her svarer drøye 64% at de er *helt* eller *ganske uenig*.

I de øvrige fasene for bekvemmelighet: beslutnings-, tilgangs-, transaksjons- og nyttebekvemmelighet svarer respondentene at bekvemmelighet er viktig for dem.

Tilgangsbekvemmelighet skiller seg noe ut med en median på *ganske enig*, som er høyere enn i de øvrige faktorene. I snitt er nesten 80% av respondentene *helt* eller *ganske enig* i at tilgang er en viktig bekvemmelighetsfaktor. Transaksjonsbekvemmelighet har en median innenfor *enighets*-området, men gjennomsnittet er noe lavere enn i de øvrige faktorene. De to faktorene som synes å være viktigst for respondentene er at betalingsapplikasjonen kan benyttes i mange utsalgssteder og at det kreves få klikk for å gjennomføre en betaling.

**A5: Push-varsler basert på tjenester og personalisert reklame vil for millennials oppleves som en postnyttebekvemmelighet**


***Figur 12:*** *Funn "Push-varsler"*

På spørsmålet om hvorvidt det er viktig for respondentene å bli tilsendt push-varsler fordeler 63% seg over *litt, ganske* eller *helt uenig.* Drøye 21% av respondentene stiller seg likegyldig til spørsmålet, videre er omtrent 11% av respondentene *litt enig.*


***Figur 13:*** *Funn "Reklame basert på forbrukermønster"*

Majoriteten av respondentene er *uenig* i spørsmålet vedrørende å motta reklame basert på sitt forbrukermønster. Hele 41% svarer at de er *helt uenig* og i underkant av 8% av respondentene svarer at de i en eller annen grad er *enig,*

Faktorene som var ment til å måle postnyttebekvemmelighet i undersøkelsen hadde begge medianer som differensierer seg i stor grad fra de øvrige faktorene som måler bekvemmelighet. Med utgangspunkt i litteraturen om postnyttebekvemmelighet, samt graden av *uenighet* i hvorvidt det var viktig i spørreskjemaet, tyder på at det å motta push-varsler og reklame kan opplevelses som ubekvemmelig i mobilbetalingsapplikasjoner for millennials. Dette støttes i tidligere forskning gjort på millennials og mobilapplikasjoner. En undersøkelse fra Oracle viser at 56 % av de spurte millennials ikke liker å motta uoppfordret kommunikasjon i form av push-varsler som for brukeren fremstår som irrelevant (Leggatt, 2015). Vi vil på bakgrunn av dette avkrefte antakelsen og videre anse variablene som er benyttet til å måle postnyttebekvemmelighet heller som et mål på ubekvemmelighet.

**A6: For millennials er bekvemmelighet viktigere enn sikkerhet**

Den samlede medianen for alle bekvemmelighetsfaktorene er *ganske enig* mot den samlede medianen på *litt enig* i sikkerhetsfaktorene. Av denne enkle sammenligningen fremstår det at respondentene faktisk bekrefter antakelsen. Det er likevel noen momenter som bør påpekes. Sikkerhet måles ved flere faktorer enn bekvemmelighet. To av de originale faktorene som målte viktigheten av bekvemmelighet er fjernet, som nevnt i avsnittet over. Det er variasjon i underkategoriene for begge faktorene som måles. Eksempelvis har offentlig regulering og lovverk en median på *helt enig* mot forbrukernes egne sikkerhetstiltak med en median på *litt uenig.* Videre må antakelsenes gyldighet sees opp mot validiteten og reliabiliteten i spørreundersøkelsen. Vi har fastslått at innholdsvaliditeten anses som god, men det er visse forhold som påvirker spørreundersøkelsens reliabilitet. Dette vil bli utredet i det følgende avsnittet.

### 5.1.1 Reliabilitetsresultater

Det ble benyttet Cronbachs alfa for å teste reliabiliteten i spørreundeskjema. Cronbachs alpha ble målt til 0,65 for samtlige faktorer. Ettersom at postnyttefaktorene kan vurderes som mål på ubekvemmelighet valgte vi å fjerne dem fra den helhetlige analysen. Dette ga en Cronbachs alpha på 0,67 (se Appendikset). Kriteriet for at reliabiliteten skal være akseptabel er en alpha på 0,7. Undersøkelsens reliabilitet vil i dette tilfellet måtte vurderes som noe lav. Fremfor å fjerne flere variabler for å oppnå en høyere alpha vurderer vi det slik at respondentene i stor grad vil kunne være påvirket av utenforstående hendelser. Eksempelvis kom det frem i fokusgruppene at sikkerhet ikke var en prioritet for noen av deltakerne

nettopp fordi de ikke hadde opplevd ondsinnede angrep selv. Spørreundersøkelsen ble gjennomført ikke lenge etter det som er blitt omtalt som Facebook-Cambridge Analytica-skandalen (BBC, 2018). Dette er en hendelse som vi antar kan ha påvirket respondentenes tilbøyelighet for å verdsette sikkerhet. Slike eksterne hendelser vil i fremtiden kunne påvirke respondenter dersom spørreskjemaet skulle bli retestet. På tross av en noe lav reliabilitet i spørreskjemaet anser vi likevel datainnsamlingen som et godt grunnlag for å undersøke og diskutere problemstillingen både på grunn av mengden respondenter og nøysomt og omfattende forarbeid.

# 6.0 Diskusjon

I dette kapittelet vil vi på bakgrunn av funnene i spørreskjemaet diskutere de mest fremtredende holdningene blant de spurte millennials hva angår sikkerhet, bekvemmelighet, og avveiningen mellom de to begrepene. Videre skal vi holde dette opp mot tidligere forskning og litteratur. I tillegg til at fokusgruppenes hensikt var å skape operasjonaliserbare definisjoner knyttet til bekvemmelighet og sikkerhet har vi valgt å benytte noen av utsagnene for å ytterligere styrke diskusjonen der det egner seg.

## 6.1 Millennials holdninger til sikkerhet

Vår antakelse da vi startet arbeidet med denne masterutredningen var at millennials sine holdninger til sikkerhet i mobilbetalingsapplikasjoner var av mindre betydning enn deres holdninger og krav til bekvemmelighet. Funnene i spørreskjemaet bekreftet til en viss grad våre antakelser på et overordnet nivå, men vi oppdaget at det var vesensforskjeller i holdningene når sikkerhet som sådan ble nærmere definert og kategorisert.

Det var svært viktig for respondentene av spørreskjemaet at det eksisterte et eksternt sikkerhetssystem som ivaretok dem og forebygget ondsinnede angrep. Deltakerne i fokusgruppene ytret at slike eksterne sikkerhetssystem var noe de hadde tillit til. De hadde ikke bare tillit til offentlig regulering og lovverk, men også tillit til at finansinstitusjoner og banker tok dem i vare. Denne tilliten synes å være en karakteristikk ved milleniumsgenerasjonen. En Gallup-undersøkelse gjort på millennials om datasikkerhet (Fleming og Adkins, 2016) viser at 67 % har høy tillit til sin primærbank, men kun 4 % av dem har høy tillit til sosiale medier. Dette samsvarer med spørreskjemaet vi gjennomførte, hvor 67 % var litt til helt enig i at det var viktig at en bank var involvert på eiersiden i en mobilbetalingsapplikasjon. Da deltakerne i fokusgruppene diskuterte hvem de ønsket som leverandør var det liten tillit til blant annet Facebook og andre sosiale medier: "*[...] jeg kommer ikke til å stole på at de vil mitt beste sånn som jeg tror *ler* banken vil.*" Dette tyder på at millennials har relativt klare holdninger til hvem de opplever at ivaretar deres sikkerhet. Funnene fra spørreskjemaet viser tydelig at den eksterne sikkerheten er viktigere enn tiltak de som forbruker selv kan utføre. Millenniumsgenerasjonens høye tillit til eksterne organisasjoner (Alton, 2017) kan være årsaken til at det er vesentlig mindre viktig for dem å lese leverandørenes vilkår, samt bruke tid og krefter på å jevnlig oppdatere sine passord.

Et par spørsmål som dukket opp etter gjennomføringen av fokusgruppene var: Er millennials klar over potensielle skader ved manglende sikkerhet? Tar de sikkerheten for gitt? Er tilliten til det offentlige og leverandørene et resultat av kunnskap eller mangel på kunnskap? Eller, bryr de seg ikke?

For det første, inngående kjennskap til det tekniske aspektet ved sikkerheten i mobilbetalingsapplikasjoner er, basert på fokusgruppene, ikke allmenkunnskap blant millennials. Det de like fullt har, er god erfaring i å ta beslutninger basert på andre kriterier. De har tillit til kjente merkenavn med store brukermasser. De vet at en svikt i sikkerheten til en online tjenestetilbyder kan føre til tap av brukere, og med det inntekt, og antar derfor at sikkerhet er en viktig prioritet. De forstår forretningsmodellen til denne typen leverandører, fordi de har levd et liv hvor slike aktører alltid har eksistert. Enkelt sagt, de gjennomskuer forsøk på svindel av typen e-poster hvor en "nigeriansk prins" ønsker å overføre et millionbeløp til mottakerens konto. Gruppen millennials som er spurt er bosatt i Norge, et land hvor korrupsjonsnivået er lavt (Transparency International, 2018) og tilliten til det offentlige vil derfor naturlig være på et visst nivå. Sikkerhet er viktig for millennials, men det er ikke nødvendigvis viktig å bruke tid og innsats på å gjøre noe utover det tjenestetilbyderen eller det offentlige allerede har gjort. Videre følger en diskusjon om holdninger til bruk av tid og innsats, selve definisjonen på bekvemmelighet, i de øvrige funksjonene i en mobilbetalingsapplikasjon.

## 6.2 Millennials holdninger til bekvemmelighet

I *5.0 Funn* fremmet vi antakelsen om at bekvemmelighet er like viktig i alle de fem fasene, men ut ifra svarene vi fikk i spørreskjemaet var dette ikke mulig å bekrefte. I fokusgruppene kom det frem ulike holdninger til å motta reklame eller push-varsler basert på stedtjenester og forbrukermønster. En av deltakerne mente at slike virkemidler kunne ha forenklet vedkommendes hverdag, og ville ha satt pris på å få reklame som var tilpasset seg selv som forbruker. En annen av deltakerne var bevisst det faktum at hver gang vedkommende godtok vilkår som innebar at tilbyder ville samle persondata, ville intensjonen være å bruke denne informasjonen i markedsføringsøyemed. Deltakeren stilte seg relativt likegyldig til dette og uttrykte at slike tjenester ikke var viktig. Det var flere av deltakerne i fokusgruppen som stilte seg negativ til innhenting av persondata. Flere hadde inntrykk av at virksomheter som innhentet slik data allerede hadde mer enn nok informasjon om dem som forbruker, og

ønsket ikke å oppgi mer informasjon om seg selv. De deltakerne som var negativ til informasjonsinnhenting ga uttrykk for at de ikke var fortrolig med tilbydernes intensjoner og stilte spørsmål ved dette. Det fremkom også av samtalene at informasjonsinnhentingen er en form for overvåkning som forbruker ikke er seg bevisst. Slik innhenting av informasjon er beskrevet i vilkårene til tjenestetilbyder, men som det fremgår av spørreskjema er det få av de spurte millennials som tar seg tid til å lese disse.

Faktorene som i spørreskjemaet ble benyttet for å måle postnyttebekvemmelighet fremstår som *ikke viktig* for respondentene. Det er dermed ikke sagt at postnyttebekvemmelighet ikke er viktig for millennials. I *5.0 Funn* vurderte vi det slik at faktorene som ble benyttet for å måle dette ikke er å anse som en bekvemmelighet i denne spesifikke typen tjenester. Det kan imidlertid være andre faktorer innenfor postnyttebekvemmelighet som er viktig for forbruker, men som ikke er undersøkt i spørreskjemaet, eksempelvis tilbyders kundeservice. Det faktum at respondentene av spørreskjemaet ikke verdsetter de faktorer av postnyttebekvemmelighet som ble undersøkt kan bekreftes av forskning som tilsier at millennials ikke ønsker uoppfordret kommunikasjon fra applikasjonstilbydere. Dette kan tyde på at mobilbetalingstjenester av den typen som for eksempel Alipay tilbyr ikke er attraktivt for den norske millennial, nettopp fordi disse i stor grad baserer seg på å varsle den enkelte forbruker direkte om tilpassede tilbud eller liknende. Millennials har vokst opp med internett og smarttelefoner og vet hvor de skal finne informasjon om et produkt eller en tjeneste når de trenger den.

Bekvemmelighetsfaktoren som har høyest median, det vil si midt mellom *ganske* og *helt enig*, handler om at mobilbetalingsapplikasjonen må kunne brukes i alle, eller de fleste, utsalgssteder. Dette er gjerne ikke så unaturlig. I fokusgruppene var det flere deltakere som stusset over hvorvidt det var mer bekvemmelig med en mobilapplikasjon fremfor et bankkort. Dersom den ene betalingsformen skal erstatte den andre er det essensielt at den er tilgjengelig i alle utsalgssteder. At selve utførelsen av betalingen krevde få klikk hadde også en høy median, *ganske enig.* Begge disse karakteristikkene handler direkte om å spare tid og krefter i en betalingssituasjon. Forbrukeren må kunne ta frem smarttelefonen sin og benytte seg av en applikasjon som allerede er lastet ned og på kort tid få gjennomført transaksjonen. Blant de spurte i spørreskjemaet var medianen til hvorvidt de ønsket at applikasjonen husket deres innloggingsinformasjon *litt enig*. En slik funksjon er tidsbesparende, og man kan si at

man sparer kognitive krefter på å slippe å huske passord. Fokusgruppene var dog enig om at innloggingsfunksjonen med BankID på mobil var bekvemmelig nok, samtidig som de anså den som sikker.

## 6.3 Millennials avveininger mellom sikkerhet og bekvemmelighet

Når millennials gjør avveininger mellom sikkerhet og bekvemmelighet i bruken av mobilbetalingsapplikasjoner, ser vi flere sammenhenger mellom de ulike faktorene fra spørreskjemaet. I forbindelse med sikkerhet ble det fremmet en påstand om hvorvidt respondentene ønsket å motta påminnelser om utskifting av innloggingsinformasjon, hvor medianen var *verken eller*. Denne påstanden kan sammenlignes med de to spørsmålene i bekvemmelighet som gjelder push-varsler, median *litt uenig,* og personalisert reklame, median *ganske uenig*. Alle disse tre spørsmålene omhandler uoppfordret kommunikasjon fra leverandør. Ut ifra disse påstandene kan vi tolke respondentene dit hen at uoppfordret kommunikasjon fra leverandør som gjelder sikkerhet er viktigere enn kommunikasjon som angår push-varsler og personalisert reklame.

Faktoren "husk min innloggingsinformasjon", median *litt enig*, kan settes opp mot påstanden om sikker innlogging som leverandør tilbyr, median *helt enig*. Sammenligning av disse funnene kan bidra til å oppklare et av spørsmålene som er stilt innledningsvis i dette kapittelet: Har millennials tilstrekkelig kunnskap? Sikkerheten i mobilbetalingsapplikasjoner vil reduseres dersom forbrukere benytter seg av "husk min påloggingsinformasjon", jf. en av deltakerne i fokusgruppen sitt problem med å få dekket sitt tap etter svindel i Paypal. At forbrukerne verdsetter bekvemmeligheten ved å benytte seg av "husk min innloggingsinformasjon" kan tyde på at de ikke kjenner til risiki ved manglende sikkerhet, at de ikke har tilstrekkelig kunnskap om sikkerheten i online betalinger på tross av at det er viktig for dem.

"Husk min innloggingsinformasjon", median *litt enig*, kan også sammenlignes med respondentenes holdninger til det å benytte seg av ulike PIN-koder, median *verken eller*, og å endre PIN-koder, median *ganske uenig*. Å benytte seg av ulike PIN-koder, og å endre disse ved jevne mellomrom, vil øke forbrukernes sikkerhet. Som det fremgår av svarene fra spørreskjemaet er respondentene verken *enig* eller *uenig* i at det er viktig å benytte ulike PIN-koder. Vi kan med dette anta at millennials ikke benytter et stort antall ulike PIN-koder.

Det kan tenkes at en av årsakene til at millennials ikke benytter seg av like mange ulike PIN-koder som foregående generasjoner, er at de er mer fortrolig med å benytte biometriske metoder for innlogging, eksempelvis fingeravtrykk, og verdsetter tiden og innsatsen de sparer ved slike metoder (IBM, 2018). Annen forskning viser også at 45% av millennials skifter passord kun når de må (Intercede, 2015).

Respondentene av spørreskjemaet ble spurt om det var viktig for dem at mobilbetalingsapplikasjonen ikke fikk tilgang til andre applikasjoner på deres smarttelefon. Funnet her var en median på *ganske enig*. De ble også spurt om det var viktig for dem at mobilbetalingsapplikasjonen kunne kommunisere med andre applikasjoner, som for eksempel telefonlister. Her fikk vi en median på *litt enig.* Dette fremstår noe selvmotsigende. Det som bør bemerkes er at respondentene ble introdusert til påstandene på denne måten: "I forbindelse med sikkerhet, vurder følgende påstand" /"I forbindelse med bekvemmelighet, vurder følgende påstand." Dette kan tyde på at forbrukerne må gjøres oppmerksom på at en slik funksjon kan ha sikkerhetsimplikasjoner. Altså, bekvemmeligheten ved at en mobilbetalingsapplikasjon kan benytte seg av kontaktlisten er viktig for millennial-forbrukeren, men det fremstår ikke for dem som en potensiell sikkerhetsfare med mindre de gjøres oppmerksom på at det faktisk kan være det. Ved å benytte seg av en slik funksjon gir forbrukeren ikke bare fra seg egen kontaktinformasjon, men også informasjonen til hele kontaktlisten. Det samme er tilfellet dersom man benytter seg av Facebook- eller Google-konto som autentiseringsmetode i andre applikasjoner, en API-løsning som mange applikasjoner benytter.

For å oppsummere: Ut ifra diskusjonen over kan det tolkes at millennials gjør avveininger på grunnlag av hvorvidt sikkerhetstiltakene oppleves bekvemmelig. En påminnelse fra tjenestetilbyder om å skifte passord vil ikke nødvendigvis oppfattes som ubekvemmelig, på tross av at kommunikasjon initiert av tjenestetilbyder i andre tilfeller ikke er ønskelig. På tross av viktigheten ved at det tilbys sikker innlogging er de spurte millennials likevel tilbøyelig til å benytte seg av at innloggingsinformasjonen kan lagres og huskes, samt unngå å benytte flere ulike PIN-koder, og bekvemmeligheten dette medfører. Det tyder også på at millennials må gjøres bevisst på at det å gi en mobilbetalingsapplikasjon tilgang til andre applikasjoner kan medføre redusert sikkerhet, selv om dette kan øke bekvemmelighet i bruken.

# 7.0 Konklusjon

Denne masterutredningen hadde til formål å undersøke følgende problemstilling: Hvilke holdninger har norske millennials til sikkerhet og bekvemmelighet i mobilbetalingsapplikasjoner? Dette er et samfunnsaktuelt og viktig spørsmål ettersom flere aktører, deriblant Vipps og Apple Pay, denne våren har meldt at de planlegger å tilby slike tjenester til norske forbrukere.

I utvikling av spørreskjemaet har det blitt identifisert tre ulike former for sikkerhetstilnærminger som er relevante for norske millennials i mobilbetalingsapplikasjoner; **Offentlig regulering og lovverk; Sikkerhetstiltak fra leverandørs side; Sikkerhetstiltak som forbruker selv kan utføre**. Funnene i spørreskjemaet har bidratt til å forstå hvilke holdninger norske millennials har til sikkerhet i mobilbetalingsapplikasjoner på et overordnet nivå, samt til de tre ulike formene for sikkerhet. Tjenestebekvemmelighetskonstruksjonens fem faser har også blitt operasjonalisert gjennom fokusgruppene og tilpasset mobilbetalingsapplikasjoner. Gjennom spørreskjemaet har vi funnet hvilke holdninger norske millennials har til bekvemmelighet som sådan i mobilbetalingsapplikasjoner, samt holdninger i de ulike fasene: **Beslutnings-, tilgangs-, transaksjons-, nytte- og postnyttebekvemmelighet**. Vi finner at Henrik Lie-Nielsens påstand "Convenience trumfer sikkerhet når som helst" (Stefanovic og Ribe, 2017, s. 44) til en viss grad kan bekreftes, men at det finnes nyanser i de to begrepene hvor sikkerhet er viktigere enn antatt.

Tidligere forskning og litteratur, kombinert med innsamlingen av data fra målgruppen og en pågående diskusjon i det offentlige rom om temaet mobilbetalingsapplikasjoner, har lagt grunnlaget for vår forståelse av bekvemmelighetsoppfatningene til dagens millennials. Opparbeidet forståelse for hvordan sikkerhetsmekanismer fungerer i mobilbetalingsapplikasjoner gjorde det tydelig i datainnsamlingen at dette ikke er noe den gjengse millennial har innsyn i. Vi oppdaget dog funn som tyder på at sikkerhetsoppfatninger i større grad påvirkes av erfaring og tillit.

Oppsummert ser vi at millennial-forbrukeren gjør en avveining mellom høy bekvemmelighet hva angår tilgang og beslutning om å anskaffe en mobilbetalingsapplikasjon, og det de oppfatter som en sikker tjeneste basert på offentlig regulering og lovverk, samt tillit til

tjenestetilbyder. Basert på funnene våre, samt tidligere forskning, later det til at denne tilliten er såpass sterk blant millennials at de tar valg basert hovedsakelig på bekvemmeligheten i tjenesten, og at en stor brukermasse og en kjent tjenestetilbyder er tilstrekkelig til å dekke sikkerhetsbehovet. Det er viktig for norske millennials at mobilbetalingsapplikasjonen er sikker å bruke, men samtidig er det viktig for millennials at kreves lite tid og innsats fra deres egen side for å styrke denne sikkerheten.

Berry, Seiders og Grewals (2002, s. 4) tjenestebekvemmelighetskonstruksjon har i denne oppgaven blitt benyttet til å direkte omhandle mobilbetalingsapplikasjoner. Det har også blitt utviklet en kategorisering av sikkerhetsaspekter basert på millennial-forbrukernes holdninger. At det er viktig med høy tillit til leverandør i forbindelse med sikkerhet, som har vært tema i tidligere forskning på denne aldersgrupper og deres holdninger til digitale tjenester, har blitt ytterligere styrket gjennom funnene fra spørreskjemaet.

Av praktiske implikasjoner kan funnene være veiledende for eksisterende og nye tjenestetilbydere som ønsker å lansere applikasjoner for mobilbetaling i butikk, spesielt nå som PSD2 tillater tredjepartsaktører. Avveiningene og holdningene blant millennial-forbrukere kan benyttes i utvikling av fremtidige forretningsmodeller. Vi anser sikkerhet som en essensiell del av merkevarebyggingen til fremtidige tjenestetilbydere, men det viktigste, bekvemmelighetsfokuset, må rettes mot brukergrensesnitt og nyttebekvemmelighet.

**Begrensninger og fremtidig forskning**

En tidligere utredning har undersøkt mobilbetaling og adopsjonsproblemer med fokus på et utvalg innenfor millenniumsgenerasjonen (Fjeldheim og Strøm, 2016, s.47-48). Intensjonen i deres arbeid var ikke å undersøke sikkerhet og bekvemmelighet spesielt, men de gjorde likevel funn som tydet på at sikkerhet er et viktig tema blant utvalget de forsket på. Ettersom at sikkerhetsproblematikk har vært en stor del av denne utredningen, og avdekket holdninger blant millennials og deres vekting av temaene, ser vi muligheter for at bekvemmelighetsaspektet i enda større grad kan utredes og forskes på. Det kan gjennomføres mer praktiske eksperimenter hvor brukergrensesnitt i selve applikasjonen kan testes og måles med fokus på tidsbruk og innsats. Dette kan bidra til et tydeligere bilde av forbrukernes bekvemmelighetsbehov. Ettersom mobilbetaling i butikk i skrivende stund er

svært begrenset hadde det vært ønskelig å gjennomføre et lignende forskningsarbeid når løsningene blir mer utbredt. Siden vårt arbeid i hovedsak baserer seg på persepsjoner rundt tilnærmet hypotetiske tjenester, er det mulig at avveiningene vil kunne endres når tjenesten først har blitt tatt i bruk over en periode. Forbrukernes tillit til det offentlige og leverandører kan også forrykkes dersom det oppstår uønskede hendelser knyttet til mobilbetaling i butikk. Begrensninger med tanke på hvorvidt funnene i spørreskjemaet er generaliserbare for norske millennials, og eventuelt post-millennials, utover de spurte i spørreskjemaet, kan eksistere. Vi er likefullt av den oppfatning at kvaliteten på påstandene som er benyttet i skjemaet og antallet respondenter styrker funnenes generaliserbarhet, og at de følgelig er til å stole på.

Det at spørreskjemaets reliabilitet målt ved Cronbachs alpha var noe lav er en svakhet ved forskningen. Dette kan skyldes korrelasjoner som følge av at noen av sikkerhetsfaktorene også fanget opp bekvemmelighetskarakteristikker, og vice versa. I fremtidig forskning kan faktorene som er benyttet i spørreskjemaet videreutvikles og konkretiseres i enda større grad. Det er også en fordel om forskere på et senere tidspunkt kan operasjonalisere postnyttebekvemmelighet fra en annen vinkel, for eksempel ved å undersøke faktorer som kundeservice.

# 8.0 Litteraturliste

Accenture, (u.å.) *Managing Security Threats In A Digital World.* Hentet 07.02.2018 fra https://www.accenture.com/us-en/insight-managing-security-threats-digital-world#block-overview

Agarwal, S., Khapra, M., Menezes, B., og Uchat, N. (2007). Security issues in mobile payment systems. *Indian Institute of Technology, Bombay, India*. 142-152. http://www.908.openacademy.slideshare.csi-sigegov.org/2/14_310_2.pdf

Alton, L. (2017, 26. desember). The 4 Top Security Concerns On The Minds Of Millennials. *Forbes.* Hentet 03.05.2018 fra https://www.forbes.com/sites/larryalton/2017/12/26/the-4-top-security-concerns-on-the-minds-of-millennials/#2115143b7dc7

Amazon (u.å.) *AmazonGo*. Hentet 09.02.2018 fra https://www.amazon.com/b?node=16008589011

Au, Y. A., og Kauffman, R. J. (2008). The economics of mobile payments: Understanding stakeholder issues for an emerging financial technology application. *Electronic Commerce Research and Applications*, *7*(2), 141-164. doi:10.1016/j.elerap.2006.12.004

Baugerød Stokke, O. P. (2018, 3. Mai). Slik skal Vipps banke Apple Pay. *Dinside.no.* Hentet 07.06.2018 fra https://www.dinside.no/okonomi/slik-skal-vipps-banke-apple-pay/69766065

BBC. (2018). *Facebook scandal "hit 87 million users".* Hentet 03.05.2018 fra http://www.bbc.com/news/technology-43649018

Bengtsson, M. (2016). How to plan and perform a qualitative study using content analysis. *Nursing Plus Open*, *2*, 8-14. Hentet fra https://ac.els-cdn.com/S2352900816000029/1-s2.0-S2352900816000029-main.pdf?_tid=2f2c9802-f38b-46af-acf0-7b49d5df7928&acdnat=1527583980_4748c7fcc5e8103e00ac8ad398aacb19

Berry, L. L., Seiders, K., og Grewal, D. (2002). Understanding service convenience. *Journal of marketing*, *66*(3), 1-17. Hentet fra: http://www.jstor.org/stable/pdf/3203451.pdf?casa_token=PkYOLDk78QoAAAAA:v1FthEZIcn9h7ROqJYiPMeVMJTSrjBM5zUuC4RI16vzl6GmlBGF_FVSTkf97FgUr_AvACHoz9WXzbjIU8_p6TpXKfrUwky0CL-t-AN--G8MCMere

Boden, R. (2017). *WeChat Pay and offline mobile payments see "incredibly high" uptake in China.* Hentet 04.04.2018 fra https://www.nfcworld.com/2017/04/26/351800/wechat-pay-offline-mobile-payments-see-incredibly-high-uptake-china/

Brown, L. G. (1990). Convenience in services marketing. *Journal of Services Marketing*, *4*(1), 53-59. doi: 10.1108/EUM0000000002505

Bull, G. (2010). The always-connected generation. *Learning & Leading with Technology*, *38*(3), 28-29. Hentet 04.04.2018 fra https://files.eric.ed.gov/fulltext/EJ903513.pdf

Chen, T. (2017). *China Mobile Payment Report 2017*. Hentet 12.02.2018 fra https://walkthechat.com/china-mobile-payment-report-2017/

Crosman, P. (2016). *Trade-Off Gets Tougher Between Security, Convenience.* Hentet 12.02.2018 fra https://www.americanbanker.com/news/trade-off-gets-tougher-between-security-convenience

Dimock, M. (2018). *Defining generations: Where Millennials end and post-Millennials begin*. Hentet 04.04.2018 fra http://www.pewresearch.org/fact-tank/2018/03/01/defining-generations-where-millennials-end-and-post-millennials-begin/

Elefant, S. M. (2011). *Secure online payment systems requires end-to-end encryption*. Hentet fra http://searchsecurity.techtarget.com/magazineContent/Secure-online-payment-system-requires-end-to-end-encryption

eMarketer (2017). *Personal Mobile Payments on the Rise in Europe.* Hentet 04.02. fra https://www.emarketer.com/Article/Personal-Mobile-Payments-on-Rise-Europe/1015592

Finans Norge. (u.å). *PSD2 eller betalingstjenestedirektivet*. Hentet 06.02.2017 fra https://www.finansnorge.no/tema/bank/psd2-eller-betalingstjenestedirektivet/

Fleming, J., og Adkins, A. (2016). *Data Security: Not a Big Concern for Millennials.* Hentet 03.05.2018 fra http://news.gallup.com/businessjournal/192401/data-security-not-big-concern-millennials.aspx

Fjeldheim, O.V. K., og Strøm, S. D. (2016). *Mobilbetaling og Adopsjonsproblemet: Hvordan kan mobilbetaling som integrert del av en "mobil lojalitetsplattform" fungere som et sterkere incentiv til adopsjon enn å kun tilby transaksjonsløsningen.* (Bacheloroppgave). Høyskolen Kristiania

Geetha, S., og Sujatha, S. (2017). Secured Mobile Banking and Digital Payment System. *International Journal of Innovations & Advancement in Computer Science, 6*(9), 192-198. Hentet fra http://academicscience.co.in/admin/resources/project/paper/f201709161505583598.pdf

Guinn, Jim (u.å.) *New Lessons For Cyber Preparedness.* Accenture.com. Hentet 07.02.2018 fra https://www.accenture.com/us-en/insight-highlights-utilities-increasing-cyber-threats

Güngör, A. S. (2017). Are You Ready To Take The Risks Of Mobile Payment App? Early Adopters Vs Laggards. *İktisadi ve İdari Bilimler Fakültesi Dergisi, 19*(3), 952-974. Hentet fra http://www.idealonline.com.tr/IdealOnline/pdfViewer/index.xhtml?uId=65926&ioM=Paper&preview=true&isViewer=true#pagemode=bookmarks

Gwinner, K. P., Gremler, D. D., og Bitner, M. J. (1998). Relational benefits in services industries: the customer's perspective. *Journal of the academy of marketing science*, *26*(2), 101-114. Hentet fra http://journals.sagepub.com/doi/pdf/10.1177/0092070398262002

Handelshøyskolen BI, (u.å.). *Studere ved BI: Campus Bergen.* Hentet 09.05.2018 fra https://www.bi.no/studere-ved-bi/campus-bergen/

Hasham, S., Vancauwenberge, M., Weiner, J., og Rezek, C. (2016, august). Is cybersecurity incompatible with digital convenience? Hentet 06.02.2018 fra https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/is-cybersecurity-incompatible-with-digital-convenience

Hoemsnes, A., og Trumpy, J. (2017, 12. oktober). Kaller mobilepay "en fiasko". *Dagens Næringsliv*. Hentet 11.05.2018 fra https://www.dn.no/nyheter/2017/10/11/2054/Finans/kaller-mobilepay-en-fiasko

Hærnes, C. (2017, 28. Desember). Digitalåret 2018: Fire trender og én utfordring som vil prege digitaliseringen av Norge i 2018. *Dagens Næringsliv*. Hentet 27.01.2018 fra https://www.dn.no/etterBors/2017/12/28/2030/Teknologi/digitalaret-2018

IBM. (2018). *IBM Future of Identity Study: Millennials Posed to Disrupt Authentication Landscare.* Hentet 04.05.2018 fra https://www-03.ibm.com/press/us/en/pressrelease/53646.wss

Intercede. (2015). *Intercede Millennial Survey Findings.* Hentet 04.05.2018 fra https://media.scmagazine.com/documents/162/intercede_millennial_survey_to_40262.pdf

Jaouad, B., og El Hillali Wadii, E. G. (2014). Architecture of a Mediation System for Mobile Payment. *International Journal of Advanced Computer Science and Applications*, *5*(9), 42-51. Hentet fra https://thesai.org/Downloads/Volume5No9/Paper_8-Architecture_of_a_Mediation_System_for_Mobile_Payment.pdf

Lam, S. Y., & Shankar, V. (2014). Asymmetries in the effects of drivers of brand loyalty between early and late adopters and across technology generations. J*ournal of Interactive Marketing*, *28*(1), 26-42. doi: 10.1016/j.intmar.2013.06.004

Lee, S. Y. (2014). Examining the factors that influence early adopters' smartphone adoption: The case of college students. *Telematics and Informatics*, *31*(2), 308-318. doi: 10.1016/j.tele.2013.06.001

Leggatt, H. (2015). *Millennials want convenient, functional and relevant mobile app experience.* Hentet 03.05.2018 fra http://www.bizreport.com/2015/05/millennials-want-convenient-functional-and-relevant-mobile-a.html

Lenhart, A., Purcell, K., Smith, A., og Zickuhr, K. (2010). Social Media & Mobile Internet Use among Teens and Young Adults. Millennials. Hentet 03.05.2018 fra https://files.eric.ed.gov/fulltext/ED525056.pdf

Liamputtong, P. (2011). *Focus group methodology: Principle and practice*. London: Sage Publications Ltd.

Lindvoll, Eilin. (2017). *Ser du dette skiltet må du likevel åpne lommeboken*. Hentet 12.02.2018 fra https://www.dinside.no/okonomi/ser-du-dette-skiltet-ma-du-likevel-apne-lommeboken/68663258

Mallat, N. (2007). Exploring consumer adoption of mobile payments–A qualitative study. *The Journal of Strategic Information Systems*, *16*(4), 413-432. doi: 10.1016/j.jsis.2007.08.001

Maske, Nelly S., (2017) *Årsrapport 2016*. Hentet 11.05.2018 fra http://aarsrapport.smn.no/2016/content/344/Digital-utvikling

Masrom, M. (2007). *Technology acceptance model and e-learning.* Paper presentert på The 12th International Conference on Education, Universiti Brunei Darussalam.

Norges Handelshøyskole. (2018). *Høyere opptaksgrense også i 2017.* Norges Handelshøyskole. Hentet 24.03.2018 fra https://www.nhh.no/nhh-bulletin/artikkelarkiv/nyheter-fra-nhh/2017/juli/hoye-opptaksgrenser-ogsa-i-2017/

Saunders, M., Lewis, P. and Thornhill, A. (2016). *Research methods for business students* (7. utg). Harlow: Pearson Education Limited.

Seljehaug, J.I. (2018) Tommel opp til Vipps-fusjon. *Hegnar.no.* Hentet 11.05.2018 fra http://www.hegnar.no/Nyheter/Boers-finans/2018/04/Tommel-opp-til-Vipps-fusjon

Smith, K.T. (2011). Digital marketing strategies that Millennials find appealing, motivating, or just annoying. *Journal of Strategic Marketing, 19*(6), 489-499. doi: 10.1080/0965254X.2011.581383

Statistisk Sentralbyrå. (2018). *Studenter i høyere utdanning*. Hentet 24.03.2018 fra https://www.ssb.no/utdanning/statistikker/utuvh

Stefanovic, A. M., og Ribe, A. C. (2017). Mobile lommebøker: en eksplorativ studie av dagens konkurransesituasjon og fremtidig utvikling. (Masteroppgave). Norges Handelshøyskole. Bergen.

Stewart, D. W., & Shamdasani, P. N. og Rook, D.W. (2007). *Focus groups: Theory and practice* (2. utg). London: Sage publications.

Sæter, M. & Sterri, A. B. (2015). Innholdsanalyse. I *Store norske leksikon*. Hentet 18. februar 2018 fra https://snl.no/innholdsanalyse

Taylor, P. (2014). *More than half of Millennials have shared a "selfie"*. Hentet 04.04.2018 fra http://www.pewresearch.org/fact-tank/2014/03/04/more-than-half-of-millennials-have-shared-a-selfie/

Tedeschi, B. (2000, 12. juni). E-commerce Report: Easier-to-use sites would help e-tailers close more sales. *New York Times.* Hentet 12.03.2018 fra https://www.nytimes.com/2000/06/12/business/e-commerce-report-easier-to-use-sites-would-help-e-tailers-close-more-sales.html

Telenor. (2017). *Digital Sikkerhet 2017: Et Tryggere Samfunn.* Hentet 07.02.2017 fra https://www.telenor.no/Images/DIGITAL%20SIKKERHET%202017_FINAL_PDF_tcm94-320051.pdf

Transparency International. (2018). *Corruption Perceptions Index 2017.* Hentet 04.05.2018 fra https://www.transparency.org/news/feature/corruption_perceptions_index_2017#regional

Trumpy, J. (2018, 27. april). Vipps er forsinket med mobilbetaling. *Dagens Næringsliv.* Hentet 03.05.2018 fra https://www.dn.no/nyheter/2018/04/27/2000/Finans/vipps-er-forsinket-med-mobilbetaling

Venkatesh, V., Thong, J. Y., og Xu, X. (2012). Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology. *MIS quarterly*, 157-178. Hentet 03.05.2018 fra http://www.jstor.org/stable/41410412?seq=1#page_scan_tab_contents

Vizzarri, A., Vatalaro, F., og Vari, M. (2013). *Security in mobile payments.* Paper presentert på AEIT Annual Congress 2013, Palermo.

Wadgave, U., og Khairnar, M. R. (2016). Parametric tests for Likert scale: For and against. *Asian journal of psychiatry*, *24*, 67-68. doi: 10.1016/j.ajp.2016.08.016

WeChat Pay. (u.å.). *Numerous Active Users*. Hentet 12.02.2018 fra https://pay.weixin.qq.com/wechatpay_guide/intro_users.shtml

Weir, C. S., Douglas, G., Carruthers, M., og Jack, M. (2009). User perceptions of security, convenience and usability for ebanking authentication tokens. *Computers & Security, 28(*1-2), 47-62. doi: 10.1016/j.cose.2008.09.008

# 9.0 Appendiks

## 9.1 Vedlegg 1 - Fjern- og nærbetalinger

**Fjernbetalinger:**

- Kunden bruker sin egen mobilenhet til å sende en betalingsforespørsel til en betalingstjenesteleverandør (Payment Service Provider, PSP) over et trådløst nettverk. Forespørselen inneholder forhandlerens detaljer, samt summen som skal betales
- PSPen verifiserer kundens legitimasjon og forhandlerens identitet. I praksis sjekker PSPen at kunden og selgeren er registrert i mobilbetalingssystemet
- PSPen kan også be kunden om flere detaljer, eksempelvis passord for autentiseringsformål
- Når kundens legitimasjon er vurdert, ber PSPen forhandleren om en bekreftelse ved å videresende betalingsinformasjonen
- Forhandleren sender deretter en bekreftelsesmelding til PSPen
- Ved bekreftelse utfører PSPen en backend-behandling for å oppdatere kontoen til kunde og forhandler
- Betalingskvittering sendes så til kunde. En "transaksjon-fullført"-melding kan eventuelt sendes til forhandler

**Nærbetalinger:**

- Kunden benytter sin mobilenhet til å sende en betalingsforespørsel direkte til kunden, gjennom en form for NFC, Bluetooth eller RFID
- Deretter videresender forhandleren denne forespørselen til PSP over et trådløst nettver.
- PSPen verifiserer kundens legitimasjon og forhandlerens identitet. I praksis sjekker PSPen at kunden og selgeren er registrert i mobilbetalingssystemet
- PSPen utfører en backend-behandling for å oppdatere kontoen til kunde og forhandler
- Betalingskvittering sendes så til kunde. En "transaksjon-fullført"-melding kan eventuelt sendes til forhandler

## 9.2 Vedlegg 2 - Intervjuguide

| Tidsramme | Forslag til spørsmål/tema |
|---|---|
| **Rammesetting (5-10 min)** | Uformell prat, kaffeservering<br>Informasjon og introduksjon<br>• Informasjon om prosjektet<br>• Taushetsplikt og anonymisering<br>• Lydopptak<br>• Transkribert versjon tilgjengelig for deltakerne<br>• Navnerunde |
| **Introduksjonsspørsmål (10 min)** | • Kan dere fortelle litt om hvilke typer apper dere laster ned?<br>• Hvor ofte hender det at dere laster ned en app og sletter den etter kort tid? Hvorfor?<br>• Hva slags research gjør dere før dere laster ned en app? |
| **Overgangsspørsmål (10 min)** | • Hvilke betalingsapper kjenner dere til?<br>• Hvordan opplever dere brukervennligheten i betalingsapper?<br>• Hvordan opplever dere sikkerheten i betalingsapper?<br>• (Bruke materiell: Facebook/Amazon/Apple/AliPay/Payr-logo). Hva tenker dere om å bruke betalingstjenester fra leverandører som ikke har en bank i ryggen?<br>• Tenk tilbake til forrige gang du utførte en betaling i en (fysisk) butikk. Kan dere se for dere en annen måte å utføre betalingen på? |
| **Fokusspørsmål (20 min)** | • Hva gjør en mobilbetalingstjeneste sikker? (Autentisering/personlige passord/pinkode/bank-ID/fingeravtrykk/ansiktsgjenkjenning, en leverandør med godt rykte (tillit), samarbeidspartnere, "garanti" for beskyttet mot angrep/hacking)<br>• Hva gjør mobilbetalingstjeneste bekvemmelig? (Brukergrensesnitt, lite nedetid, kundeservice, tilgjengelighet, kan brukes til all betaling, rask autentisering)<br>• Kan dere gi en beskrivelse av hvordan dere vil at en mobilbetalingstjeneste skal være? |
| **Oppsummeringsspørsmål (5 min)** | • Moderator stiller oppsummeringsspørsmål basert på punkter som assisterende moderator sender i et google doc. Punktene gjelder tema som trenger oppklaring/mer diskusjon. |
| **Konklusjonsspørsmål (5 min)** | • Er det noe dere gjerne vil legge til?<br>• Hvordan opplevde dere å være med i fokusgruppen? |

## 9.3 Vedlegg 3 - Kodeliste

**SIKKERHETSKODER**

**Generell oppfatning av sikkerhet:** Utsagn som er vanskelig å plassere under noen konkret form for sikkerhet.

*EKS:*

*"[...] det er ganske mange som er veldig redd for den der overvåkningen."*

*"Jeg har ikke noe problem med det selv, det har jeg ikke, men jeg vet om folk som absolutt ikke skal la big brother kunne vite hvor, eller hva, og hvorfor "*

**Ekstern sikkerhet**: Regelverk og PSD2. Tillit til myndigheter. Utsagn som omhandler sikkerhet utenfor leverandør og forbrukers kontroll.

*EKS:*

*"Da er det helt sikkert noe regelverk som tar oss i vare"*

*"Og hvis noen skulle svindle deg, så altså, det blir små beløper. Eh, pluss at du får det jo igjen. "*

**Leverandørs sikkerhet:** Det som omhandler tillit til leverandørers sikkerhet. Leverandørkontroll.

*EKS:*

*"[...] når den der DnB-skandalen var i forfjor, [...] Da hadde ikke jeg Vipps en stund. Og da var jeg ganske megaskeptisk."*

*"De har DnB bak. At det er en bauta bak der. Du stoler på det, sant du har jo*

**Forbrukers sikkerhet:** Hva forbrukerne selv gjør for å være sikre (f.eks gjøre research, lese vilkår). Forbrukerkontroll.

*EKS:*

*"Du må godkjenne med swipe. Det gir ikke mening, swipe er ikke noe som man gjør i Vipps."*

*"Men der har jeg vært litt dum for lenge siden, for jeg har jo sånn, 7-8 passord jeg rullerer på, men jeg mistenker at det som har skjedd der er at samme passordet som har vært på Ebay-kontoen er da det samme som det som har vært på den verified by visa-koden. … Nei, altså det er åtte tegn, fire bokstaver, fire tall, capslock og helt tilfeldig generert"*

*"Men det er noe som du som regel må inn i innstillingene og skru på selv (tofaktorautentisering)."*

**BEKVEMMELIGHETSKODER**

Beslutningsbekvemmelighet Utsagn om hvordan de tar beslutninger når de laster ned app.

*EKS:*

*"Jeg er mer sånn der, jeg vet hva jeg skal ha, hvilken app jeg skal ha, eller hvilken type app jeg leter etter, og så trykker jeg på den med finest bilde (latter, enighet)"*

*"I hvert fall lest de der vilkårene for tilbakebetaling i så fall [messenger pay]. "*

Tilgangsbekvemmelighet Tilgangsbekvemmelighet omhandler forbrukernes oppfattede bruk av tid og innsats som kreves for å initiere en tjenesteleveranse. Dette omfatter aktivitetene en forbruker må utføre for å forespørre tjenesten, og i noen tilfeller aktiviteter som kreves for å motta den.

*EKS:*

*"[…] hvorfor skal du ha liksom tre forskjellige?"*

Transaksjonsbekvemmelighet Transaksjonsbekvemmelighet fokuserer kun på handlingen forbrukeren må utføre for å sikre seg retten til en tjeneste. Hovedsakelig ser vi på autentiseringsprosessen.

*EKS:*

*"Det går på bekostning av brukeropplevelsen da. (bankID) så kan jeg heller eh, ha en firesifret kode eller tommelen."*

Nyttebekvemmelighet Nyttebekvemmelighet er forbrukernes oppfattede bruk av tid og innsats på å oppleve, eller dra nytte av, en tjenestes kjernefordel.

*EKS:*

*"At du på et eller annet vis får opp de varene du skal betale for, sånn at du også ser det, kanskje."*

*"Enkelt design"*

Post-nyttebekvemmelighet Post-nyttebekvemmelighet involverer forbrukernes oppfatning av bruk av tid og innsats når de på ny initierer kontakt med en bedrift etter selve nyttestadiet. Noen aktiviteter relatert til post-nyttebekvemmelighet initieres av tjenestebedriften.

*EKS:*

*"De bruker det (personlig informasjon) kun til å selge det til reklamebyrå, som kan gi deg spesifikk, personalisert reklame."*

*"Det er det jeg egentlig setter pris på. Altså jeg godtar bevisst med at jeg vet det, så får jeg reklame som jeg vet at passer til meg. Og da kanskje det dukker opp noe jeg har lyst til å kjøpe, hvis jeg ikke gjorde det ville jeg gått glipp av"*

## 9.4 Vedlegg 4 - Spørreskjema

| Form | Tekst | Svaralternativ | Måler |
|---|---|---|---|
| Informasjon | Takk for at du tar deg tid til å svare på denne undersøkelsen! I forbindelse med masterutredningen vår ved Norges Handelshøyskole skal vi gjennomføre en undersøkelse for å kartlegge hvordan forbrukere forholder seg til sikkerhet og bekvemmelighet i mobilbetalingsapplikasjoner.<br><br>Med mobilbetaling dreier det seg her om gjennomføring av betaling i fysisk butikk/utsalgssted ved bruk av en mobil enhet.<br><br>Dine svar kan ikke spores til deg, undersøkelsen er 100% anonym. Estimert gjennomføringstid er på ca. 5 minutter. | | |
| Spørsmål | Har du benyttet deg av en mobilbetalingsapplikasjon den siste måneden (f. eks. Vipps, Paypal) | Ja/Nei | |
| Spørsmål | Er du over 35 år? | Ja/Nei | |
| Spørsmål | Hvilket kjønn identifiserer du deg med? | Mann/Kvinne/Annet | |
| Informasjon | De følgende utsagnene dreier seg om sikkerhet i mobilbetalingsapplikasjoner. Med sikkerhet menes hva du som forbruker selv kan gjøre for å unngå ondsinnede angrep (f. eks. hacking, overvåking, svindel, misbruk av persondata), men også hva leverandøren av applikasjonen og det offentlige kan gjøre for å håndtere sikkerhetsutfordringer. På de følgende utsagnene ønsker vi at du svarer på en skala fra Helt uenig til Helt enig. | | |

| | | | |
|---|---|---|---|
| Påstand | Det er viktig for meg å lese vilkår før jeg tar i bruk en mobilbetalingsapplikasjon | Likertskala | Forbruker |
| Påstand | Det er viktig for meg at det finnes en sikker innloggingsmetode, som hindrer andre i å få tilgang til min mobilbetalingsapplikasjon (f. eks. PIN-kode, Passord, Bank ID på mobil) | Likertskala | Leverandør |
| Påstand | Det er viktig for meg å benytte ulike PIN-koder i ulike mobilbetalingsapplikasjoner | Likertskala | Forbruker |
| Påstand | Det viktig for meg å endre PIN-koder ofte (med ofte menes 2 eller flere ganger i året) | Likertskala | Forbruker |
| Påstand | Det er viktig for meg at det eksisterer et offentlig regelverk som forebygger ondsinnede angrep i en mobilbetaling | Likertskala | Offentlig |
| Påstand | Det er viktig for meg at det eksisterer et offentlig regelverk som beskytter meg dersom jeg blir utsatt for ondsinnede angrep i en mobilbetaling | Likertskala | Offentlig |
| Informasjon | De følgende utsagnene dreier seg om sikkerhet i mobilbetalingsapplikasjoner. Med sikkerhet menes hva du som forbruker selv kan gjøre for å unngå ondsinnede angrep (f. eks. hacking, overvåking, svindel, misbruk av persondata), men også hva leverandøren av applikasjonen og det offentlige kan gjøre for å håndtere sikkerhetsutfordringer. På de følgende utsagnene ønsker vi at du svarer på en skala fra Helt uenig til Helt enig. | | |
| Påstand | Det er viktig for meg at mobilbetalingsapplikasjonen ikke får tilgang til andre applikasjoner på min smarttelefon | Likertskala | Leverandør |
| Påstand | Det er viktig for meg at leverandøren av en mobilbetalingsapplikasjon er helt eller delvis eid av en bank | Likertskala | Leverandør |

| | | | |
|---|---|---|---|
| Påstand | Det er viktig for meg at en mobilbetalingsapplikasjon er utgitt av en norsk leverandør | Likertskala | Leverandør |
| Påstand | Det er viktig for meg å få en oversikt over varene/tjenestene jeg skal kjøpe, samt sum, før jeg gjennomfører en betaling i en mobilbetalingsapplikasjon | Likertskala | Leverandør |
| Påstand | Det er viktig for meg at en mobilbetalingsapplikasjon sender meg regelmessige påminnelser om å endre innloggingsinformasjon | Likertskala | Leverandør |
| Informasjon | De følgende utsagnene dreier seg om bekvemmelighet i mobilbetalingsapplikasjoner. Med bekvemmelighet menes tid og innsats spart fra du velger å laste ned en mobilbetalingsapplikasjon til du gjennomfører et kjøp og eventuelt benytter deg av øvrige tjenester etter at kjøpet er gjennomført. På de følgende utsagnene ønsker vi at du svarer på en skala fra Helt uenig til Helt enig. | | |
| Påstand | Det er viktig for meg at en mobilbetalingsapplikasjon har gode kundeomtaler | Likertskala | Beslutning |
| Påstand | Det er viktig for meg at en mobilbetalingsapplikasjon kan benyttes i mange utsalgssteder | Likertskala | Tilgang |
| Påstand | Det er viktig for meg å benytte meg av ”husk min innloggingsinformasjon” i mobilbetalingsapplikasjoner | Likertskala | Transaksjon |
| Påstand | Det er viktig for meg at en mobilbetalingsapplikasjon krever få klikk for å gjennomføre en betaling | Likertskala | Nytte |
| Påstand | Det er viktig for meg at en mobilbetalingsapplikasjon kan kommunisere med andre applikasjoner på min smarttelefon (f. eks. applikasjoner med lojalitetsprogram) | Likertskala | Nytte |
| Påstand | Det er viktig for meg at en mobilbetalingsapplikasjon sender meg | Likertskala | Postnytte |

| | | | |
|---|---|---|---|
| | push-varsler (f. eks. gode tilbud basert på stedtjenester) | | |
| Påstand | Det er viktig for meg at en mobilbetalingsapplikasjon sender meg reklame basert på mitt forbrukermønster | Likertskala | Postnytte |

# 9.5 Vedlegg 5 - Spørreskjema fordeling

Det er viktig for meg å lese vilkår før jeg tar i bruk en mobilbetalingsapplikasjon

| | |
|---|---|
| Helt uenig | 18,27 % |
| Ganske uenig | 29,81 % |
| Litt uenig | 11,54 % |
| Verken eller | 8,65 % |
| Litt enig | 24,04 % |
| Ganske enig | 5,77 % |
| Helt enig | 1,92 % |

Det er viktig for meg å benytte ulike PIN-koder i ulike mobilbetalingsapplikasjoner

| | |
|---|---|
| Helt uenig | 5,77 % |
| Ganske uenig | 17,31 % |
| Litt uenig | 13,46 % |
| Verken eller | 16,35 % |
| Litt enig | 14,42 % |
| Ganske enig | 17,31 % |
| Helt enig | 15,38 % |

Det er viktig for meg at det finnes en sikker innloggingsmetode, som hindrer andre i å få tilgang til min mobilbetalingsapplikasjon (f. eks. PIN-kode, Passord, Bank ID på mobil)

| | |
|---|---|
| Helt uenig | 0,96 % |
| Ganske uenig | 0,00 % |
| Litt uenig | 0,00 % |
| Verken eller | 0,96 % |
| Litt enig | 1,92 % |
| Ganske enig | 19,23 % |
| Helt enig | 76,92 % |

Det viktig for meg å endre PIN-koder ofte (med ofte menes 2 eller flere ganger i året)

| | |
|---|---|
| Helt uenig | 28,85 % |
| Ganske uenig | 25,96 % |
| Litt uenig | 13,46 % |
| Verken eller | 17,31 % |
| Litt enig | 10,58 % |
| Ganske enig | 1,92 % |
| Helt enig | 1,92 % |

Det er viktig for meg at det eksisterer et offentlig regelverk som forebygger ondsinnede angrep i en mobilbetaling

| | |
|---|---|
| Helt uenig | 0,00 % |
| Ganske uenig | 0,00 % |
| Litt uenig | 0,00 % |
| Verken eller | 1,92 % |
| Litt enig | 8,65 % |
| Ganske enig | 20,19 % |
| Helt enig | 69,23 % |

Det er viktig for meg at mobilbetalingsapplikasjonen ikke får tilgang til andre applikasjoner på min smarttelefon

| | |
|---|---|
| Helt uenig | 2,88 % |
| Ganske uenig | 0,96 % |
| Litt uenig | 5,77 % |
| Verken eller | 13,46 % |
| Litt enig | 19,23 % |
| Ganske enig | 30,77 % |
| Helt enig | 26,92 % |

Det er viktig for meg at det eksisterer et offentlig regelverk som beskytter meg dersom jeg blir utsatt for ondsinnede angrep i en mobilbetaling

| | |
|---|---|
| Helt uenig | 0,00 % |
| Ganske uenig | 0,00 % |
| Litt uenig | 0,00 % |
| Verken eller | 1,92 % |
| Litt enig | 4,81 % |
| Ganske enig | 17,31 % |
| Helt enig | 75,96 % |

Det er viktig for meg at leverandøren av en mobilbetalingsapplikasjon er helt eller delvis eid av en bank

| | |
|---|---|
| Helt uenig | 1,92 % |
| Ganske uenig | 2,88 % |
| Litt uenig | 7,69 % |
| Verken eller | 20,19 % |
| Litt enig | 25,96 % |
| Ganske enig | 23,08 % |
| Helt enig | 18,27 % |

Det er viktig for meg at en mobilbetalingsapplikasjon er utgitt av en norsk leverandør

| | |
|---|---|
| Helt uenig | 2,88 % |
| Ganske uenig | 8,65 % |
| Litt uenig | 7,69 % |
| Verken eller | 24,04 % |
| Litt enig | 26,92 % |
| Ganske enig | 18,27 % |
| Helt enig | 11,54 % |

Det er viktig for meg at en mobilbetalingsapplikasjon sender meg regelmessige påminnelser om å endre innloggingsinformasjon

| | |
|---|---|
| Helt uening | 3,85 % |
| Ganske uening | 13,46 % |
| Litt uening | 21,15 % |
| Verken eller | 24,04 % |
| Litt enig | 20,19 % |
| Ganske enig | 12,50 % |
| Helt enig | 4,81 % |

Det er viktig for meg å få en oversikt over varene/tjenestene jeg skal kjøpe, samt sum, før jeg gjennomfører en betaling i en mobilbetalingsapplikasjon

| | |
|---|---|
| Helt uenig | 0,00 % |
| Ganske uenig | 0,96 % |
| Litt uenig | 0,00 % |
| Verken eller | 1,92 % |
| Litt enig | 7,69 % |
| Ganske enig | 28,85 % |
| Helt enig | 60,58 % |

Det er viktig for meg at en mobilbetalingsapplikasjon har gode kundeomtaler

| | |
|---|---|
| Helt uenig | 0,00 % |
| Ganske uenig | 0,96 % |
| Litt uenig | 0,96 % |
| Hverken eller | 4,81 % |
| Litt enig | 28,85 % |
| Ganske enig | 34,62 % |
| Helt enig | 29,81 % |

Det er viktig for meg at en mobilbetalingsapplikasjon kan benyttes i mange utsalgssteder

| | |
|---|---|
| Helt uenig | 0,00 % |
| Ganske uenig | 0,96 % |
| Litt uenig | 0,00 % |
| Hverken eller | 5,77 % |
| Litt enig | 13,46 % |
| Ganske enig | 29,81 % |
| Helt enig | 50,00 % |

Det er viktig for meg at en mobilbetalingsapplikasjon krever få klikk for å gjennomføre en betaling

| | |
|---|---|
| Helt uenig | 0,00 % |
| Ganske uenig | 0,96 % |
| Litt uenig | 1,92 % |
| Hverken eller | 3,85 % |
| Litt enig | 15,38 % |
| Ganske enig | 34,62 % |
| Helt enig | 43,27 % |

Det er viktig for meg å benytte meg av "husk min innloggingsinformasjon" i mobilbetalingsapplikasjoner

| | |
|---|---|
| Helt uenig | 5,77 % |
| Ganske uenig | 6,73 % |
| Litt uenig | 9,62 % |
| Hverken eller | 17,31 % |
| Litt enig | 20,19 % |
| Ganske enig | 22,12 % |
| Helt enig | 18,27 % |

Det er viktig for meg at en mobilbetalingsapplikasjon kan kommunisere med andre applikasjoner på min smarttelefon (f. eks. applikasjoner med lojalitetsprogram)

| | |
|---|---|
| Helt uenig | 3,85 % |
| Ganske uenig | 3,85 % |
| Litt uenig | 11,54 % |
| Verken eller | 26,92 % |
| Litt enig | 28,85 % |
| Ganske enig | 17,31 % |
| Helt enig | 7,69 % |

Det er viktig for meg at en mobilbetalingsapplikasjon sender meg push-varsler (f. eks. gode tilbud basert på stedtjenester)

| | |
|---|---|
| Helt uenig | 24,04 % |
| Ganske uenig | 23,08 % |
| Litt uenig | 16,35 % |
| Verken eller | 21,15 % |
| Litt enig | 11,54 % |
| Ganske enig | 2,88 % |
| Helt enig | 0,96 % |

Det er viktig for meg at en mobilbetalingsapplikasjon sender meg reklame basert på mitt forbrukermønster

| | |
|---|---|
| Helt uenig | 41,35 % |
| Ganske uenig | 23,08 % |
| Litt uenig | 15,38 % |
| Verken eller | 12,50 % |
| Litt enig | 5,77 % |
| Ganske enig | 0,96 % |
| Helt enig | 0,96 % |

# 9.6 Vedlegg 6 - Cronbachs Alpha

| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | *Q2* | *Q8* | *Q4* | *Q5* | *Q7* | *Q6* | *Q9* | *Q10* | *Q11* | *Q12* | *Q13* | *Q14* | *Q15* | *Q16* | *Q17* | *Q18* | |
| Q2 | 1 | | | | | | | | | | | | | | | | |
| Q8 | 0,07363113 | 1 | | | | | | | | | | | | | | | |
| Q4 | 0,50801887 | 0,14518894 | 1 | | | | | | | | | | | | | | |
| Q5 | 0,38145187 | 0,18874351 | 0,63311319 | 1 | | | | | | | | | | | | | |
| Q7 | 0,12346429 | 0,23285797 | 0,10169484 | 0,09977521 | 1 | | | | | | | | | | | | |
| Q6 | 0,10548209 | 0,26825766 | 0,13446695 | 0,10615197 | 0,72687625 | 1 | | | | | | | | | | | |
| Q9 | 0,29275744 | 0,12780551 | 0,27074468 | 0,23604877 | 0,1303756 | 0,06438537 | 1 | | | | | | | | | | |
| Q10 | 0,1699685 | 0,0655701 | 0,03838743 | 0,11142166 | 0,31808167 | 0,23217665 | 0,36068599 | 1 | | | | | | | | | |
| Q11 | 0,18912898 | 0,05111517 | 0,06799676 | 0,14851732 | 0,12123071 | -0,0587556 | 0,33571348 | 0,40347087 | 1 | | | | | | | | |
| Q12 | 0,18682209 | 0,10179959 | 0,00606296 | 0,05844788 | 0,23963966 | 0,16276744 | 0,32950234 | 0,27537097 | 0,26857061 | 1 | | | | | | | |
| Q13 | 0,31864639 | 0,06642106 | 0,44183075 | 0,44144182 | 0,16739801 | 0,06859703 | 0,28029018 | 0,10837536 | 0,11870154 | 0,11466687 | 1 | | | | | | |
| Q14 | 0,34332232 | 0,12332618 | 0,17965288 | 0,17407004 | 0,18565111 | 0,27532577 | 0,07479455 | 0,16378709 | 0,00195258 | 0,18572866 | 0,15485185 | 1 | | | | | |
| Q15 | -0,0481231 | 0,06256804 | -0,0864741 | -0,0757329 | 0,11356315 | 0,31421424 | -0,066926 | -0,1277093 | -0,0973223 | 0,15102661 | -0,1499962 | 0,16971124 | 1 | | | | |
| Q16 | -0,1428209 | -0,0643653 | -0,2039355 | -0,0790192 | 0,01126176 | 0,04912845 | -0,2421741 | -0,0869553 | 0,0262498 | -0,0135784 | -0,0446494 | -0,0466993 | 0,20071554 | 1 | | | |
| Q17 | -0,0920273 | 0,01798394 | -0,0766491 | 0,00296808 | 0,07374978 | 0,30757727 | -0,0450757 | -0,0383672 | -0,1607257 | 0,04476081 | -0,1628756 | 0,11901901 | 0,52767701 | 0,3694849 | 1 | | |
| Q18 | -0,1286205 | 0,08292718 | -0,1807036 | -0,2238003 | 0,10383523 | 0,19735876 | -0,3554082 | -0,1988567 | -0,1457319 | 0,10383423 | -0,1281875 | 0,15023884 | 0,35139809 | 0,21051656 | 0,32513183 | 1 | |
| | | | | | | | | | | | | | | | | | |
| Average | 0,11414339 | | | | | | | | | | | | | | | | |
| Antall | 16 | | | | | | | | | | | | | | | | |
| Ant*Average | 1,82629429 | | | | | | | | | | | | | | | | |
| 1+Average*(Ant-1) | 2,7121509 | | | | | | | | | | | | | | | | |
| **Cronbachs alpha:** | **0,67337488** | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | |