Examensarbete

HÖGSKOLAN I SKÖVDE

# BIOMETRISKA AUTENTISERINGSMETODER

Privatpersoners påverkan av autentiseringsmetod vid användning av smartphone

# BIOMETRIC AUTHENTICATION METHODS

Private influence of authentication method when using smartphone

Examensarbete inom informationsteknologi med inriktning mot informationssystem IT607G

Grundnivå 30 Högskolepoäng

Vårtermin 2019

Josefin Johansson

Handledare: Hanife Rexhepi

Examinator: Eva Söderström

## Sammanfattning

Den här studien har som inriktning gentemot autentisering. Främst de biometriska autentiseringsmetoderna men även en viss omfattning fokuserar på den traditionella autentiseringsmetoden. I dagens samhälle växer teknologin för varje dag som går, och allt fler privatpersoner besitter känslig information som berör deras vardag i sin smartphone som är attraktiva för tjuvar.

Studiens forskningsmetod är den kvalitativa metoder, där litteraturstudie samt intervjuer har genomförts för att komma fram till ett resultatet. Intervjuerna genomfördes med privatpersoner som respondenter, av den anledning att finna deras åsikter kring autentiseringsmetoderna.

Studien fann fyra olika kategorier som är bidragande faktorer till användningen av de biometriska autentiseringsmetoderna, samt vad som faktiskt påverkar en privatpersons åsikter kring användningen. Huruvida de biometriska metoderna hjälper eller stjälper användningen av smartphones, samt vad privatpersoner vill skydda med hjälp av autentiseringsmetoder. Även synpunkter kring lagringen och individens identitet och integritet kom upp som en synpunkt av stor relevans kring användandet av dessa metoder.



Nyckelord: *Autentiseringsmetoder, biometri, smartphone, privatpersoner*

# Innehållsförteckning

# 1. Inledning

Redan på 1950-talet har biometri gestaltats i filmer av olika slag, exempelvis fingeravtrycksigenkänning vilket används vid brottsutredningar. Tekniken har gått framåt och utvecklats allt mer, vilket även filmerna har fångat upp och biometri har framställts som både futuristiskt och realistiskt. Biometri används på sätt som är imponerande i filmer, men är inte alltid trovärdig men i vissa fall skildras den biometriska tekniken på ett sätt vilket beskriver den verkliga användningen av dessa biometriska metoder (Muller, 2017).

Sedan den första mobiltelefonen lanserades 1983 har en fantastisk utveckling av mobiltelefoner skett. Mobiltelefonens förändring har skett genom att först vara endast tillgänglig för rika människor, på grund av höga kostnader. Därefter var mobiltelefonens nästa utvecklingsmål att storleken skulle minska, till följd av att mobiltelefonens storlek minskade så kraftigt att det inte längre var användbart att krympa objektet ytterligare. Fokus hamnade istället på dess funktioner, svartvitt display blev färgdisplay och så vidare (Pocovnicu, 2009). Efter all denna utveckling framåt, har mobiltelefonen istället blivit attraktiva för tjuvar, av den anledning att mobiltelefonens funktionalitet och en ständig utveckling sker. Typiska funktionaliteter vilket är attraktiva är digital bank, personligt digitalt stöd etcetera (Burgbacher et al., 2014).

En studie genomförd av Pocovnicu (2009) har påvisat att de medverkande ansåg att säkerhetsfunktionen med PIN-kod ansågs vara alltför besvärlig och förtroendet för funktionen saknades. Därav använde majoriteten av studiens medverkande inte funktionen alls, och använde istället en helt oskyddad telefon.
Det är lätt att bli skeptisk när svenskarnas lösenordsvanor granskas. Det slarvas kraftigt när det gäller lösenord och dess tillhörande rutiner, fastän att rapporter avlöser varandra om lösenordsläckor. I nutid är det möjligt att med hjälp av vår egen kropp att logga in på datorer och telefoner, vilket kallas för biometri (Wollner, 2018). Däremot har även stora läckor publicerats när det gäller biometri, trots att denna autentiseringsmetod ställer krav som är skyhöga på tillverkaren. Det är inte endast säkerheten som skall skyddas, utan även integriteten för personen som använder metoden. Detta innebär i stort att våra fingeravtryck och dylikt finns lagrade på flertalet av servrar som finns världen över (Wollner, 2018).

Autentisering med hjälp av biometriska metoder har vuxit i popularitet vilket ett sätt att erbjuda personlig identifiering. Personlig identifiering är betydande vid en stor mängd av ansökningar och kreditkortsbedrägerier samt att identitetsstölder stadigt har ökat under de senaste åren. Det påvisar att detta är ett problem i samhället som är av ett stort intresse. Autentiseringar med hjälp av lösenord och PIN-koder har alla brister och begränsar användbarheten (Bhattacharyya, Ranjan, Alisherov & Choi, 2009).

Denna studie syftar till att undersöka och analysera hur privatpersoner anser de biometriska autentiseringsmetoder jämfört med lösenord samt studera hur säkra

privatpersoner upplever att dess smartphone faktiskt är med hjälp av de utvalda autentiseringsmetoder. Litar privatpersonerna på de framtagna metoderna?

För att få fram ett resultat på denna studie tillämpas den kvalitativa metodansatsen, med intervjuer och litteraturstudie som bidrar till information. Det slutliga resultatet resulterade i fyra olika faktorer som påverkar en privatpersons val av de biometriska autentiseringsmetoderna. De fyra olika kategorierna som framkom under studiens gång är ekonomi, biometrin skall vara enkel att använda, lagring av personlighetsdrag samt identitet och integritet. Dessa faktorer indikerar på att privatpersoner som använder smartphones är medvetna om att det finns hot gentemot smartphones, samt att privatpersoner är reflekterande kring vad användning av de biometriska autentiseringsmetoderna bidrar till. Samtidigt är det av stor relevans att autentiseringsmetoderna skall vara enkla vid användning, för att få en lätt åtkomst till sin smartphone.

# 2. Bakgrundskapitel

*I detta kapitel presenteras viktig bakgrundsfakta om traditionella autentiseringsmetoder samt biometrisk autentisering. Ytterligare information om biometrins specifika metoder för autentisering presenteras, och därtill även dess för- och nackdelar för att kunna få en bredare syn av området.*

## *2.1. Informationssäkerhet*

För en organisation är information en tillgång vilket är betydande för en organisation, enligt Andronache och Althonayan (2018). Därtill är manipulation, skydd samt lagring nödvändigt och bör ingå i en organisations kultur och organisation. Von Solms och van Niekerk (2013) menar även att syftet med informationssäkerhet är företagets kontinuitet skall säkerställas samt att minimera företagsskador genom att säkerhetsincidenter begränsas. En del av den information som vi besitter är av värde för både organisationer och för enskilda individer (MSB, 2015). All information, såsom forskningsresultat, fotografier till fastighetsförteckningar och saldot på bankkontot. Ibland är information livsviktig som exempelvis information i patientjournaler eller kärnkraftverks styrsystem. Går information som sådan förlorad eller är felaktig, kan katastrofala följder ske.

Information är värdefullt och ovärderligt, och behöver därför skyddas efter behov (MSB, 2015). Ett informationssäkerhetsarbete som har utförts på ett bra sätt är en förutsättning för korrekt och effektiv informationshantering. Information är ett hjälpmedel för att kunna förmedla kunskap, där individer kan kommunicera med hjälp av information, vi kan lagra informationen samt att med hjälp av information kan processer styras. Information behövs till det mesta som vi gör. Tvrdíková (2008) menar även att en viktig del av informationssystemsdesign och utveckling är den tillhörande säkerheten till systemet. Det går inte att endast lösa säkerheten kring informationssystemet, genom informationsteknikssäkerhet, av den anledning att informationsteknik utgör endast en del av informationssystemet. En syn på säkerheten för informationssystem bör vara omfattande och integrerad samt överväga alla dess tillhörande delar, såsom mjukvara, hårdvara, data, mänskliga faktorer och verklighetens verkan. En väl implementerat informationssäkerhetshanteringssystem är utformat på ett pålitligt sätt, genom att skydda informationen i en institution eller ett företag (Tvrdíková, 2008).

Informationssäkerhet är en strategisk fråga vilket har var varit avgörande inom organisationshantering. Informationssäkerhetshantering är en process som är systematisk och är effektiv genom att hantera hot och risker gentemot säkerheten kring informationen som finns i en organisation. Implementering- och underhållningskostnader är höga, vilket leder till att organisationer måste skilja mellan kontroller som anses vara kritiska respektive mindre kritiska, menar Tu och Yuan (2014).

Information har en viktig roll inom företagens affärsverksamhet, genom att stödja och underlätta för organisationen att uppnå konkurrenskraft gentemot andra organisationer, fortsätter Tu och Yuan (2014). Information är dyrbar för organisationen, men är även en kritisk faktor för organsationen av den anledningen att den även utsetts för flertalet attacker, både inom samt utanför organisationer såsom virus, hackare och dataförluster med mera. Informationssäkerhetshanteringens mål är att skydda integriteten, konfidentialiteten samt tillgängligheten av information och även att lindra olika hot och risker mot information som sådan. Tu och Yuan (2014) menar även att informationssäkerhetshantering kan vara till hjälp för organisationer genom att minska hoten mot säkerheten avsevärt samt dela information som finns inom företaget på ett sätt som är trovärdigt.

Det är viktigt att skydda informationen genom dessa definitioner (MSB, 2015; Åhlfeldt, Spagnoletti & Sindre, 2007; Andronache & Althonayan, 2018; von Solms & van Niekerk, 2013):

- *Tillgänglighet* - att informationen finns tillgänglig när vi är i behov av den.
- *Riktighet* - att informationen är tillförlitlig, att den är korrekt och inte förstörd eller manipulerad.
- *Konfidentialitet* - att informationen endast är åtkomlig för behöriga personer.

Även Åhlfeldt et al. (2007) beskriver dessa definitioner, men lägger även till spårbarhet som ytterligare en definition. Spårbarhet innebär att operationer skall på ett tydligt sätt kunna härledas till en individ. Åhlfeldt et al. (2007) förklarar även att säkerhetsåtgärder som är tekniska eller administrativa krävs för att kunna uppnå dessa fyra definitioner. Säkerhet inom det administrativa innebär hantering av informationssäkerhet, såsom policyer, riskbedömningar, utbildning, strategier etcetera. Det krävs ett strukturerat arbetssätt vid planering och genomförande av säkerhet. Åtgärderna för att skydda information behöver anpassas efter behov, så att skyddet är tillräckligt bra. Skyddet får inte vara för svagt, för krångligt eller för dyrt (MSB, 2015). Konsekvenserna som kan inträffa vid ett skydd som är bristande är för höga för att åsidosättas. Informationssäkerhet som är bra och utefter behov bör vara en självklarhet för alla.

En stor mängd av olika typer av information hanterar vi dagligen (MSB, 2015). Det kan exempelvis vara personuppgifter, fotografier, betyg eller banksaldon, med andra ord information som för privatpersoner är viktig på olika sätt samt som individer är rädda om. Information som är värdefull skall behandlas med varsamhet, vilket är vad informationssäkerhet handlar om (MSB, 2015). Informationssäkerhet som privatperson kan innebära att föremål som ligger på skrivbordet eller vid samtal om information med känsligt innehåll, bör individer vara medvetna och tänka på att andra personer inte bör se, läsa eller höra informationen.

En annan förklaring av begreppet informationssäkerhet ges av SIS (2015). De hävdar följande:

*”Information är en grundläggande byggsten i en organisation. En arbetsdag utan tillgång till information är i princip ogenomförbar. Information ger kunskap till individer och organisationer och kan inhämtas, lagras, kommuniceras och bearbetas i olika former. En stor del av informationen är extra värdefull, och det kan innebära stora negativa konsekvenser för en organisation om t.ex. informationen går förlorad och inte finns till hands när den behövs. ”*
(SIS 2015, s.5)

Som framgår av det ovannämnda finns det olika definitioner av informationssäkerhet. Samtliga definitioner betonar betydelsen av att skydda information från obehöriga. I likhet med definitionerna av MSB (2015), Andronache och Althonayan (2018), Tu och Yuan (2014), SIS (2015) samt Åhlfeldt et al. (2007) är informationssäkerhet ett viktigt begrepp, som kan vara av stor relevans för företagen, även bidra med konsekvenser om det inte sköts rätt. Dessa författare är mycket inne på organisationer, där informationssäkerhet har en stor betydelse. Dock är betydelsen lika stor för privatpersoner också, vilket innebär att i denna studien kommer definitionen av informationssäkerhet utgå från definitionen av MSB (2015), där inriktningen är på privatpersoner specifikt.

## *2.2 Smartphones och dess användning idag*

Året 1983 gjorde det första kommersiella mobilsamtalet. Mobiltelefonen var mycket dyr på den tiden och vägde lite mer än ett kilo (Pocovnicu, 2009). Endast väldigt rika människor hade råd att kunna köpa en mobiltelefon. Sedan dess har en fantastisk utveckling skett som har gynnat mobiltelefonerna. Mellan 1992-2002 var mobiltelefonernas främsta utvecklingsmål att mobiltelefonens storlek skulle minska. Runt 2002 var telefonerna så små, att det inte längre var praktiskt att krympa mobiltelefonerna ännu mer från användarvänlig synpunkt (Pocovnicu, 2009). Det var runt denna tiden då fokuset började förändras och blev mer inriktat på mobiltelefonens funktioner, utöver röst- och SMS-textning. Den först svart-vita bilden blev utbytt mot färgdisplay och dess skärmupplösning blev allt högre och högre. Mobiltelefonanvändare kunde börja dra nytta av de nya funktionerna såsom internet, e-post, multimedia samt personlig organisatör, beskriver Pocovnicu (2009).

Enligt Burgbacher et al. (2014) är mobila enheter såsom smartphones avseende både för privat och professionellt bruk. Detta leder till att lagringsutrymmet och anslutningsmöjlighet som dessa enheter skall lagra, generera eller få tillgång till information som är känslig och privat. Dessutom används ofta dessa enheter i miljöer

som är osäkra, där de är mottagliga för obehörig åtkomst samt olika sorters attacker. Dessa enheter är även attraktiva för tjuvar, pågrund av dessa höga kostnad samt dess bärbarhet, menar Burgbacher et al. (2014). Även Pocovnicu (2009) menar på att de är attraktiva för tjuvar, eftersom dess funktionaliteter ökas och utvecklas ständigt, såsom personligt digitalt stöd, användning av digital bank och fjärrarbete etcetera. Pocovnicu (2009) förklarar även att en studie som har utförts där de flesta användarna av mobiltelefoner är medvetna om säkerhetsfunktionen med PIN-kod men mer än 50% av användarna utnyttjar inte denna säkerhetsfunktion av anledningen att brist på förtroende av funktionen eller pågrund av att funktionen är besvärlig. Majoriteten av dess användare tycker att en annan valmöjlighet av tillvägagångssätt för säkerhet skulle vara en bra idé.

Idag är mobila enheter en viktig del i vårt vardagliga liv, av den anledningen att de används för att kunna bruka många olika applikationer som är mobila. Genom att införa autentisering av biometri via våra mobila enheter, kan identitetsverifieringen bli starkare, av den orsaken att autentiseringsfaktorerna som karaktäriseras som ”något du har” samt ”något du är” sammanlänkas, beskriver Ferrag et al. (2019). Även Buriro et al. (2016) håller med om att mobila enheter används mycket i dagens samhälle. De menar även på att dessa enheter genererar och lagrar en oerhörd stor mängd av information som är känslig, samt att enheterna används för att utföra transaktioner som är säkerhetskritiska såsom mobila betalningar eller fjärråtkomst till intranät hos företag. De senaste åren har Smartphones genomgått en snabb och betydelsefull innovation. De senaste telefonernas generation innehar allt mer tekniska specialfunktioner, enligt Bao, Pierce, Whittaker och Zhai (2011).

## *2.3 Traditionella autentiseringsmetoder*

De traditionella autentiseringsmetoderna såsom grafiska lösenord, PIN-koder är sårbara av den anledning att autentiseringsprocessen kan observeras lätt förklarar Burgbacher, et al. (2014). Användningen av lösenord är ganska enkel och rak på sak, menar Pfleeger, Pfleeger och Margulies (2015). En användare anger någon slags del av identitet, exempelvis ett tilldelat användarID eller ett namn. Som fortsättning har systemet en förfrågan efter ett lösenord, och om lösenordet matchar med användarens identitet är tillträde in i systemet ett faktum. Om dessa två kombinationer inte matchar, blir användaren nekad och får försöka igen.

### 2.3.1 Pinkod

Den mest använda autentiseringsmekanismen i mobiltelefoner är PIN-koden, som består av hemliga siffror i rätt kombination, menar Burgbacher et al. (2014). PIN-mekanismen anses av många användare emellertid vara obekväm vilket leder till att användare inte nyttjar säkerhetsmekanismen och på så vis lämnar telefoner oskyddade. Burgbacher et al. (2014) förklarar även att användare kan även använda sig av svaga kombinationer,

dela PIN-koden till andra system samt skriva ned koden vilket är problem som är oundvikliga.

### 2.3.2 Attacker mot traditionella metoder

För att kunna förhindra attacker av olika slag mot system används lösenord som skydd mestadels (Bhanushali, Mange, Vyas, Bhanushali och Bhogle, 2015). Den autentiseringsmetod som är den mest använda metoden är textlösenord som normalt innehåller en serie av bokstäver, siffror samt specialtecken. Med dessa textlösenord brukar användaren ofta välja lösenord som är lätta för användaren att minnas, exempelvis telefonnummer eller födelsedatum. Denna teknik är användarvänlig, men är däremot känslig för attacker av olika slag, förklarar Bhanushali et al. (2015).

Harakannanavar, Renukamurthy och Raja (2019) förklarar kortfattat attacker som används mot autentiseringssystem som använder lösenord eller tokens enligt tabellen nedan:

| **Attacker mot autentisering med ”något du kan”** | |
|---|---|
| **Klientangrepp** | Lösenorden gissas & tokens är stulna. |
| **Host-attack** | Angriparen får tillgång till textfil som innehåller lösenord. |
| **Shouldersurfing** | Tjuvkikar över axeln för att se lösenord. |
| **Repudiering** | Angriparen påstår att tokens är felplacerad. |
| **Angrepp med trojanska hästar** | En falsk inloggningsskärm installeras för att kunna stjäla lösenord. |
| **Beteendeavsättning** | Med avsikt leverera ett felaktigt lösenord vid flertalet gånger vilket leder till att systemet misslyckas. |

*Tabell 1 - attacker gentemot traditionella autentiseringsmetoder*

Bhanushali et al. (2015) beskriver ytterligare en attack, Dictionary attack. I denna attack används en lista med en grundlig lista med ord,  som används för att lösenordet skall brytas. Denna lista med ord är de mest troliga som en användare väljer att använda som lösenord.

## *2.4 Biometri*

Faundez-Zanuy (2006) beskriver att ordet biometri härrör från de grekiska orden ”bios” som betyder liv och ”metrikos” som betyder mått. Detta hänvisar till vetenskapen som involverar statistiska analyser av biologiska egenskaper. Detta innebär att de säkerhetsapplikationer som använder identifiering av biometri, analyserar egenskaper som är mänskliga för identitetsverifiering samt identifiering. Användandet av biometri medför ett tillvägagångssätt som är lovande för säkerhetsapplikationer, med några fördelar i förhållande till de klassiska metoderna (Faundez-Zanuy, 2006). De klassiska

metoderna innebär att användaren har något som hjälpmedel till identifiering eller verifiering, såsom nyckel, kort etcetera eller något som användaren vet. En annan klassisk metod innebär lösenord, PIN-kod eller liknande vilket är något som användaren vet och måste komma ihåg. En egenskap som är tilltalande med de biometriska egenskaperna är att den utgår från något som användaren är eller något som användaren gör. Faundez-Zanuy (2006) förtydligar även att med denna teknik innebär det att användaren inte behöver komma ihåg någonting eller ha något med sig för att kunna identifiera eller verifiera dig.

Matyas och Riha (2003) och Pocovniu (2009) förklarar att det finns två sätt som biometri kan fungera:

- *Identitetsverifiering* = detta inträffar när användaren påstår sig vara registrerad i systemet genom att presentera ett inloggningsnamn eller ID-kort, detta kallas även för en till en-matchning. Systemet jämför den biometriska datan till posterna som finns i databasen som användaren har presenterat.

- *Identifiering* = kallas även för sökning, en till många-matchning eller igenkännande. Detta inträffar när identiteten av användaren är okänd. Systemet utför en matchning av den biometriska data som användaren presenterar mot alla poster som finns i databasen, eftersom användaren kan existera i databasen eller inte.

Ferrag, Maglaras och Derhab (2019) förklarar att med hjälp av biometri och dess identifiering blir det möjligt för slutanvändarna att använda attribut som är fysiska, istället för PIN-kod eller lösenord som en metod som med säkerhet ger åtkomst till en databas eller ett system. Denna teknik, *Biometri*, grundar sig i att ersätta konceptet som innebär att användaren behöver ha med sig något eller komma ihåg något, med att endast identifiera sig genom att vara den specifika användaren. Detta sätt att identifiera sig har blivit ett säkrare sätt att bevara information som är personlig. Ferrag et al. (2019) påpekar även att möjligheterna med identifiering med hjälp av biometri är enorma. Enligt Buriro, Crispo, DelFrari och Wrona (2016) har säkerhetsforskningens fokus flyttats till de autentisieringssystem som är baserade på biometri. Beteendebiometri speciellt, av anledningen att det ser attraktivt ut eftersom det är lätt att implementera på de flesta moderna smartphones eftersom endast den vanliga hårdvaran som tillhandahålls krävs.

### 2.4.1 Biometriska metoder

Den biometriska autentiseringsmetoder används av många datorsystem, såsom iris, fingeravtryck samt ansikts- och röstigenkänning. Även smartphones har börjat introducera denna metod in i systemet, däremot så system innebär flertalet utmaningar, påpekar De Luca och Lindqvist (2015).

#### Fingeravtrycksautentisering

Många smartphones idag använder fingeravtrycksautentisering för att underlätta upplåsning. Detta är en metod som är enkel att använda samt att det är en metod som

har låga kostnader vid implementation, menar De Luca och Lindqvist (2016). Denna teknik tittar på mönster som en fingertopp har, och är en av de mest etablerade metoderna inom de biometriska autentiseringsmetoderna, säger Faundez-Zanuy (2006). Han tillägger även att sannolikheten att hitta två personer med identiskt fingeravtryck är en på en miljard, vilket det har utförts beräkningar på.
Utmaningen med fingeravtrycksautentisering är att hastigheten av rekognitionen av den biometriska profil som presenteras försämras när fingret är vått och skrynkligt. Detta är något som forskningen måste åtgärda för vidare systemutveckling, menar Harakannanavar et al. (2019).

**Ansiktsigenkänning**
Av de biometriska autentiseringsmetoderna är ansiktsigenkänning förmodligen det sätt som är mest naturliga att utföra autentisering på mellan individer (Faundez-Zanuy, 2006). Denna biometriska metod kan förlita sig på videosekvens, stillbilder eller flera stillbilder. Harakannanavar et al. (2019) menar på att ansiktsigenkänning har utmaningar som måste åtgärdas för att systemet skall vara tillförlitligt. De utmaningar som förekommer är bland annat ansiktets rotation, problem med belysning vid autentisering, brukare som använder hatt, glasögon etc, samt att olika ansiktsuttryck försämrar systemets prestanda.
Även De Luca och Lindqvist (2015) påpekar dess osäkerhet. Det är idag möjligt att lura denna biometriska metod genom att visa upp en digital bild.

**Röstigenkänning**
Inom biometrisk autentisering är röstigenkänning en populär metod, förklarar Choudhury, Then, Issac, Raman & Haldar (2018). Metoden identifierar vokalkaraktären av personen som identifierar sig i samma ögonblick som personen uppger lösenordet eller passfrasen. Dock påverkas denna metod mycket av bakgrundsljudet.

**Iris-igenkännande**
Igenkänning av iris är en metod som har ännu högre säkerhet än fingeravtryck. Detta är dock en metod som är svår att använda i synnerhet om de lägsta kostnadsenheterna används, menar Faundez-Zanuy (2006). Iris-igenkännande ger en förmåga att skilja mellan individer som är mycket hög, även mellan det vänstra samt högra ögat på användaren. Harakannanavar et al. (2019) förklarar även att irisbilderna som fångas för autentiseringsprocessen analyseras i olika databaser som är skapade för iris-igenkänning.

Forskningen inom iris-igenkännande behöver fortsätta framåt och förbättras för att tillförlitligheten skall säkerställas mot viktiga faktorer, såsom glasögon, kontaktlinser samt vattniga ögon, fortsätter Harakannanavar et al. (2019) att tydliggöra.

### 2.4.2 Biometrins fördelar samt nackdelar
Att välja mellan de olika biometriska metoderna är inte enkel uppgift, påpekar Pocovniu (2009). Alla olika biometriska metoden bär med sig både positiva och negativa aspekter, och valet av metod för en applikation bör inte bara väljas utefter dess matchande

prestanda utan även utefter andra faktorer som bedömer om en biometriska metod anses som lämplig. Pocovniu (2009) förklarar även att ingen biometrisk metod är perfekt, ingen av de biometriska metoderna skulle tillfredsställa alla egenskaper till 100%.

Biometriska autentiseringsmetoders främsta fördel är att de gör precis det som ska; de skall verifiera användaren (Matyas & Riha, 2003). Biometriska egenskaper är väsentligen oföränderliga samt permanenta vilket innebär att användaren inte kan skicka dem till en annan användare lika enkelt som det är möjligt att göra med passerkort eller lösenord. Majoriteten av de biometriska metoderna grundar sig funktioner som inte kan glömmas bort eller tappas bort. Detta är en stor fördel för användaren, men även för systemadministratörer som undviker problem och kostnader som förknippas med förlorade, tillfälliga eller omfördelade kort, tokens eller lösenord, förklarar Matyas och Riha (2003).

*Sammanfattningsvis är de positiva delarna med biometri följande:*

- Autentiseringsmetoderna verifierar användaren
- Det är en personlig autentiseringsmetod, vilket innebär att det inte går att skicka personlighetsdrag till någon annan som vill ha åtkomst
- Det går inte att tappa bort, vilket leder till problem och kostnader minskar

Biometriska metoder och dess system kan bryta mot användarens integritet, fortsätter Matyas och Riha (2003). Biometriska egenskaper är uppgifter som är känsliga samt innehåller personuppgifter. Även en förlust av anonymitet innebär användningen av biometriska system, genom att biometriska system kopplar ihop olika användaråtgärder till en enskild identitet trots att användaren kan ha flera identiteter när metoderna för autentisering är baserade på något användaren har eller vet. Biometriska system kan även tyckas vara påträngande eller personligt invasiva enligt användare. Vissa individer tycker inte om att röra vid saker som andra individer har berört, eller att fotograferas (Matyas & Riha, 2003). Dessa problem och dess tillhörande problematik är något som behövs lösas innan biometriska system kan användas på ett säkert och pålitligt sätt.

En nackdel som är av stor betydelse är frustrerade användare vid nyttjandet av fingeravtrycksigenkänningssystem, menar Mayron, Bahr och Hausawi (2013). Vid system som använder fingeravtrycksigenkänning kan dålig användbarhet minska prestandan, som i sin tur resulterar i frustrerade användare. Att användarna trycker sig finger på ett felaktigt sätt mot sensorn är ett fel som inte kan förvärvas då det orsakas av användarna. Temperaturen i miljön kan även vara en påverkande faktor för att sensorn skall känna av fingeravtrycket. Mayron et al. (2013) menar även på att system som är användbart riktar användarna samt systemoperatörerna på ett effektivt sätt för att presentera dess fingeravtryck på ett effektivt sätt kan bidra till minskning av tekniska fel och en förbättras säkerhet. När dessa användbarhetsrelaterade fel som är tekniska

minskas och förbättras säkerhet kan system med fingeravtrycksigenkänning effektiviseras, och användas på ett mer effektivare och tillfredställande sätt.

Enligt Choudhury et al. (2018) kan inkräktare presentera biometri framför sensorerna som är falsk. Exempelvis kan fingeravtryck av ett falskt finger som sedan presenteras framför sensorerna eller framställa bilder av den berättigade användaren framför kameran för att kringgå systemet med ansiktsigenkänning. Vid iris-skanner kan inkräktaren bära ena viss sort av linser för att kringgå skannern som läser av irisen, tillägger Choudhury et al. (2018). Detta gäller även för ansiktsigenkänning, där användaren behöver ta bort eventuella glasögon eller liknande för att systemets noggrannhet ska förbättras, enligt Mayron et al. (2013).
Dessa farhågor med framkallning av falska fingeravtryck har enligt Dobos (2018) bekräftats av amerikanska forskare vilket har utvecklat en metod som konstruerar fingeravtryck av syntet, vid namn Deep Master Prints. Forskarna påbörjade arbetet för att skapa fingeravtryck som är partiellt falska i ett försök att lura sensorerna vid biometrisk autentisering. Nu har forskarna tagit resultaten för studien ett steg längre och använder maskininlärning och Artificiell Intelligens (AI) för att skapa falska fingeravtryck i fullskaliga bilder (Dobos, 2018). Forskarna menar på att dess arbete visar att det är fullt möjligt att det är möjligt att kunna förfalska biometriska metoder och kringgå systemet.

*Sammanfattningsvis är de negativa delarna med biometri följande:*

- Biometri kan bryta mot användarens integritet
- Kan leda till frustrerade användare vid användning
- Biometriska egenskaper är uppgifter som är känsliga
- Möjligt att förfalska biometriska egenskaper för att kringgå systemet

### 2.4.3 Lagring av den biometriska datan

Enligt Prabhakar, Pankanti och Jain (2003) kan biometrisk data användas till annat än vad den biometriska datan är ämnad för att användas till, vilket är en osäkerhet vid användning. Detta innebär att följderna av användning av den biometriska metoden kan leda till inskränkning av rättigheter i olika former, förslagsvis användarens personliga vanor eller hälsotillstånd är i riskzonen. Den biometriska datan kan även avslöja användarens identitet, mot användarens vilja. Om användaren, av någon anledning, vill hålla sin identitet hemlig och vara anonym kan detta vara i riskzonen vid användning av någon av de biometriska metoderna (Prabhakar et al., 2003). Med andra ord kan en identifiering utföras utan att individen är varse om identifieringen som sker, vilket leder till att den anonymitet som önskas av individen försvinner, enligt Prabhakar et al. (2003).

Känsliga uppgifter kan komma att avslöjas om de biometriska egenskaperna lagras i databasservern direkt utan att säkerhetsmetoder av stark karaktär används, menar Nguyen & Dang (2019). De autentiserande servrarna bör inte vara trovärdiga vid bearbetning av användarns biometriska egenskaper, och dessa serverar och dess tillhörande förtroende bör diskuteras mer. En annan viktig komponent vid lagring av de biometriska egenskaperna är säkerheten kring nätverket (Nguyen & Dang, 2019). När processen för autentisering sker över ett nätverk som anses som osäkert finns det möjlighet för alla som är nyfikna närma sig den information som består av biometriska egenskaper.

Biometri och dess tillhörande egenskaper går inte att återkallas vid användning. Detta innebär att om en biometriska egenskap vid något tillfälle utsätts för fara, kommer egenskapen alltid att vara utsatt för fara (Prabhakar et al., 2003). En användare har ett begränsat antal av egenskaper som kan användas vid biometriska metoder, såsom ett biometriskt ansikte eller 10 fingrar för att påvisa ett exempel. Dessa egenskaper är inte lätta att ersätta, som ett lösenord är (Prabhakar et al., 2003 & Nguyen & Dang, 2019). Om ett lösenord för ett kreditkort äventyras, kan lösenordet bytas ut och ett nytt kort med nytt kortnummer börja användas som ersättning. De biometriska egenskaperna kan användas till olika slags tillämpningar, kan en bedragare komma över en användares biometriska egenskap för att sedan använda den vid andra användningsområden, fortsätter Prabhakar et al. (2003). Nguyen och Dang (2019) tillägger även att en bedragare kan stjäla en mall av fingeravtryck i databasen där dessa mallar lagras för att sedan användas för att få åtkomst till den specifika personens journaler eller kriminalregister etcetera.

# 3. Problemområde

Mobiltelefonen har gjort en otrolig utveckling sedan det första kommersiella mobilsamtalet utfördes år 1983, som Pocovnicu (2009) beskriver. Vid den tiden var det endast de rika som hade råd att köpa en mobiltelefon. Numera är de mobila enheterna istället en viktig del av det vardagliga livet, förklarar Ferrag et al. (2019) Burgbacher et al. (2014) hävdar att mobila enheter som till exempel smartphones används primärt i privata men också professionella sammanhang. Detta innebär att smartphones besitter information som är privat eller känslig, samt att dessa smartphones ofta används i osäkra miljöer där de är tillgängliga för obehöriga som utför olika sorters attacker för att komma åt den information som finns i enheten Burgbacher et al. (2014). Dessa enheter är attraktiva för tjuvar, av den anledning att de ständigt utvecklas och får nya funktioner samt att de innehåller personligt stöd såsom digital bank med mera.

Pocovnicu (2009) förklarar att en studie har utförts där användarna av dessa mobila enheter är medvetna om säkerhetsfunktionen med PIN-kod anser hälften av användarna att säkerhetsfunktionen är besvärlig samt att de saknar förtroende för funktionen, vilket leder till att de användarna inte använder denna funktion med PIN-kod. Pocovnicu (2009) fortsätter med att förklara att merparten av användarna från denna studie tycker att fler valmöjligheter av tillvägagångssätt av säkerhetsfunktioner skulle vara en bra lösning.

Grafiska lösenord, i egenskap av lösenord eller PIN-koder är processer som är av de traditionella autentiseringsmetoderna vilket är sårbara metoder som kan observeras lätt av obehöriga. Burgbacher et al. (2014) förklarar även att den autentiseringsprocess i mobiltelefoner som är den mest använda är PIN-koden. Många användare av PIN-mekanismen betraktar den specifika säkerhetsmekanismen som obekväm och lämnar istället enheterna oskyddade. Vid användning av biometri resulterar i ett tillvägagångssätt vilket verkar lovande för säkerhetsapplikationer, förklarar Faundez-Zanuy (2006). En tilltalande egenskap med de biometriska egenskaperna är att autentiseringen bygger på något som användaren är eller något som användaren gör. Med den biometriska metoden behöver användaren inte komma ihåg något, eller ha något med dig för att kunna identifiera eller verifiera sig, vilket kan vara problematiskt i den traditionella autentiseringsmetoden (Faundez-Zanuy, 2006).

Denna forskning syftar till att få en ökad förståelse inom området av autentiseringsmetoder som inkluderar privatpersoner och deras användning av biometri vad det gäller smartphones. Forskningen syftar till att fånga upp perspektiv som privatpersoner bedömer autentiseringsmetoder som betryggande respektive otillräcklig som en säkerhet för privatpersoners bruk av smartphones och den tillhörande informationssäkerheten som autentiseringsmetoderna skall bidra till. Med hjälp av denna forskning kan perspektiv inom användningen av autentiseringsmetoder fångas, där privatpersoner har möjligheten till att yttra deras personliga åsikter kring dess användning. Forskningen kan även bidra till upptäcka förbättringsförslag av de autentiseringsmetoder som används av privatpersoner.

## *3.1. Frågeställning*

Utgångspunkten för denna forskning där granskning och analysering skall ske har följande frågeställning formulerats:

- *Vad påverkar en användares val av biometriska metoder vid användning av en smartphone?*

Denna frågeställning är av både relevans och betydelse av den anledning att de biometriska autentiseringsmetodernas tillämpas allt mer som funktioner som skall styrka informationssäkerheten gentemot privatpersoners bruk av smartphones, vilket är en del av vårt vardagliga liv.

## *3.2. Avgränsningar*

För att studien inte skall bli allt för omfattande samt att tidsramen skall hållas kommer en avgränsning att ske till privatpersoner. Däremot finns privatpersoner allestädes, vilket innebär att ännu en avgränsningar har skett till närliggande avgränsningar.

Den primära inriktningen av studien innefattar smartphones, vilket leder till att studien avgränsar sig ytterligare, av den anledning till den angivna tidsramen som har angetts.

## *3.3. Förväntat resultat*

Forskningen förväntas frambringa ett resultat där privatpersoner yttrar dess synvinklar, åsikter och perspektiv kring de biometriska autentiseringsmetoderna, samt anledning till val av en viss specifik autentiseringsmetod. Förväntningarna på resultatet är även att få fram privatpersoners perspektiv kring huruvida säkra de känner sig vid autentiseringsmetoderna, samt vad privatpersonernas primära fokus ligger på vid informationssäkerheten.

Denna studie avser att identifiera styrkor och svagheter som privatpersoner upplever med biometriska metoder vid användning av smartphone. Resultatet av detta kan användas för att utveckla befintlig forskning inom området, men även en fördjupad förståelse för privatpersoners åsikter kring dessa metoder och användning.

# *4. Metod*

*I detta kapitel presenteras den metodansats som lämpas bäst för att utföra denna forskning. Här presenteras även delmoment av metodansatsen att presenteras som kommer att bidra till insamling av information för att på ett bra och korrekt sätt genomföra studien. Sedan redogörs även det faktiska utförandet av den valda metoden, för att kunna få en skildring på hur processen var planerad respektive hur den faktiskt realiserades.*

## *4.1 Val av metod*

Berndtsson, Hansson, Olsson, och Lundell (2008) beskriver att varje mål kan uppnås genom olika slags metoder. Med hjälp av en metod kan vi på ett systematiskt sätt arbeta och lyckas ta itu med problemet. Genom att angripa projektets mål dess associerade mål måste en passande metod tillämpas så att målsättningen uppnås. Detta innebär inte att samma metod skall användas för att uppnå alla mål, snarare att olika metoder väljs utefter de olika målsättningarna. Berndtsson et al., (2008) beskriver även att när ett val av metod utses innebär det att varje metod är en slags strategi eller ett verktyg för att säkerställa att komma fram till slutmålen och att de uppnås. Vid val av metod bör övervägningar ske, där frågan är om det slutliga målet kan uppnås med hjälp av den utvalda metoden som eftersträvas utan även undersöka tillvägagångssättet som metoden använder för insamling av data.

Enligt Oates (2006) inkluderar kvalitativ data all slags data som är icke-numeriskt, såsom ord, ljud, bilder etcetera. Kvalitativ data kan finnas i band från intervjuer, företagsdokument, dagböcker och webbsidor för att bara nämna några få. Kvalitativ data är den huvudsakliga typen av data eller bevis som genereras av åtgärdsforskning, fallstudier samt etnografi. Detta är tillskillnad från den kvantitativa datan, som är evidensbaserad eller av siffror (Oates, 2006). Den viktigaste typen av data inom den kvantitativa metoden genereras av enkäter eller experiment.

Den kvalitativa metoden har sina rötter i samhällsvetenskapen, och är främst intresserad av att få en ökad förståelse för ett visst området, snarare än att berätta orsaken om området (Oates, 2006). Denna studie vill fånga upp privatpersoners perspektiv och åsikter kring biometri, därav faller valet på den kvalitativa metodansatsen, av den orsak att få en ökad förståelse för området. Med hjälp av intervjuer kan forskaren fånga upp åsikter som annars är svåra att fånga vid tillämpning av andra datainsamlingsmetoder (se kapitel 4.2 för genomförande av studien).

### 4.1.1 Kvalitativ metodansats

Under detta kapitel presenteras metoder som är lämpliga för datainsamling.

### 4.1.2 Litteratursökning

Litteratursökning innebär att en systematisk undersökning sker utefter ett problem, vilket i sig innebär att en analys sker av källor som är publicerade. Litteratursökning sker även utefter ett specifikt syfte, menar Berndtsson et al. (2008). Det finns flertalet olika tekniker som kan tillämpas för att kunna avgöra vilka källor som är av intresse för forskningen. Två av dessa tekniker som kan tillämpas är bibliografiska databaser där forskaren använder sig av nyckelord för att kunna hitta relevanta källor (Berndtsson et al. 2008). Även tidskrifter och konferenshandlingar är en teknik, där sökning efter relevanta artiklar sker på tidskrifters webbplats.

En svårighet som är relaterad till litteratursökning är att veta när sökningen är fullständig (Berndtsson et al. 2008). Att veta när sökningen av litteratur är fulländad är förvisso svårt att veta, men forskaren bör alltid se till att ha tillräckligt med material angående ämnet som det skall forskas kring. Det är även av stor vikt att att de källor som används är av relevans för ämnet, vilket kan granskas genom systematisk analys samt en noga granskning av varje enskild källa. För att veta om litteraturen är relevant kan forskaren kolla efter ämnet som undersökningen utförs utefter, tillförlitligheten samt publikationsdatum (Berndtsson et al. 2008).

Berndtsson et al. (2008) menar även på att det är viktigt att forskaren är uppmärksam samt självreflekterande när det gäller sin personliga kunskap. Det är även viktigt att forskaren eftersträvar ett synsätt som är opartiskt och objektivt i urvalet av litteratur, men även i delarna där resultat och analys skall lyftas fram.

### 4.1.3 Intervjuer

Enligt Berndtsson et al. (2008) kan intervjuer utföras på flertalet olika sätt och med olika mål. Vid beslut av en lämplig metod att utföra intervjuer på finns det flertalet olika infallsvinklar som behövs vägas in innan ett slutgiltigt beslut fattas. Olika typer av intervjuer har varierande styrkor och svagheter, som är sammanlänkade till din egna förmåga som forskare att åta sig en specifik teknik av intervju. Oates (2006) förklarar även att intervjuer är en speciell typ av konversation, men att den har en uppsättning av antaganden som en normal konversation inte har. Normalt sett har en person en avsikt att utföra intervjun vilket är att hämta information från den andra parten. Detta innebär att konversationen inte förkommer av en slump, utan att konversationen är planerad i förväg av forskaren (Oates, 2006). Intervjuer är en metod som är passade vid datainsamling när en studie vill erhålla detaljerad information, undersöka känslor eller erfarenheter som inte är lätta att observera eller vid frågeformulär med förbestämda frågor.

Det finns tre olika typer av intervju-typer (Oates, 2006):

- *Strukturerade intervjuer:* Förutbestämda, standardiserade och identiska frågor till varje intervju. Frågan ställs till respondenten för att sedan anteckna svaret.

- *Semistrukturerade intervjuer:* Här används fortfarande en lista av de teman som intervjun skall bestå av samt frågor som skall ställas, men ordningen på frågorna kan variera beroende på respondentens svar samt tilläggsfrågor kan ställas om intervjun kommer in på ämnen som inte är förbestämda.

- *Ostrukturerade intervjuer:* Forskaren har ingen eller liten kontroll över vad som lyfts under intervjun. Ämnet introduceras för respondenten för att sedan låta respondenten tala fritt om ämnet och forskaren försöker att inte avbryta eller vara för påträngande.

Hänseenden som är viktigt att tänka vid intervjuer som metod av datainsamling är att även välja respondenter som är relevanta för studiens ämne (Berndtsson et al., 2008). Det är även av stor betydelse att flödesstrukturen på intervjun planeras innan, samt att ha med i åtanke att inspelningsutrustning kan vara fördelaktigt om det är under intervjun är svårt att hinna med att notera vad som sägs. Med hjälp av inspelningsutrustning kan forskaren lyssna noga på vad respondenten säger, samt att inspelningsutrustningen bidrar till att en återgivning av intervjun som är exakt kommer att finnas samt det kommer att finnas möjlighet till att använda sig av direktcitat som respondenten har givit under intervjun, vilket annars kan vara svårt att fånga upp vid endast notering (Patton, 2015).

Patton (2015) påpekar även att det är av stor relevans att undvika frågor som respondenten har möjlighet till att svara ja/nej på. Genom att ställa öppna frågor kan forskaren fånga resonemang kring ämnet från respondenten, men även möjlighet för forskaren att ställa följdfrågor (Patton, 2015). Vid följdfrågor kan ytterligare information yttras, av den anledning att människor besitter information som är icke-verbal och kan komma från vid följdfrågor.

I denna studie är semistrukturerade intervjuer planerad att användas för insamling av data. Intervjuer kan bidra till att fånga upp privatpersonernas erfarenheter eller känslor angående biometriska autentiseringsmetoder, av den anledning att avsikten med studien i stort är att fånga åsikter och perspektiv från parter som har erfarenhet inom området. För att kunna täcka de viktigaste punkterna, men ändå kunna behålla möjligheten till att ställa tilläggsfrågor är semistrukturerade intervjuer en ”typ” som är lämplig att använda vid denna studie.

### 4.1.4 Analys av insamlad data

Innehållsanalys, som skall tillämpas i denna studie (se kapitel 4.2.3), refererar till att räkna återkommande ord eller teman som finns i en text, text som har samlats in från datainsamlingen (Patton, 2015). Mer generellt innebär innehållsanalys att analysera en text såsom dokument, intervjutranskript eller dagböcker. Innehållsanalysen hänvisas även till den kvalitativa metodansatsen, som samlar på sig en omfattande volym av insamlad data, och på så sätt kan forskaren identifiera sammanhang och meningar.

Vid användning av den kvalitativa metodansatsen, kan den kvalitativa datan som har samlats in kodas för att slutligen skapa en teori, menar Oates (2006). För att den

kvalitativa datan skall kunna analyseras måste den insamlade datan delas in i beskrivande kategorier, såsom relevanta teman. Men datan kan klassificeras in till flera olika kategorier. Genom detta sätt kan antalet av de möjliga insikter som materialet presenteras öka, säger Ryen (2004). Denna process är tidskrävande, men kan även medföra struktur, ordning och mening åt datan som har samlats in. Däremot är det viktigt att först få den insamlade datan i redo för att analyseras, förklarar Oates (2006). Vid analys är det lättare att den insamlade datan är i samma eller liknande format, samt att ljudband som eventuellt har använts vid intervju har transkriberats. Det är av stor relevans för arbetet att förstå att en intervju kan kräva nästintill 4-5 timmars transkribering (Oates, 2006). När denna process är genomförd kan forskaren börja läsa igenom materialet för att få en överskådlig syn av informationen som har samlats in.

*Fördjupning:* När intervjuerna är genomförda är det dags att påbörja transkriberingen av ljudfilerna till text. Rosenthal (2016) menar även på att detta är en del i processen som kan vara mycket lång, men helt beroende på den kvalitén av inspelningarna. Detta är även en del i processen som är nödvändig för att behålla respondenternas konfidentialitet (Rosenthal, 2016). Vid fördjupningens skede handlar det om att sätta sig in och förstå det material som har samlats in. Vid denna process är det till sin fördel att samma person som har utfört intervjuerna även transkriberar, i annat fall kan ansiktsuttryck försummas. I händelse av att det är en annan person som utför transkribering är det viktigt att förtydliga att allt skall skrivas ordagrant samt ta med pauser eller skratt etcetera (Trost, 2005). Om personen som transkriberar inte tar med pauser exempelvis, går forskningen miste om helhetsintrycket samt att det kan bli svårare att fånga förståelsen för respondenterna.

*Kodning:* I kodningsfasen delas den insamlade datan in i olika områden, som berör olika ämnen. Detta kan innebär att markeringar sker i marginalen av dokumentet där den transkriberade datan finns på (Oates, 2006 *&* Patton, 2015). Under denna fas är det även viktigt att komma ihåg att dessa områden som datan delas in inte är avgörande för arbetet, utan kan kan ändras senare om så önskas Oates (2006). Patton (2015) menar på att överstrykningspennor, med olika färger per kategori kan vara hjälpsamt för att strukturera upp de olika områden som upptäckts. Ett annat alternativ kan även vara att använda självhäftande prickar i olika färger eller post-it lappar för att strukturera.

Generellt sett identifieras ett stort antal koder under denna process, samt att många av dessa koder överlappar varandra i dess avsikter, menar Rosenthal (2016). Här krävs en tydlig känsla av sammanhanget av datan som skall analyseras.

*Kategorisering:* I denna fas är det dags att börja förfina de olika områden som har framkommit under tidigare fas. Vissa områden kan vara för stora, och kan behövas brytas ned i subkategorier. Vissa av de upptäckta områdena kan vara sällsynta, som istället kan kombineras in till andra kategorier, enligt Oates (2006). Här arbetar sedan forskaren fram och tillbaka mellan den insamlade datan och de indelade kategorierna för att verifiera de olika betydelsefulla kategorierna samt noggrant granskar de olika placeringarna av den insamlade datan i de indelade kategorierna, säger Patton (2015).

*Identifiering av tema:* Till sist skapas teman utifrån de kategorier som har frambringats under tidigare steg (Patton, 2015). Ett tema är mer än en kategori som den insamlade datan har delats in i under tidigare steg i processen. Generering av teman kräver testning av data och med teorin som är av relevans för studien av dess förklaringar. Den omfattande empiriska analysen samt den teoretiska analysen ger följaktligen en mer djup och omfattande litteratur. Det är alltså i detta steg i processen som forskaren beslutar sig att processen för analys av den insamlade datan är avslutad (Patton, 2015).

Efter att alla dessa steg är utförda, kan även forskaren kontakta den intervjuade personen för att utföra en kontroll, där respondenten får läsa igenom och godkänna det transkriberade dokumentet. Denna kontroll är ett sätt som hjälper till att säkerställa processens trovärdighet, avslutar Rosenthal (2016).

### 4.1.5 Etiskt beaktande

Forskning är både viktigt och nödvändigt för utvecklingen av samhället och individer (Vetenskapsrådet, 2002). Samhället och medlemmarna i samhället har av den anledningen ett berättigat krav på att forskning bedrivs samt att den fokuserar på frågor som är väsentliga och håller en hög kvalitet. Detta kallas för *forskningskravet* och innebär att kunskaper som är tillgängliga utvecklas och fördjupas och förbättring av metoder sker (Vetenskapsrådet, 2002). Medlemmar i samhället har samtidigt ett krav som är berättigat på skydd mot olämplig insyn, som exempelvis i individens livsförhållande. Individer får heller inte utsättas för fysisk eller psykisk skada, kränkning eller förödmjukelse. *Individskyddskravet* som det kallas, är en utgångspunkt för forskningsetiska överväganden (Vetenskapsrådet, 2002).

Individskyddskravet kan förtydligas i fyra allmänna huvudkrav. Dessa krav kallas för samtyckeskravet, informationskravet, nyttjandekravet och konfidentialitetskravet (Vetenskapsrådet, 2002). Dessa forskningsetiska principerna har som målsättningar att ge regler för förhållandet mellan undersökningsdeltagare eller uppgiftslämnare och forskare, samt att vid eventuellt konflikt kan en god avvägning ske mellan individskyddskravet och forskningskravet.

*Samtyckeskravet* - Respondenterna i forskningen har rätten att bestämma själva över sig medverkan, och kan avbryta sin medverkan närsomhelst under forskningen.

*Informationskravet* - Forskaren skall informera respondenterna om forskningens syfte.

*Nyttjande kravet* - De insamlade uppgifterna om respondenterna får endast använda till den specifika studiens ändamål.

*Konfidentialitetskravet* - Uppgifter om respondenterna i forskningen skall behandlas med konfidentialitet, samt att personuppgifterna skall förvaras så att obehöriga ej kan få åtkomst till personuppgifterna.

## *4.2 Genomförande*

*I detta underkapitel presenteras hur den vetenskapliga metodansatsen har genomförts under studiens gång.*

### 4.2.1 Litteratursökning

Studien påbörjade genom att granska litteratur som är relevant för studiens valda ämne som har publicerats. Detta utfördes för att kunna få en bakgrund av ämnet, men även för att kunna få en uppfattning av vad tidigare forskning har kommit fram till och vad de påpekar. Genom litteratursökningen kom frågeställning fram, av den anledning att frågeställningen inte var till hundra procent fastställd vid studiens början samt att det var med hjälp av litteratursökningen som frågeställningens vinkling kom till.

För att kunna besvara frågeställningen var det av stor relevans att hitta tillräckligt med empiri för att kunna besvara studien syfte. Detta innebär att flertalet artiklar av vetenskapligt syfte, inom studiens utvalda område, granskats för att sedan ställas med eller mot varandra.

Urvalsprocessen vid insamling av litteratur till bakgrunden har Högskolan i Skövdes databaser använts. De databaser som denna studie har använt vid anskaffning av litteratur är *IEEE Xplore*, *arXiv* samt *Web of Science*. Utöver dessa databaser har även Google Schoolar använts, som är en sökmotor över många olika databaser, vilket även där har resulterat i artiklar som har publicerats på nämnda databaser ovan.

Sökord som har använts vid den vetenskapliga litteratursökningen är de som presenteras i tabell 2 nedan:

| | |
|---|---|
| *Biometric authentication* | *Biometric security technology* |
| *Traditional authentication* | *Biometric pros and cons* |
| *Smartphone / Smartphone users* | *Password* |
| *Authentication methods* | *Biometric concerns* |

*Tabell 2 - Använda sökord vid litteratursökning*

Dessa sökord har använts separat men även i kombination för att kunna hitta mer specifika artiklar som behandlar det utvalda området.

Fortsättningsvis har artiklarna valts ut efter det övergripande ämnet autentisering, både traditionell samt biometrisk för att kunna fånga upp de olika synvinklar och perspektiv på de olika metoderna som studien behandlar. Årtalet för artiklarnas publicering har även uppmärksammats men av anledning att detta område, speciellt biometri, är relativt nytt har årtalet inte varit högsta prioritet, men har varit en synpunkt att ta i beaktande vid sökningen för att hålla forskningen så aktuell som möjligt.

Det skall även tilläggas att artiklar från tidigare kursen har använts, främst vid redogörande av vad informationssäkerhet innebär generellt. Även populärvetenskaplig litteratur har använts för att fånga läsaren samt att läsaren skall få en lättare förståelse av vad ämnet är har använts. Dessa artiklar har sökts på Google, med sökorden *"Biometri i filmer"* samt *"lura biometriska metoder"*.

Precis som Berndtsson et al. (2008) förklarade var det svårt att veta under arbetets gång när tillräckligt med material samlats in vid litteratursökningen. Det blev slutligen många insamlade artiklar som inte fyllde någon slags funktion eller bidrog med något av värde till studien av den anledning att arbetets gång blev studiens syfte mer inriktad och fick ett mer inriktad område än vid litteratursökningens början.

### 4.2.2 Urval av respondenter samt utförande av intervjuer

För att inte låsa sig vid en specifik generation eller åldersgrupp, har ett brett urval av privatpersoner deltagit i forskningen (Patton, 2015). Genom att ha en så bred ålderskategori som möjligt ger även det fler möjligheter till att fånga upp olika åsikter och synpunkter, av den anledningen att med förutfattad mening att olika åldrar använder sin smartphone till olika saker, vilket i sin tur kan bidra till att privatpersonerna har olika slags information som de anser vara av värde och vill skydda.

Den främsta avgränsningen som har skett är att enbart ha privatpersoner som respondenter, då denna forskning handlar om hur privatpersoner påverkas av biometriska metoder och hur de uppfattar dess informationssäkerhet.

Ytterligare avgränsningar har skett efter dessa privatpersoner som respondenter, är att en förutsättning är att privatpersonen skall ha en smartphone med funktionen ansiktsigenkänning, tidigare haft fingeravtrycksläsare eller vice versa. Genom att utföra denna avgränsning kan denna studie fånga upp olika vinklar angående det valda ämnet, samt kunna samla in information och åsikter kring autentiseringsmetoderna.

För att kunna hitta respondenter som passar in på avgränsningar kommer anmälan av intresse för deltagande att placeras ut på utvalda platser där privatpersoner vistas, samt i olika åldrar. Platser som dessa är bibliotek, företag samt Högskolan i Skövde. Ett önskemål kring antalet respondenter är på ett ungefär 10 privatpersoner, beroende på hur många som fyller i anmälan av intresse för deltagande till att medverka i denna studie. Urvalet bygger på frivilligt deltagande, vilket innebär att det är svårt att förutbestämma ett exakt antal av respondenter.

För att kunna hitta respondenter till forskningen som passade den avgränsning som ett i urvalet som har beskrivits placerades anmälan av intresse för deltagande ut på två olika ställen (se bilaga 1). Dessa ställen valdes ut av den anledning att det fanns olika ålderskategorier på dessa platser, för att kunna fånga dessa olika åldrar som respondenter. Anmälan om intresse för deltagande i studien låg utplacerade i matsalen på det utvalda företaget samt på flera olika ställen på biblioteket i Lidköping av den anledning att biblioteket är stort, samt att det var svårbedömt var flest folk vistades i

biblioteket. Efter en vecka hämtades anmälan av intresse in, för att se resultatet av intresserade. Önskemålet var att ett tiotal respondenter hade anmält sig som intresserade men så blev inte fallet. Därav placerades ytterligare en anmälan av intresse för deltagande ut på en tredje plats, vilket blev ett utbildningscenter. Dessa tre platser genererade tillsammans ett önskvärt antal av deltagare till studien.
De intresserade kontaktades för att boka ett tillfälle för intervju.

Utförandet av intervjuerna skedde på gemensamt bestämd plats, vilket i majoriteten av fallen blev på den plats som anmälan av intresse för deltagande hade placerats, för att förenkla för både respondenten samt forskaren. De övriga föreslog själva att intervjun kunde utföras på dess kontor.

Som tidigare planerat utfördes intervjuerna utefter den semistrukturerade intervju-typen, som innebar att intervjun genomfördes med vissa stängda frågor, men även öppna frågor för att kunna ställa följdfrågor, som (Oates, 2005) beskrev. Tio intervjuer genomfördes, vilket var den önskvärda siffran i antalet intervjuer. Mer information angående respondenterna och dess pseudonym presenteras nedan (se tabell 3). Inledningen av intervjun började med att förklara för respondenten om dess etiska rättigheter, såsom att respondenten har möjligheten till att avsäga sig sin medverkan när som helst under studiens gång, respondentens rätt till anonymitet, samtycke från respondenten inhämtades samt att dessa uppgifter och information som samlas in för forskningen endast kommer att nyttjas för forskningens ändamål. Fortsättningsvis ställdes de intervjufrågor som var förberedda, som framtogs utefter den information som framkom under litteratursökningen som skedde tidigare i studiens process.

Under intervjutillfällena ställdes frågor som berörde de olika områden och punkter (se bilaga 2), dock ändrades ordningen på intervjufrågorna eller att vissa frågor uteslöts av den anledning att respondenten självmant hade svarat på detta under en annan fråga, vilket ledde till att det blev flera frågor besvarade under en fråga. Däremot tillkom även andra frågor som inte var planerade, men även dessa frågor som tillfördes bidrog med relevant information till forskningen. Tidsåtgång per intervjutillfälle varierade mellan 30-45 minuter, vilket var en tillräcklig tid för att hinna ställa alla frågor samt följdfrågor som lämpades för det specifika intervjutillfället.

Majoriteten av intervjuerna spelades in där respondenterna gav sitt godkännande till inspelning, dock utfördes en intervju utan inspelning av den orsak att respondenten inte godkände inspelning av intervjun av privata skäl. Under den intervjun upptogs informationen endast av anteckningar, vilket innebar att det var av stor vikt att forskaren var tvungen att vara extra uppmärksam och fokuserad, för att säkerställa att allt antecknades.

Därefter transkriberades inspelningarna samt den intervjun som endast utfördes med anteckningar.

| Respondent | Ålder | Yrke | Plats för upphittande |
|---|---|---|---|
| **R1** | 28 | Projektledare på elektrikerföretag | Lidköpings bibliotek |
| **R2** | 25 | Mammaledig/Undersköterska | Lidköpings bibliotek |
| **R3** | 38 | Industriarbetare | Utvalt företag |
| **R4** | 27 | Mäklare | Lidköpings bibliotek |
| **R5** | 27 | Student | Utbildningscenter |
| **R6** | 36 | Student | Utbildningscenter |
| **R7** | 24 | Student | Utbildningscenter |
| **R8** | 39 | Industriarbetare | Utvalt företag |
| **R9** | 22 | Industriarbetare | Utvalt företag |
| **R10** | 33 | Student/Snickare | Utbildningscenter |

*Tabell 3 - Översikt över respondenter (R).*

### 4.2.3 Utförande av dataanalys

För att kunna få fram ett resultat av den insamlade datan utfördes en transkribering. Transkriberingsfasen från dess början till slut var en mycket tidskrävande process, och för att vara så effektiv som möjligt utfördes transkribering av intervjuerna så fort som möjligt efter varje intervju utfördes, av den anledning att kunna få med respondenternas ansiktsuttryck eller signaler, som Trost (2005) förklarar. Intervjuerna utfördes under en relativt bred tidslinje, vilket även det bidrog till att tiden emellan de inbokade intervjuerna användes till att transkribera, vilket bidrog till att i slutet av intervjufasen var den omfattande transkriberingsfasens första steg relativt klart. Detta innebär att transkribering från inspelningsmaterialet har förts ned på papper. Här bestämdes även formatet på informationen som skall transkriberas ytterligare i efterkommande faser, av den anledning att det anses vara lättare om datainsamlingens information är av samma format (Oates, 2005).

Fortsättningsvis utfördes steg 2, vilket innebär fasen *kodning*. Här delades den insamlade datan in i olika delar, olika specifika ämnen som informationen berörde. De olika ämnena märktes ut och förtydligades för att underlätta. Redan under denna fas kunde koder gå om lott i dess syfte, vilket Rosenthal (2016) förklarade. Kodningsfasen illustreras med ett exempel nedan, där relevant information från stycket har markerats:

- **När kan du känna att den biometriska metodens funktion brister?**

Jag tycker att fingeravtryckskläsaren fungerade riktigt dåligt. För oss hantverkare var den värdelös faktiskt. Om man exempelvis fick ett sår eller något på fingret vilket ofta händer i arbetet gjorde det svårt att logga in med den funktionen. Det problemet har jag aldrig med FaceID, det enda som kan vara störande är när jag använder solglasögon. Då måste jag ta av solglasögonen för att kunna bekräfta att det är jag, det är väl det enda negativa med ansiktsigenkänningen vad jag kan komma på.

*Figur 1 - Illustration över kodningsfasen*

När de olika ämnena hade märkts ut och förtydligats delades de sedan upp i kategorier. Detta utfördes genom att de olika kategorierna och dess tillhörande data som hade samlats in hamnade i olika dokument för att kunna särskilja de olika kategorierna. Med detta menas alltså att de likartade intervjusvar hamnade i det specifika dokument som kategorin handlade om. Däremot fanns det även undantag och motsägelser, som även dem sorterades in i en specifik kategori.

Avslutningsvis av transkriberingsfasen skapades teman som hade genererats efter de tidigare stegen i processen. För att nämna ett tema som framkom under processen är ”autentiseringsmetoderna underlättar”.

För att vara säker på att intervjuerna har uppfattats på rätt sätt har den transkriberade versionen sedan skickats till respektive respondent, för att få ett godkännande (Rosenthal, 2016).

### 4.2.4 Tillämpning av de etiska principerna

Vid genomförande av intervjuerna tillämpades individskyddskravet för att respondenterna skall ha en förståelse av dess rättigheter, som förklaras mer ingående i kapitel 4.1.5. De tillämpades genom att vid start av intervjuerna beskriver för respondenten vad studien handlar om, enligt *informationskravet*. Dessutom förklarade forskaren för respektive respondent att hen närhelst under forskningsprocessen har rätten till att avbryta sin medverkan, och dess intervjusvar genast tas elimineras, vilket är *samtyckeskravet*. Respondenten fick även information om att hen får vara anonym som går i enlighet med *konfidentialitetskravet*, men att under denna forskning kommer alla deltagande respondenter att vara anonyma vilket innebär att deras namn aldrig kommer att presenteras avslöjas i forskningen. De redogörs istället som en pseudonym, och är endast spårbar av forskaren av den anledning att forskaren skall kunna hålla isär de olika respondenterna.
Respondenterna informerades även om att deras medverkan endast används till denna forskning och därmed inte användas till något annat ändamål, i enlighet med Vetenskapsrådets (2002) *nyttjandekravet*.

Efter att intervjuerna är genomförda och transkriberingen är slutförd skickas den transkriberade versionen till respektive respondent för att ge sitt godkännande att den

information som har framkommit är korrekt. När forskningen är klar tillhandahålls även respondenterna med det slutgiltiga resultatet.

Alla dessa etiska principer tillämpas för respekt av människovärdet.

# 5. Empiri

*I detta kapitel redovisas empirin från de genomförda intervjuerna, där uttalanden från respondenterna resonerar kring det utvalda forskningsområdet.*

Den insamlade datan från intervjuerna resulterade i olika kategorier. Dessa kategorier beskriver privatpersonernas synvinklar på privatpersoners tycke och tänkande kring de biometriska autentiseringsmetoderna, men även kring vad de kan bidra till generellt.

## 5.1 Skydd av information

Respondenterna är alla eniga om att det är viktigt att skydda den information som dess tillhörande smartphone besitter. Däremot anser de att denna viktiga information som är av stor relevans att skydda är av olika slags information. Vissa påpekar att deras bilder är mycket viktiga och vill inte att de skall komma ut till någon obehörig. Även information relaterad till privata familjekonversationer från sms, mail eller sociala medier anses viktiga att skydda.
Samtliga respondenter tycker även att det är av stor relevans att skydda är information som har med deras privata ekonomi att göra, såsom Carpay, Swish, BankID, Klarna eller den generella bank-appen där det är lätt att föra över pengar på med endast ett knapptryck. En respondent (R8) anser även att viktig information som finns i telefonen är jobbrelaterat, där respondenten besitter information om accesser till olika slags system i telefonen. Respondenten menar även på att arbetsgivaren ställer höga krav på arbetarna att de skall ha hög säkerhet på telefonen för att göra det svårt för eventuella bedragare. Två av respondenterna (R6 och R10) förklarar även att de lagrar olika slags lösenord eller PIN-koder i sina telefoner för att kunna komma ihåg dem. De menar på att de har så många olika koder och lösenord på olika saker att de behöver skriva upp dem någonstans. Detta är även en anledning till att dessa respondenter anser att det är viktigt att skydda sin telefon, för att potentiella bedragare inte skall få tillgång till dessa delar också.

Respondenterna är relativt av samma åsikter vid att telefonerna har inte köpts av dess säkerhetsfunktioner, i alla fall inte för de biometriska autentiseringsmetoder. Två respondenter (R8 och R9) har däremot köpt sina telefoner pågrund av andra funktioner som bidrar till informationssäkerheten, men inte de biometriska. För övrigt hade övriga köpt sina telefoner på grund av att de behövde en ny telefon, och köpte därför den senaste som kommit ut på marknaden.

## 5.2 Traditionell autentiseringsmetod

Fyra av tio respondenter använder fler än fyra tecken eller siffror vid den traditionella autentiseringsmetoden, vilket är ett förutbestämt antal. Anledningen till det är att privatpersonerna anser att fyra är alldeles för lätt att knäcka, men att sex siffror gör det svårare för bedragare men blir ändå inte för krångligt för användarna vid användning respektive autentisering.

Respondenterna är inte eniga om hur de känner vid autentisering i stora folkmassor, eller på allmänna platser. Fyra av respondenterna resonerar kring hur de faktiskt gör när de skall trycka in sin kod för att kunna använda mobilen, vilket innebär att de är medvetna om att attacker. Attacker som shoulder surfing påpekar Respondent 10 kan hända och att man bör vara medveten om sådana händelser. Respondent 10 uttrycker även att privatpersoner inte skall vara så naiva och tro gott om folk, av den anledning att det faktiskt finns folk som är ute efter att se din kod.
Däremot är respondenterna inte särskilt oroliga över att bedragare skall se respondenternas PIN-koder till mobilen, utan oroar sig mer över att deras koder till BankID, carpay etcetera skall synas av den anledning att det har med respondenternas ekonomi att göra.

## 5.3 Biometrins funktionalitet

Majoriteten av respondenterna har stängt av funktionen med ansiktsigenkänning, eller gör det under en viss årstid som Respondent 6. De anser inte att funktionen är tillräckligt bra och uttrycker ofta en frustration att funktionen inte bidrar till något mervärde för användning. Istället tycker majoriteten att funktionen endast krånglar, och inte är användarvänlig. Tillfällen där funktionen brister är exempelvis om man använder glasögon/solglasögon, det är mörkt i rummet eller att det blev för många moment vid upplåsning av telefonen.

Respondent 6 förklarar att *”just nu använder jag FaceID på telefonen, men under sommaren exempelvis stänger jag av funktionen. Som förra sommaren, då stängde jag av den efter att ha använt den i en vecka, för att det inte fungerade alls när jag använde solglasögon som jag använder mycket under sommaren. Så man kan säga att jag använder FaceID under vintern, så snart kommer jag att stänga av funktionen igen, tyvärr.”*

Även Respondent 9 menar att ansiktsigenkänningen inte fungerar som den bör. Respondent 9 säger *”jag slutade använda funktionen när jag förstod att den inte fungerade med mina glasögon på. Men ytterligare en bidragande faktor var att det inte fungerade när det var för mörkt”. x*

De som har tillgång till att använda fingeravtrycksläsaren använder den istället, och de respondenter som inte har tillgång till det använder bara pinkoden - eller inte alls…

Även fingeravtrycksläsaren anser respondenterna vara krånglig, samt att den inte alltid fungerar som den ska. Två av respondenterna (R1 och R10) uttrycker att fingeravtrycksläsaren inte fungerar optimalt för hantverkare, där de använder händer mycket i arbetet där de slits mycket. De anser att fingeravtrycken fungerar *”riktigt dåligt”* för att vara ordagrann, av den anledning att de ofta får sår eller skär sig i arbetet och dess fingeravtryck blir ogiltigt vid verifiering. Däremot har de inte använt funktionen som till fullo, där möjligheten att ha flera fingrar som möjliga att verifiera sig med. De ansåg att funktionen inte fungerade tillräckligt bra för att de skulle lägga ned tiden på att lägga in alla sina fingrar för identifiering, trots att det inte tar lång tid.

Minoriteten tycker istället att funktionen fungerar ypperligt och ser inga problem alls med funktionen.

Respondenter är eniga om att de biometriska autentiseringsmetoderna underlättar av den anledning att användaren inte behöver komma ihåg eller ha med sig något för att bevisa att jag har behörighet. De påpekar även att funktionen i sig är smidig, men att den bör utvecklas mer för att funktionen skall vara felfri samt kännas säker för att användas.

Vid frågan om privatpersoner känner sig mest säkra vid användning av fingeravtryckskläsaren eller ansiktsigenkänningen är det spridda åsikter, ungefär 50/50 om vad de anser. Men anledningen är alltid den samma som respondenterna anger, de är inte lika lätt att förfalska den valda autentiseringsmetoden jämfört med den andra. Respondenterna är även införstådda med att det redan finns tillvägagångssätt att manipulera de biometriska autentiseringsmetoderna, men är inte oroliga över att de skall hända just dem. Återigen kommer uttryckssätt såsom *”varför just mig?”*.

Två av respondenterna (R8 & R10) yttrar sig även om att biometrins fördelar vid den säkra autentiseringen som den bidrar till, försvinner lite i och med att PIN-koden alltid finns med ändå. De anser att PIN-koden drar ned säkerheten, av den anledning att det är lätt för bedragare att komma på koden, vilket leder till att de får tillgång till mobilen trots att de använder sig av de biometriska metoderna. Däremot är de även reflekterande över om den biometriska funktionen skulle sluta fungera, då är det bra att den traditionella funktionen fortfarande finns kvar så att de ändå kan komma in i sin mobil. De yttrar en tveksamhet huruvida bra det är att både de biometriska och de traditionella metoderna finns som alternativ vid autentisering.

## 5.4 Integritet och identitet vid biometrisk autentisering

Samtliga respondenter har uttryckt att de börjar att känna sig allt mer bevakade och tror att teknikens framgång bidrar till allt mer övervakning av privatpersoner. Även om meningen kanske inte är att övervaka, så kommer ändå möjligheten att finnas för detta och ett slags maktmissbruk eller liknande tror respondenterna att biometri och dess tillhörande metoder kommer att leda till. Genom att dessa biometriska autentiseringsmetoder utvecklas allt mer tror majoriteten av respondenterna även att dessa framsteg är en nackdel för privatpersoner i stort. Respondenterna uttrycker en synvinkel som är bekymrad, av den anledning att merparten av respondenterna tror att de biometriska egenskaperna som används för att identifiera sig vid tillgång till sin smartphone finns lagrade någonstans där de inte kan ha kontroll. Respondent 2 beskriver de biometriska autentiseringsmetoderna som *”för att kunna identifiera mig så måste min identitet finnas lagrad någonstans i min telefon, och det finns förmodligen någon som har tillgång till det som lagras, vilket medför att om denna lagring hamnar i fel händer kan bidra till förödande konsekvenser. Exempelvis ID-kapningar eller liknande, eftersom det trots allt är min identitet som lagras”.*

Även Respondent 8 beskriver den biometriska metoden bryter mot privatpersoners integritet samt identitet. Respondent 8 förklarar att *”Biometriska metoder innebär att mycket känslig data lagras, eftersom det är min identitet. Detta kan i sin tur leda till identitetskapningar som kan missbrukas om det hamnar i fel händer”*

Minoriteten av respondenterna anser inte att de biometriska metoderna bryter mot deras integritet eller identitet. Respondent 6 bedömer beskriver detta såsom *”när jag börjar tänka i dem banorna så blir man självklart lite bekymrad, med tanke på att de förmodligen lagras någonstans. Det mesta lagras ju nu förtiden. Men jag tänker mer på vad ska dem ha mina biometriska egenskaper till, eller varför ska någon ens kolla innehållet i min mobil? Varför just mig?”*

Med andra ord är minoriteten av de intervjuade privatpersonerna inte alls oroliga över var deras biometriska egenskaper hamnar vid användande av dessa autentiseringsmetoder. Tre av tio respondenter resonerar på detta viset, och finner ingen anledning att oroa sig kring sådant.

Respondent 8 uttrycker även att ansiktsigenkänningen medför att kameran på displayen förmodligen alltid är på för att kunna vara aktiv vid när en autentisering skall ske. Detta bidrar även det till övervakning, *”vem som helst kan kolla på mig just nu?”* uttrycks.

# 6. Analys

*I detta kapitel jämförs bakgrunden som består av teori med den insamlade datan från intervjuerna. Här kan de både insamlingsmetoderna styrka varandra, men även försvaga varandra, vilket bidrar till en större uppfattning kring dess relevans.*

## 6.1 Privatpersoner om informationssäkerhet

Information som är av stor relevans och är viktigt för privatpersoner skall behandlas med varsamhet, av den anledning att det är information som är värdefull för privatpersoner (MSB, 2015). Detta håller även de intervjuade privatpersonerna med om, och menar att den information som de anser vara värdefulla för just dem är den information som finns i deras mobiltelefoner. Värdefull information för privatpersonerna är  bilder, familjekonversationer, mail eller dess sociala medier. Information som privatpersonerna anser vara värdefull att behandla varsamt och som de inte vill skall hamna i fel händer är deras privata ekonomi som finns i telefonen och som ska skyddas från obehöriga vilket ligger i linje med begreppet konfidentialitet och riktighet av Åhlfeldet et al. (2007). Dessa olika applikationer som respondenterna använder som nämns som har med den privata ekonomin är BankID, Swish och Klarna för att nämna några som berör den delen av information som de anses vara känslig för obehöriga. Samtliga respondenter är eniga om att den privata ekonomin är en slags information som är extra känslig om den hamnar i fel händer, och tycker därför att det är av stor relevans att skydda sin smartphone på grund av detta. Respondent 5 uttrycker sig om ekonomin i sin smartphone; *”Det värdefullaste som jag anser att jag har i min telefon är alla appar som har med min ekonomi att göra. Exempelvis Swedbank-appen, där kan lätt föra över pengar med endast ett knapptryck i dagsläget”.* Denna synvinkel, den digitala ekonomin som används i dagens samhälle, är även något som Pocovnicu (2009) berättar. Han berättar även att dagens smartphone och dess tillhörande funktioner i egenskap av användning av digital bank är en bidragande faktor till att smartphones är attraktiva för tjuvar i dagens läge. Detta förklarar även Buriro et al. (2016), att i dagens samhälle används mobiltelefonerna till att utföra transaktioner som exempelvis mobila betalningar eller fjärråtkomster till intranät till den anställdes företags system.

Även funktioner som fjärrarbete är något som även är attraktivt för tjuvar (Pocovnicu, 2009) , vilket Respondent 8 förklarar att hen har i sin smartphone, för att kunna ha åtkomst när som helst oavsett plats. Att ha åtkomst vid behov överensstämmer med definitionen av informationssäkerhet, tillgänglighet (MSB, 2015; Åhlfeldt et al. 2007; Andronache & Althonayan, 2018; von Solms & van Niekerk, 2013).  Respondent 8 menar på att hen besitter information som är av stor relevans inom jobbet, och får inte läckas ut. Information som sådan kan exempelvis vara åtkomst till systemen de använder inom jobbet som även är information som är känslig för obehöriga och kan skapa oerhörda konsekvenser för både Respondent 8 samt det specifika företaget, vilket även SIS (2015) skriver. Däremot är arbetsgivaren mycket noggrann med att de anställda använder sig av säkerhet till mobiltelefonen

Vid frågan om respondenterna använder sina mobiler i osäkra miljöer, som Burgbacher et al. (2014) beskriver som miljöer där mobiltelefonerna är mer mottagliga för åtkomst av obehöriga samt ökad risk för attacker, svarar alla respondenter att de gör det. Samtliga respondenter använder sina enheter på allmänna platser, och de flesta av respondenterna kopplar även upp sig på gratis wi-fi om det finns. Respondent 9 påpekar att *"jag kopplar upp mig för att spara på min surf, och tycker det är bra när det finns tillgängligt så att man kan koppla upp sig gratis"*. Dock menar Respondent 3 att hen tänker ofta på om det egentligen är så bra att koppla upp sig, men ibland trots sitt konsekvenstänkande gör det ändå av den anledning att surfen är på väg att ta slut eller att täckningen är dålig. Däremot är respondenterna oeniga om de alltid kopplar upp sig på det wifi som erbjuds eller inte, men alla förutom en respondent (R3) har tankesättet att det finns ökad risk för attacker vid uppkoppling av wifi eller om mobilens funktion som söker efter att koppla upp sig på wifi är på under vistelser utanför huset. Ibland menar Respondent 3 på att hen stänger av den funktionen vid tillfällen som respondenten lämnar sin bostad. Ingen av respondenterna har blivit utsatta av någon slags attack på sin mobil, men flertalet av respondenterna vet närstående som har blivit utsatta av olika slags attacker.

## 6.2 Den traditionella autentiseringsmetoden

Burgbacher et al. (2014) förklarar att autentiseringmetoden av den traditionella typen är sårbara, av den anledning att det är lätt för utomstående att observera. Detta påpekar även flertalet av respondenterna i de utförda intervjuerna, vilket även de ser som en nackdel med just den metoden. Respondent 10 menar på att det inte finns många fördelar med de traditionella autentiseringsmetoderna alls, men att det finns många nackdelar istället. Respondent 10 menar även på att det finns flera olika sätt att kunna hacka lösenord eller PIN-koder genom att använda program som är lätta att använda för de som kan och som vill komma åt andras lösenord av någon anledning. Respondent 8 menar istället att lösenord och PIN-koder kan vara förutsägbara, som även det anses som en nackdel. Respondent 8 påpekar även att många gör det lätt för sig och använder samma kod eller lösenord på flertalet ställen, såsom att ha samma fyrsiffriga kod som verifiering till sin smartphone och samma kod till sitt bankkort. Detta beskriver även Burgbacher et al. (2014) som en nackdel med denna autentiseringsmetod, att användare använder sig av svaga kombinationer, eller till och med skriver ned sina lösenord respektive PIN-koder till system på något ställe. Dessa problem påpekar Burgbacher et al. (2014) vara oundvikliga.

Detta problem är även något som tas upp under intervjuerna. Ett par av respondenterna förklarar att de lagrar sina lösenord eller PIN-koder i sina mobiler, vilket medför att de anser att det är viktigt att skydda den information som de har i sina smartphones. Respondent 7 berättar även att den PIN-kod som Respondent 7 använder för att identifiera sig vid autentisering består enbart av fyra siffror, och att samma fyrsiffriga kod har Respondent 7 använt sedan den första mobilen köptes. Respondent 7 uttrycker

sig: *" Jag använder mig av en fyrsiffrig kod, eftersom jag vill ha en lätt kod samt att det ska gå fort och smidigt att komma in i telefonen. Jag har använt samma kod sedan den dagen jag köpte min första telefon, men då var koden istället PUK-kod, och den har hängt med sedan dess".*

Enligt Burgbacher et al. (2014) lämnar privatpersoner sina telefoner oskyddade, av den anledningen att de anser att funktionen är obekväm och tycker då istället att det är lättare att lämna telefonen helt oskyddad. Detta instämmer Respondent 2 med, som lämnar sin telefon helt oskyddad. Respondent 2 tycker att mobilen är alldeles för stor för händerna, eftersom Respondent 2 oftast använder en hand vid användning. Respondent 2 tycker att i det stora hela är all slags autentisering krånglig, och det är en anledning till att mobilen lämnas helt oskyddad. Respondenten anser att det inte känns säkert, men att det är viktigare att det ska gå snabbt och smidigt att använda, och *"vill inte lägga till krångliga funktioner"*.

Fördelar med den traditionella autentiseringsmetoder är inte många som respondenterna uppger, men den mest framkommande fördelen är alla vet vad det faktiskt är, samt att det är lätt att lära sig om man inte vet vad det är. Majoriteten av respondenterna uppger att de använder samma PIN-koder eller lösenord till olika saker, samt att det blir lätt att komma ihåg om användaren använder samma. Däremot är de medvetna om att det inte är ett säkert sätt, att använda samma kombinationer till många olika inloggningar, men uttrycker sig för jämnan att det skall gå snabbt och smidigt. Detta innebär att användarna använder kombinationer som de anser vara lätta att komma ihåg, vilket går i enighet med vad Bhanushali et al. (2015) förklarar. Bhanushali et al. (2015) förklarar även att detta är en teknik som är praktisk för användaren, men är istället känslig för attacker av olika slag.

Två av respondenterna (R8 och R10) menar på att den traditionella autentiseringsmetoden drar ned nyttan vid användning av den biometriska autentiseringen. De förklarar båda att fördelen med den biometriska funktionen är att det inte skall gå att hackas, och att det skall vara så personligt som möjligt, vilket försämras när den traditionella metoden fortfarande finns kvar. De påpekar att oavsett om de använder den biometriska funktionen, så kan bedragare ändå använda sig av olika program som Bhanushali et al. (2015) beskriver, som finns av den anledning att PIN-koden finns kvar som en säkerhetsfunktion till den biometriska, vid bristande funktionsduglighet. De anser att det är lite motsägelsefullt, och att PIN-koden drar ned på säkerheten. De uttrycker även en tveksamhet kring att de båda autentiseringsmetoderna finns som alternativ.

## 6.3 De biometriska funktionerna

Ingen av respondenterna visste vad biometri var, men vid en liten ledtråd förstod de flesta vad det var. Autentiseringsmetoder inom biometri som uppgavs var ansiktsigenkänning, fingeravtrycksavläsare samt röstigenkänning vid följdfrågor. Vid

vidare frågor vad de ansåg vara för fördelar med denna autentisering var mestadels att användare inte behövde komma ihåg något eller ha med sig något, i enlighet med vad Fuandez-Zanuy (2006) förklarar. Att biometri är något som analyserar de mänskliga egenskaper som användaren besitter var det spridda åsikter kring, huruvida bra eller dåligt det var. Som tidigare nämnt påpekade samtliga tio respondenter att det är smidigt i det avseendet att användaren inte behöver med sig något eller kunnat något, utan att autentisering sker med något som användaren är. Däremot ansåg ungefär hälften av respondenterna att funktionerna som finns på mobilerna idag är bristfälliga, och bör utvecklas mer för att den smidighet som krävs för att använda det skall vara gynnsam för användaren.

### 6.3.1 Autentisering med ansiktsigenkänning

Vid frågan om de använder den eller de biometriska funktioner som respektives mobiltelefon besitter var det olika svar på. Majoriteten av respondenterna har stängt av funktionen ansiktsigenkänning, men använder istället fingeravtryckslösaren. Ansiktsigenkänningens funktion ansåg de respondenter som hade stängt av funktionen som dålig, av den anledning att den inte fungerade som den ska i alla situationer. Situationer som nämndes var vid användning av glasögon, solglasögon, när det var för mörkt eller att funktionen helt enkelt inte kunde läsa in ansiktet oavsett. *"Jag använder inte ansiktsigenkänningen eftersom den inte fungerade alls för mig. Den krånglade bara och blev helt enkelt bara i vägen för mig vid användning. Därför har jag stängt av den, och jag är inte intresserad av att sätta på funktionen igen"* uttrycker sig Respondent 7. Respondent 9 uttrycker sig liknande, men anledningen till varför respondenten stängde av funktionen var istället att den inte fungerade på grund av glasögon eller att det var mörkt; *"jag slutade använda funktionen när jag förstod att den inte fungerade med mina glasögon på. Men ytterligare en bidragande faktor var att det inte fungerade när det var för mörkt".*

Vad dessa respondenter beskriver om ansiktsigenkänningen överensstämmer med vad Harakannanavar et al. (2019) beskriver som denna biometriska metods utmaningar. Dessa utmaningar såsom problem med belysning, användare som använder sig av hatt, glasögon eller solglasögon, eller helt enkelt olika ansiktsuttryck samt ansiktets rotation är sådana utmaningar som Harakannanavar et al. (2019) nämner angående ansiktsigenkänningsfunktionen. De Luca och Lindqvist (2015) nämner även osäkerheten som finns i ansiktsigenkänningen, där det är möjligt att lura den biometriska funktionen genom att en digital bild visas upp och autentiseringen godkänns. Även detta är något som en respondent nämner. *"Jag har hört att det går att lura ansiktsigenkänningen genom att visa upp ett foto och mobilen öppnar sig, vilket jag tycker är oroväckande. Sen vet jag inte hur mycket jag tror på det, men det är helt klart skrämmande om det är så lätt"* menar Respondent 4 på.

Men alla instämmer inte att ansiktsigenkänningen fungerar dåligt. Respondent 10 menar istället på att den funktionen är den bästa metoden att använda vid autentisering och kan inte tänka sig att gå tillbaka och använda fingeravtryckslösaren igen. Även

Respondent 6 tycker att funktionen fungerar bra, men att den används under vissa perioder för användaren. *”Just nu använder jag FaceID på telefonen, men under sommaren exempelvis stänger jag av funktionen. Som förra sommaren, då stängde jag av den efter att ha använt den i en vecka, för att det inte fungerade alls när jag använde solglasögon som jag använder mycket under sommaren. Så man kan säga att jag använder FaceID under vintern, så snart kommer jag att stänga av funktionen igen, tyvärr.”*

Problematiken med att funktionen inte fungerar vid olika situationer som både respondenter samt Harakannanavar et al. (2019) beskriver stämmer överens, och vad det verkar som är detta ett relativt stort problem för användare av funktionen, om inte även frustrerande. Metoden har utmaningar som behöver åtgärdas för att systemet skall vara tillförlitligt och smidigt för användaren (Harakannanavar et al., 2019). Även Pocovniu (2009) menar på att ingen biometrisk funktion är helt perfekt.

Vid användning av ansiktsigenkänningen och dess funktion för hur användaren får åtkomst till mobilen har Respondent 5 ett betraktelsesätt om hur funktionen i sig fungerar. Respondent 5 uttrycker att ansiktsigenkänningen fungerar bra, men att nästa steg för att få åtkomst är desto sämre. *”Jag har sett mina kollegors telefoner, exempelvis telefonen OnePlus. Där behöver de inte swipa upp som man behöver göra på iPhone, vilket jag ser som en bättre och smidigare lösning för användaren. Den bara känner igen ansiktet och öppnar så att man kommer till startsidan med en gång. Så vill jag också att min ska göra”.* Med andra ord krävs ingen uppsvepning vid autentisering, och detta anser Respondent 5 vara mycket smidigare.

### 6.3.2 Autentisering med fingeravtryckssläsare

*”Jag tycker att fingeravtrycket fungerar helt perfekt i dagsläget, det går smidigt och går väldigt fort att ta sig in i telefonen med att endast visa mitt fingeravtryck på baksidan av telefonen. På min tidigare anställning arbetade jag i verkstaden, vilket gjorde att jag ofta skar i mig eller fick sår på fingrar och händer. Då fungerade inte fingeravtrycksavläsaren alls, och det var fruktansvärt irriterande. Men nu när jag jobbar på kontor har jag inte alls det problemet, men det var absolut ett stort problem förut som skapade både frustration och irritation”.*

På detta vis uttrycker sig Respondent 1 om fingeravtryckssläsaren, som finner funktionen som egentligen både bra och dåligt men beror på hur man arbetar. Detta stämmer överens med vad De Luca och Lindqvist (2016) även beskriver, att det är en metod som är enkel att använda samt att funktionen underlättar upplåsning av telefonen för användaren. Men däremot tillägger även Harakannanavar et al. (2019) att funktionen inte är fullt funktionerlig vid fingrar som är våta och skrynkliga. Det Respondent 1 menar är att funktionen inte fungerar vid fingrar som har sår på fingrarna, vilket även det bör tilläggas i utmaningar kring fingeravtryckssläsaren och dess förbättringar.

Även Respondent 10 som arbetar som snickare har liknande problem, och uttrycker sig: *”Jag tycker att fingeravtrycksavläsaren fungerade riktigt dåligt. För oss hantverkare var*

*den riktigt värdelös faktiskt. Om man exempelvis fick ett sår eller något på fingret vilket ofta händer i arbetet gjorde det svårt att logga in med funktionen. Jag vet många som jag arbetar med som har samma problem".* Men det är även viktigt att tillägga att de inte har använt funktionen helt fullt ut, där det finns möjlighet till att lägga till flera fingrar för att funktionen skall vara så bra som möjlig. Men vid denna följdfråga var svaret att de inte tyckte att funktionen fungerade tillräckligt bra för att lägga ned tiden på det. Respondent 1 som idag tycker att funktionen fungerar utmärkt vid en annan anställning, kan i dagsläget tänka sig att lägga in de flesta fingrar till autentisering, för att slippa en sådan situation igen om en liknande situation skulle ske.
Dessa respondenter upplevs som frustrerade vid frågor om fingeravtryckskläsaren, men detta är även något som Mayron et al. (2013) har fångat upp sedan tidigare. Att användarna av fingeravtryckskläsare upplevs som frustrerade, men frustrationen kan även komma från att fingret placeras fel på sensorn. Även temperaturen kan vara en bidragande faktor till att funktionen inte fungerar helt korrekt.

De respondenter som har tillgång till både ansiktsigenkänning och fingeravtryckskläsare användare endast fingeravtryckskläsaren, på grund av ansiktsigenkänningens problem. Respondent 9 som inte alls var positiv till ansiktsigenkänningen är desto mer positivt till fingeravtryckskläsaren istället. Respondent 9 uttalar sig som följande: *"Jag tycker den är riktigt bra. Jag har både haft iPhone och samsung och på båda har det fungerat riktigt bra. Däremot så är samsung mycket smidigare, eftersom funktionen finns på baksidan vilket känns mer naturligt".* Även Respondent 5 tycker att fingeravtrycksavläsaren fungerar bäst, nu i efterhand. I dagsläget har respondenten en iPhone X och har därför inte tillgång till fingeravtryckskläsaren. *"Så här i efterhand tycker jag att fingeravtryckskläsaren har fungerat bäst, nu när jag använder mig av ansiktsigenkänningen. För då har jag ju ändå fingret på knappen och fingret kommer ju ändå att vara där i närheten när jag använder mobilen sedan. Med ansiktet blir det istället att man sätter upp telefonen i en lite högre position än vad man egentligen brukar har den i för att den ska kunna läsa av ansiktet".* Det som Respondent 5 uttrycker sig om ansiktsigenkänningen stämmer inte överens med vad Faundez-Zanuy (2006) förklarar med ansiktsigenkänningen, att det är det mest naturliga sättet att en autentisering utförs på för användarna. Däremot håller det med vad De Luca och Lindqvist (2016) berättar med fingeravtryckskläsare, att det är en metod som ska underlätta för användaren vid upplåsning. Att de olika tillverkarna har sin egna specifika placeringar på mobiltelefonerna går att diskutera vad som är det smidigaste egentligen för användaren. Respondenterna 9 och 5 går i enlighet med vad De Luca och Lindqvist (2006) anser om metoden - det är en metod som är enkel att använda.

### 6.3.3 Den säkraste autentiseringsmetoden

Det är spridda åsikter kring vilken av de olika autentiseringsmetoderna inom biometri som respondenterna anser som säkrast. Endast en av respondenterna, Respondent 7, tycker att röstigenkänningen bör vara den säkraste metoden. Respondent 7 menar att med röstigenkänningen bör vara svår att härma av den anledning att olika människor

använder sig av olika stämmor eller betoningar på olika ställen vid uttal av ord, som går i enlighet med vad Choudhury et al. (2018) även förklarar om hur autentiseringsmetoden fungerar. Dock tror Respondent 7 att denna metod kan vara krånglig samt inte så användarvänlig, om man vistas på allmänna platser eller konserter eller liknande. Respondent 7 tror att vid sådana tillfällen är det endast krångligt och en autentisering kommer inte att kunna utföras, pågrund av att mikrofonen som skall ta upp ljudet inte kommer att kunna urskilja det med allt ljud omkring. Detta är även något som Choudhury et al. (2018) påpekar som en sårbarhet kring autentiseringsmetoden, att just bakgrundsljudet påverkar metodens funktionalitet.

Samma gäller ansiktsigenkänningen, vilket även här endast var en av respondenterna som ansåg att denna metod var den säkraste av de biometriska metoderna. Respondent 10 bedömer ansiktsigenkänningen som den säkraste av den anledning att den är svårast att förfalska ett helt ansikte, att det är många olika personlighetsdrag som skall stämma för att kunna förfalska såpass att det faktiskt fungerar. Däremot har respondenten inte tänkt i de banor som exempelvis Respondent 4 har gjort, att det finns möjligheter till att manipulera metodens funktion genom att använda en digital bild, som även De Luca och Lindqvist (2015) beskriver.

Den autentiseringsmetod som respondenterna anser vara den säkraste, varav hälften av respondenterna valde denna metod som säkrast är iris-igenkänningen. Denna metod besitter en säkerhet som är ännu högre än fingeravtryckssläsarens säkerhet, men är istället en metod som är för dyr jämför med de låga kostnadsenheterna (Faundez-Zanuy, 2006). Vid frågan av varför respondenterna anser att just denna metod är säkrast, svarar en respondent (R3) att respondenten inte riktigt vet specifikt varför, men menar att den känns säkrare än övriga metoder och att ögon bör vara det personlighetsdrag som är mest unikt. Respondent 3 tillägger även att detta är inget som respondenten har någon kunskap kring att det faktiskt är på detta vis, men att respondenten har en slags uppfattning att det bör vara så. Även Respondent 1 tänker i samma banor, men tillägger även *”jag tror att irisigenkänning är den säkraste metoden. Ett finger går att hugga av eller fuska sig fram. Jag vet dock inte hur realistiskt det är att hugga av ett finger, men det är sådant som jag har sett i både filmer och serier men det tror man ju inte alltid på men till viss mån. Därför tror jag att irisigenkänningen är en säkrare metod, eftersom den förmodligen är mer unik och även svårare att få tag på om man ska uttrycka sig så”.*

Ett betraktelsesätt som ingen av respondenterna som ansåg att irisigenkänningen var den säkraste metoden för autentiseringen, tänkte i de banor att det blir svårare vid användning av glasögon, linser eller vattniga ögon (Harakannanavar et al, 2019). Forskningen kring denna metod behöver fortsätta, samt korrigeras för att garantera användning mot de ovannämnda faktorerna.

De resterande tre respondenter tycker att fingeravtryckssläsaren är den säkraste metoden. Anledningen att de anser att den är säkrast är att det är svårt att förfalska även här. *”Jag tror att det är svårt att få till ett fingeravtryck som är identiskt”* uttrycker sig Respondent 4. Sannolikheten att det finns två människor som har identiska

fingeravtryck är en på miljarden (Faundez-Zanuy, 2006). Detta är även ett påstående som det har utförts beräkningar på. Respondent 4 fortsätter att förklara *”jag känner mig inte stressad över att attacker mot fingeravtryck finns, eftersom det vet jag redan att det gör. Men så är det med allt tänker jag, det kommer alltid att finnas bedragare. Men varför ska dem ha min tänker jag?”.*

Respondent 2 som även hen anser att fingeravtrycksläsaren är den säkraste metoden, men menar istället på att *”Vad jag tror så är man inte helt själv med att ha just det specifika fingeravtrycket som man har, utan att det finns någon annan i världen som har samma. Men då gäller det ju även att man ska hitta den personen som har det identiska fingeravtrycket, och det gör ju att fingeravtrycket inte är 100% säkert.* Även här görs liknelsen mellan respondent och Faundez-Zanuy (2006) som är införstådda med att det finns individer i världen som har samma fingeravtryck, men att sannolikheten att hitta den andra personen med samma fingeravtryck är minimal.

Oavsett vilken slags autentiseringsmetod som respondenterna anser vara den säkraste metoden, används argumentet att det är svårt att manipulera och förfalska den utvalda metodens biometriska egenskaper.

## 6.4 Privatpersoner oroliga över lagring av de biometriska egenskaperna

Samtliga respondenterna uttrycker en oro kring de biometriska autentiseringsmetoderna huruvida det kommer till lagringen av de egenskaper som lagras vid användning av dessa autentiseringsmetoder. Merparten av respondenterna förmodar att egenskaperna lagras någonstans, och det är något som de inte kan ha kontroll över. Respondent 2 uttrycker sig *”för att kunna identifiera mig så måste min identitet finnas lagrad någonstans i min telefon, och det finns förmodligen någon som har tillgång till det som lagras, vilket medför att om denna lagring hamnar i fel händer kan bidra till förödande konsekvenser. Exempelvis ID-kapningar eller liknande, eftersom det trots allt är min identitet som lagras”.*
Detta är även något som Prabhakar et al. (2003) intygar. De menar på att datan kan komma att användas till annat som det inte är ämnad till att användas till, vilket i sig är en risk som användaren tar vid sådana metoder. De menar även på att detta kan leda till diskrimination av olika slag. Precis som Respondent 2 förklarar i det tidigare citatet så innebär det att de egenskaper som används vid dessa metoder är inom en stor fara om någon obehörig får tag på detta, och om egenskaperna en gång har blivit utsatta för fara kommer de alltid att vara det (Prabhakar et al., 2003). Egenskaperna som används vid autentisering med de biometriska metoderna är begränsade, av den anledning att vi individer endast har tio fingrar, eller ett biometriskt ansikte. Den stora nackdelen med det är att det inte är lika lätt att ersätta, som det är med lösenord etcetera. Även Nguyen och Dan (2019) håller med om detta, och förklarar att om en bedragare får tag på ett fingeravtryck finns det möjligheter för bedragaren att få tillgång till personliga saker, såsom journaler eller brottsregister för den specifika personen som har blivit kapad på sitt fingeravtryck. Det som Respondent 2 yttrar sig om är även Respondent 8

reflekterande över och yttrar sig som följande: *”Biometriska metoder innebär att mycket känslig data lagras, eftersom det är min identitet. Detta kan i sin tur leda till identitetskapningar som kan missbrukas om det hamnar i fel händer”.*

Däremot finns det respondenter som inte resonerar på samma sätt. Tre av tio respondenter är inte orolig över att deras biometriska egenskaper lagras, eller att de skall hamna i fel händer. Dessa tre respondenter menar att de inte har någon anledning till att oroa sig över att det lagras, men en av respondenterna får en insikt vad det gäller lagringen vid intervjufrågorna. Respondent 6 är inte orolig, men uttrycker *”när jag börjar tänka i dem banorna så blir man självklart lite bekymrad, med tanke på att de förmodligen lagras någonstans. Det mesta lagras ju nu förtiden. Men jag tänker mer på vad ska dem ha mina biometriska egenskaper till, eller varför ska någon ens kolla innehållet i min mobil? Varför just mig?”.*

Känslan som uppkommer vid intervjuerna är att de respondenter som är av minoritet vid ämnet om lagringen kring de biometriska egenskaperna är att de förlitar sig på att säkerheten är hög. Nguyen och Dang (2019) påpekar att den säkerhet som finns kring denna lagring bör vara stark samt att säkerheten bör diskuteras och bli ännu starkare. Det räcker att en användare utför en autentisering med ett nätverk som inte är säkert, kan en bedragare närma sig informationen som består av de biometriska egenskaperna. Likheten är slående mellan detta och vad Matyas och Riha (2003) menar när de påpekar att det inte är lika lätt att använda sig av de biometriska egenskaperna som det är med lösenord eller passerkort, som är lätt att skicka till en annan användare så att den individen också får åtkomst. Dessa respondenter som förlitar sig på de biometriska autentiseringsmetoderna tänker förmodligen i de banor att säkerheten är stark samt att en biometrisk egenskap inte är lika lätt att använda för en bedragare.

En intressant synvinkel som Respondent 8 uttalar sig om är en väckarklocka. Respondent 8 förklarar att displayen som används vid autentisering förmodligen (enligt hens teorier)behöver vara påslagen av något slag för att kunna vara beredd när en autentisering önskas av användaren. Respondent 8 uttrycker sig att *”vem som helst kan kolla på mig just nu?”.* Detta uttryck går i enlighet med vad Prabhakar et al. (2003) även skriver om, att identifiering av användare kan ske vid vilken tidpunkt som helst, utan att användaren har någon slags kännedom om det.

### 6.4.1 Biometri bryter mot användarens identitet samt integritet

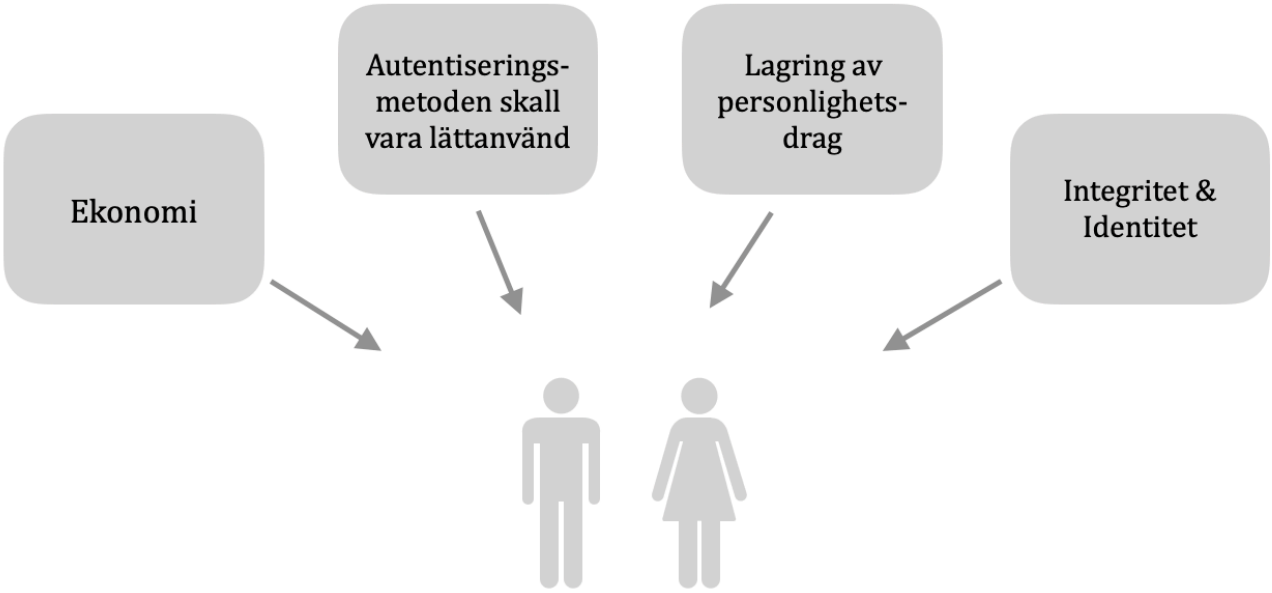
Precis som respondenterna uttrycker sig om lagringen kring deras biometriska egenskaper, går detta hand i hand med synpunkter kring användarens identitet eller integritet. Där Respondent 8 uttrycker sig om att *”vem som helst kan kolla på mig just nu?”* handlar inte endast om lagringen, utan att det blir ett överträdelse kring hur dessa biometriska egenskaper egentligen får användas samt vad de faktiskt används till. Biometriska metoder och de system som de används med kan vara i riskzonen för att bryta mot användarens integritet (Matyas & Riha, 2003). Även en förlust innebär de biometriska systemen, som menar att dessa system reducerar anonymiteten som

användare. Sju av tio respondenter uttrycker att de börjar känna sig oroliga över att de känner sig allt mer övervakade, av den anledning att teknikens framgång går så pass fort fram och att detta medför att det blir allt mer övervakning. Respondent 5 påpekar att *"Jag tror inte att meningen är att det ska övervakas, men man får känslan av det efter allt man har hört i media. Jag är själv lite reserverad kring när jag har min mobil, vid vilka tillfällen, och det finns alltid människor som vill göra onda och dumma saker som påverkar andra".* Även Respondent 3 förklarar att *"jag tänker på när jag använder min mobil. Jag tar tillexempel inte med mig min mobil in på toaletten. Man vet ju aldrig om kameran är påslagen. På något sätt känner jag mig alltid övervakad av min mobil, det tycker jag är läskigt".* Enligt Matyas och Riha (2003) kan biometriska system anses vara personligt invasiva eller påträngande enligt användare, och detta stämmer överens med vad både Respondent 3 och Respondent 5 anser om deras mobiltelefoner och vad de biometriska autentiseringsmetoderna kan leda till. Dessa system har har problematik som behöver lösas för att systemen skall kunna användas på ett pålitligt och säkert sätt (Matyas & Riha, 2003), vilket stämmer överens med vad respondenterna yttrar om dessa synvinklar.

# 7. Resultat

*I detta kapitel presenteras studiens resultat, som har fångats in från litteraturstudie och intervjuer, som sedan har sammanställts och analyserats med och mot varandra.*

Den sammanställda resultatet av denna studie sammanfattas i en modell (se figur 2), för att ge en snabb överblick av de påverkande faktorerna. Figuren presenterar de olika faktorer som påverkar en privatpersons val av de olika autentiseringsmetoderna. De olika faktorerna beskrivs mer noggrant under figuren var för sig, för att få en tydligare bild av varför dessa faktorer påverkar privatpersoners val. Dessa olika faktorer har framkommit under såväl litteraturstudien samt intervjuerna som har genomförts i denna studie.




*Figur 2. Sammanställning av de påverkande faktorerna vid val av autentiseringsmetod*

## *7.1 Ekonomin en stor faktor till informationssäkerhet*

Buriro et al. (2016) förklarar att i dagens samhälle är en av mobiltelefonernas göromål att kunna underlätta att utföra transaktioner, såsom mobila betalningar. Även åtkomst till individens företagssystem är en del av vad mobiltelefonerna skall kunna stötta användaren med, vilket går i enlighet med var respondenterna säger. Respondenternas största anledning till att skydda sin mobil idag är på grund av att de har en stor del av sin ekonomi i sin smartphone, och att det kan ske oerhörda konsekvenser om en bedragare får tag på mobilen och den inte är skyddad. Ekonomin är en faktor som är viktigt för privatpersoner att skydda, vilket bidrar till att privatpersoner att välja en autentiseringsmetod som ger ett högt skydd av informationen som dess smartphones

besitter. Respondenterna är eniga om att ekonomin är viktigt att skydda, men de tillägger även annan information såsom mail, sociala medier, bilder etcetera. MSB (2015) menar att information som har en stor betydelse och är viktig för individen ska behandlas varligt, av den anledning att det är information som är viktigt för personen i fråga. Däremot är respondenterna inte lika aktsamma vid användning av mobilen i osäkra miljöer. Respondenterna berättar att de kopplar upp sig på wi-fi som är gratis, eller använder sina enheter på allmänna platser. Enligt Prätorius och Hinrichs (2014) beskriver att sådan användning av sina smartphones kan öka risken för attacker. Endast en av tio respondenter är medveten om den ökade risken och stänger av funktionen som letar efter nätverk att koppla upp sig på, för att undvika den ökade risken för attack.

## *7.2 Autentiseringsmetoden ska vara enkel*

Den övervägande delen av respondenterna har stängt av ansiktsigenkänningen och använder istället fingeravtryckläsaren. Anledning till att respondenterna har stängt av funktionen är på grund av att funktionen inte fungerar vid användning av glasögon, solglasögon, för mörkt eller att igenkänningen inte funkade kort sagt. Detta passar ihop med Harakannanavar et al (2019) förklarar som de biometriska autentiseringsmetodernas utmaningar. De menar även att ansiktsigenkänningen har problem som behöver lösas för att det ska vara smidigt och tillförlitligt för användaren. Däremot finns det två respondenter som anser att ansiktsigenkänningen är det bästa som har hänt, och kan inte tänka sig att gå tillbaka till någon annan autentiseringsmetod.

Fingeravtryckläsaren tycker respondenterna fungerar beroende på anställning. En anställning där respondenterna arbetar mycket med händerna är inte fingeravtryckläsaren den optimalaste lösningen. Enligt Respondent 1 och 10 som arbetar som hantverkare fungerar funktionen *”riktigt dåligt”* Respondent 10 uttrycker sig. Funktionen är bristfällig vid fingrar som är våta och skrynkliga enligt Harakannanavar et al. (2019). I dessa utmaningar som nämns bör även fingrar som har sår eller läggas till som en förbättringspunkt.
Några av respondenterna tycker istället att fingeravtryckläsaren fungerar mycket bra, och tycker att funktionen är smidig. Även en respondent som i dagsläget endast har ansiktsigenkänning anser nu i efterhand att fingeravtryckläsaren är ett bättre alternativ för autentisering efter att ha använt ansiktsigenkänningen. Respondent 5, Respondent 9 samt De Luca och Lindqvist (2006) anser att fingeravtryckläsaren är en metod som är lättanvänd.

Resultatet av valet av autentiseringsmetod inom de biometriska metoderna är att funktionen skall vara enkel för användaren att använda, men som ändå bidrar till ett skydd mot informationen som privatpersoner vill skydda. Om funktionen inte är lätt att använda, autentiseringen stjälper, anser respondenterna att funktionen inte är användbar och föredrar en annan autentiseringsmetod.

## *7.3 Personlighetsdrag lagras*

*”Biometriska metoder innebär att mycket känslig data lagras, eftersom det är min identitet. Detta kan i sin tur leda till identitetskapningar som kan missbrukas om det hamnar i fel händer”,* en bra slutsats från Respondent 8 vad det gäller lagring kring de biometriska egenskaperna. Respondenterna är oroliga kring hur deras egenskaper lagras, av den anledning att det är mycket känslig information. Att använda sig av de biometriska autentiseringsmetoderna innebär en risk, enligt Prabhakar et al. (2003). De egenskaper som används vid dessa autentiseringsmetoder är begränsade, och en gång utsatt innebär att användarn alltid är utsatt för bedrägerier med deras personlighetsdrag, av den anledning att det finns ett begränsat antal av användarens unika drag. Enligt Nguyen och Dan (2019) finns även möjligheten för bedragaren att få journaler eller brottsregister till förfogande på grund av de biometriska egenskaperna. Däremot är det respondenter, tre av tio, som inte är oroliga kring att det lagras någonstans. Ett uttryck som *”varför just mig?”* uttrycks.

Att personlighetsdrag lagras är en oro som respondenterna uttrycker, vilket bidrar till att de biometriska autentiseringsmetoderna ifrågasätts. Respondenterna blir allt mer reserverade gentemot biometri på grund av lagringen, och kan innebära att biometri inte används lika mycket av privatpersoner.

## *7.4 Användarens integritet samt identitet*

De biometriska metoderna kan innebära att de biometriska egenskaperna inte endast används till det de är avsedda för i grund och botten. Sju av tio respondenter anser att de börjar känna sig alltmer övervakade. Enligt Matyas och Riha (2003) anses de biometriska systemen vara påträngande eller invasiva. Dessa system har en problemställning som bör redas ut, innan systemen är fullt pålitliga och kan användas på ett sätt som är säkert.
Att användarens integritet och identitet är i farozonen vid användning av de olika biometriska autentiseringsmetoderna är även detta en bidragande faktor till användningen. Om de biometriska autentiseringsmetoderna bryter mot identiteten samt integriteten innebär detta att privatpersoner känner sig övervakade, vilket till slut kan leda till mindre användning biometri. Detta är även något som är svårt att säkerställa, om de blir övervakade eller inte, men som är ett orosmoment.
Respondent 3 uttrycker sig som följande, som kan ses som ett bra avslut:

*”Man vet ju aldrig om kameran är påslagen. På något sätt känner jag mig alltid övervakad av min mobil, det tycker jag är läskigt”.*

# 8. Slutsats

I denna studie har följande forskningsfråga besvarats:

*Vad påverkar en användares val av biometriska metoder vid användning av en smartphone?*

Studien visar tydligt fyra olika faktorer som påverkar en användares val av den biometriska autentiseringsmetoderna.

Först och främst är det av stor relevans för användarna att skydda den ekonomiska del som användarens smartphone besitter, och stödjer användaren med. Anledningen till att respondenterna anser att ekonomin är den största anledningen till att använda sig av säkerhet av sin smartphone är då en obehörig drar nytta av deras ekonomiska position, vilket enligt respondenterna kan få förödande konsekvenser.

Privatpersonens val av de biometriska autentiseringsmetoderna bygger på att funktionen skall vara enkel. Privatpersonerna ser olika på vilket specifik autentiseringsmetod som är den absolut bästa, men det genomgående svaret är att det skall gå snabbt och smidigt att få åtkomst till sin smartphone. De olika anledningarna till de biometriska autentiseringsmetoderna är även dem i sin helhet samma, att det finns problem som avgör hur den specifika metoden fungerar i sin helhet och bidrar till att funktionen stjälper, istället för att hjälpa. I det stora hela är det funktionens enkelhet som bidrar till användarens val av biometrisk metod.

Privatpersoner som använder biometriska autentiseringsmetoder är även oroliga kring hur deras personlighetsdrag lagras, samt att de endast används för de som de är tänka till. Privatpersoner börjar känna sig allt mer övervakade, och är inte trygga med att egenskaperna endast används till just autentisering. Privatpersoner känner sig övervakade av den anledning att kameran som används till ansiktsigenkänningen är påslagen konstant vilket innebär att vem som helst kan kolla på privatpersonen i just detta tillfälle.

# 9. Diskussion

*I detta kapitel presenteras val av metodansats, resultatet kring studien, vetenskapliga, samhälleliga samt etiska aspekter att diskuteras. Samt framtida forskning, hur en forskning i framtiden kan byggas på denna utförda studie och presentera ytterligare resultat.*

## *9.1 Valet av metodansats*

Valet av metodansats realiserades tämligen omgående vid starten av denna studie. Valet föll på litteraturstudien, men möjligheten till intervjuer var även en stor bidragande faktor. Observationer var inget alternativ av den anledning att det hade varit svårt för observeraren att få fram något konkret som hade bidragit till någon nytta till studien, och frågeställningen ansågs inte passa en metod såsom observation. Med intervjuer och dess genomförande bidrog det till synpunkter, åsikter och citat som bidrog till att stärka studien, men även för att fånga upp synpunkterna som inte hade fångats vid en enkät eller liknande, som i så fall hade använts vid en kvantitativ metodansats. Den kvantitativa metodansatsen föll bort tämligen fort på grund av att studien inte var menad till att göra beräkningar eller siffror, vilket den kvantitativa metoden hade bidragit till.

I denna studie intervjuades tio privatpersoner, som föll in i det förbestämda urval som tidigare hade skapats. Genom en intervju kan missförstånd uppkomma, men för att validera dessa svar, att respondenten hade uppfattats på rätt sätt fick samtliga respondenter läsa igenom de transkriberade intervjuerna senare för att godkänna, vilket är en etisk aspekt men även för att studiens trovärdighet skulle vara så bra som möjligt. Genom att det endast är en forskare som utför denna studie, är det samma personer som utför samtliga moment, såsom intervjuer, transkribering, analys etcetera vilket bidrar till att mindre missförstånd eller missuppfattningar skedde. Forskningens validitet har även styrkts av den anledning att flertalet av respondenterna har svarat på liknande sätt under intervjuerna. Detta är ett indicium på att respondenterna har uppfattat frågan på ett korrekt sätt, eller på ett liknande sätt vilket har bidragit till att informationen stämmer.

Av den anledning att denna studie har utförts med hjälp av den kvalitativa metodansatsen, blir det aningen svårare att visa tillförlitligheten av studien. Men för att påvisa att studien är korrekt utförd samt att insamling av data och analysen har utförts på ett korrekt sätt. För att påvisa trovärdigheten av studien har urvalet av respondenter tydligt beskrivits samt dess avgränsningar. Insamling av data har tillika beskrivits grundligt, även utförandet av dataanalysen har grundligt beskrivits för att läsaren skall få en tydlig bild av hur studien faktiskt har gått till, och få en tydlig bild av att studien är realiserad på ett regelrätt sätt.
För att säkerställa att pålitligheten har varit en faktor som har tagits ställning mot i denna studie har bandspelare använts vid utförandet av intervjuerna, vilket är en viktig

del för att påvisa studiens reliabilitet. I denna studie användes en inbyggd mikrofon, av den anledning att forskaren inte hade tillgång till en separat, skall tilläggas att ljudet från respondenterna hördes tydligt vilket är det viktigaste.
Överförbarheten och tillämpningen av denna studie är tillämpbar genom att en materialpresentation har skapats, vilket innebär att under det kapitlet har endast den insamlade datan från intervjuerna skrivits ned. För att påvisa var dessa svar kommer ifrån har även en intervjuguide bifogats som en bilaga för att visa vad för frågor som ställdes samt att läsaren kan få en större förståelse för helheten av studien.

Som tidigare beskrivit hade en kvantitativ metodansats bidragit till mer siffror och beräkningar där studien hade varit mer evidensbaserad. Genom att använda den kvantitativa forskningsmetoden hade ett mer exakt antal kommit fram kring hur de olika respondenterna ansåg vilken biometrisk metod som de ansåg fungerar bäst, men ingen anledning till varför eller vad de anser hade kommit fram på samma sätt som vid tillämpning av den kvalitativa forskningsmetoden. Därav togs beslutet att den kvalitativa metodansatsen var bäst lämpad och kommer att bidra med mest intressanta aspekter kring de olika biometriska metoderna, eller den traditionella autentiseringsmetoden.

En viktigt synpunkt som skall tilläggas är att denna studie har genomförts med dessa tio respondenter, dock kommer de alla från samma ort. Med det sagt är det svårt att veta och säkerställa att studien stämmer över hela landet, samt att det kan ha varit andra svar om studien hade utförts på en annan ort, eller med andra respondenter. Även att respondenterna är i den yngre- till medelålder vilket bidrar till att den äldre generationens synpunkter inte har fångats. Detta kan innebära att den äldre generationen inte ser på samma sätt som den generation som har deltagit har uppfattats.

## *9.2 Resultatet av studien*

En synpunkt som är av stor relevans som kom fram under studien, främst från respondenterna men även från litteraturstudien, är att de biometriska autentiseringsmetoderna bidrar till att privatpersoner känner sig övervakade, eller att de anser att de bryter mot dess integritet eller identitet. De biometriska autentiseringsmetoderna lagrar de biometriska egenskaperna som privatpersoner anser vara mot deras godkännande. Att de biometriska egenskaperna lagras, är i realiteten är självklarhet på grund av att funktionen fungerar på det sättet. Dock finns det alltid förbättringssätt genom att säkerheten förbättras, vilket nämns i studien (Nguyen & Dang, 2019). Att detta är en oro hos privatpersoner är inga konstigheter, pågrund av de bedrägeri som sker idag. Allt fler bedrägerier sker dagligen och visst väcker detta oro och att privatpersoners personlighetsdrag finns att få tillgång till för bedragare än otrygghetskänsla, som forskaren till denna studie kan förstå till fullo.

En annan synpunkt som även tas upp är att alla biometriska funktioner inte fungerar varierande mellan yrken. Hantverkare har problem med fingeravtrycksläsaren, vid kontorsanställningar fungerar funktionen idealiskt. Detta är även en synpunkt som bör

tas med i förbättringsförslag, av den anledningen att en anställning inte skall göra så att funktionen i sig inte fungerar för vissa. Däremot är det förståeligt att funktionerna inte ännu är fullt utvecklade, men förhoppningvis är detta under förbättring för senare implementationer. Men även kanske detta sätt är en metod som eventuellt kommer att försvinna från smartphones i framtiden, eftersom det redan har försvunnit från vissa i dagsläget.

Den framtida forskningen som utförs inom detta område bör fokusera mer kring att fånga äldre som använder sig av dessa autentiseringsmetoder för att få en bredare syn på de faktorers om påverkar en privatpersons val. Däremot kan det vara en bidragande till att dessa privatpersoner har varit svåra att hitta i denna studie, att unga är infödda i den tekniska världen gentemot de äldre som istället har fått lära sig allt mer under årens gång. Att de har fått lära sig under årens gång kan vara en nackdel, att den ständigt kommer nya produkter inom tekniken och att de inte hänger med på samma sätt som den yngre generationen. En förutfattad mening är att den yngre generationen gillar att ha det senaste, och uppdaterar sig inom det tekniska mer kontinuerligt än vad den äldre generationen gör.

## *9.3 Vetenskapliga, Samhälleliga samt etiska aspekter*

Följande delkapitel kommer att diskutera de vetenskapliga, samhälleliga samt etiska aspekterna i förhållande till denna studie och dess resultat.

### 9.3.1 Vetenskapliga aspekter

Framtidens forskning inom biometriska autentiseringsmetoder bör fortsättningsvis fokusera på privatpersonernas säkerhet. Allt eftersom tekniken utvecklas allt mer är detta ett ämne som är av stor relevans att titta närmare på. De biometriska autentiseringsmetoderna bör bli säkrare för användarna, av den anledning att de personlighetsdrag som lagras är mycket individuella, och kan ses som närliggande till DNA (Prabhakar et al., 2003 & Nguyen & Dang, 2019). Säkerheten kring lagringen av de biometriska egenskaperna bör bli säkrare för att användarna skall känna sig helt säkra med att andra dessa funktioner. Detta yttrar sig i att respondenterna inte känner sig säkra vid användning av dessa funktioner, och det må tas på allvar.

Funktionerna är smidiga till den grad att det går snabbare för användaren att få åtkomst till sin smartphone, men priset och risken att det ska gå snabbt och smidigt börjar ses som en nackdel och att användare börjar ta avstånd gentemot dessa funktioner.

Studiens resultat inom de vetenskapliga aspekterna bidrar till att forskningen inom detta område bör prioriteras, av den anledning att allt fler enheter använder dessa autentiseringsmetoder. Dessa funktioner påvisas vara relativt dyra vid implementering, beroende på val av biometrisk autentiseringsmetod, och bör därför vara säkra vid användning. Både för användaren men även för tillverkarna, att deras användare faktiskt

använder funktionen som sådan, annars blir det till slut en funktion som endast kostar pengar och är onödig i slutändan.

### 9.3.2 Samhälleliga aspekter

Det märks tydligt att samhället är präglade inom filmer och serier vad det gäller biometriska autentiseringsmetoder (Muller, 2017). Flertalet gånger nämns det av respondenter att biometriska metoder relateras till filmer och serier, vilket innebär att privatpersoner har en viss syn på dessa metoder. I filmer och serier är inte alltid dessa metoder fullt realistiska, och som åskådare av detta påverkas privatpersoner av hur framställningen av biometrin framställs. Däremot är vissa respondenter i denna studie ifrågasättande till hur trovärdiga vissa visualiseringar av de biometriska metoderna faktiskt är, vilket är en bra sak. Som åskådare till film och serier bör tittare vara aningen ifrågasättande till hur det faktiskt fungerar samt hur realistiskt vissa scener är.

Detta innebär att vid ställningstagande till vilken biometrisk funktion respondenterna känner sig säkrast med, varav hur de tror att en manipulation fungerar kring dessa funktioner nämns ”hugga av finger” av ett par respondenter, men att de tillägger att de inte är säkra på hur realistiskt det faktiskt är. Detta är sådana sekvenser som visas när det gäller biometriska funktioner, men att det finns andra vägar att manipulera dessa funktioner.

Respondenterna yttrar en oro kring att bli allt mer övervakade. Att samhället blir allt mer övervakat, samt att som individ inte kunna göra så mycket, förutom att undvika biometriska autentiseringar som är ett alternativ. Att biometrisk autentisering bidrar till att individer känner sig allt mer bevakade, och inte litar på att smartphonen som individen använder sig av är övervakad på något sätt. Ett exempel på det kan vara att kameran är påslagen ständigt vilket inte syns eller märks av användaren. Detta anses vara ett orosmoment, och frågan är då om de biometriska autentiseringsmetoderna bidrar med positivitet, eller om det drar ned och stjälper användaren istället. Ett annat orosmoment är även lagring av de egenskaper som används vid användningen av de biometriska autentiseringsmetoderna. Är säkerheten kring detta tillräckligt eller krävs det mer? Respondenterna i denna studie uttrycker att de är oroliga kring lagringen, och vet om att de biometriska egenskaperna lagras.
Att dessa olika otrygghetskänslor uppkommer under denna studie är ett faktum, men frågan är vad för slags ytterligare synvinklar kring dessa funktioner hade nämnts vid en fördjupning inom just detta specifikt hade uppkommit. Är användarna så oroliga över detta, eller är det just dessa respondenter för denna studie som är det?

Ovanstående stycke är ett beaktansvärt resultat som har framkommit under denna studie, och som forskaren anser behövs undersökas mer - hur användarna ser på övervakning och lagring etcetera som medföljer vid användningen av de biometriska autentiseringsmetoderna. Men även att respondenterna uttrycker olika slags missnöjen med de olika metoderna, vilket även framkommer under litteraturstudien (Mayron et al., 2013). Att det både uppkommer från litteratur samt respondenterna i denna studie är

något som kan anses som en början av ett allt mer fördjupat arbete och forskning kring detta, men att en början framförallt finns är viktigt. Det viktigaste för användarna vid användning av de biometriska autentiseringsmetoderna är att det skall gå snabbt och smidigt, vilket är en bidragande effekt av hur samhället ser ut i dagsläget. Allt skall gå snabbt, det ska vara smidigt men en viktigt synpunkt är även att användaren ska känna sig säker vid användandet. Inga oerhörda konsekvenser ska ske vid någon slags attack eller bedrägeri, som är fallet vid de biometriska autentiseringsmetoderna. Ifall en attack eller bedrägeri sker skall tilläggas.

### 9.3.3 Etiska aspekter

De etiska aspekterna var av stor relevans vid utförandet av studien. Mest på grund av att de medverkande, respondenterna, har fått information om dess rättigheter vid medverkande så att de kan medverka på ett sätt som är till deras fördel. De fyra olika individskyddskraven har realiserats under denna studie, på det sätt att individerna har rätt till att förbli anonyma (konfidentialitetskravet). Däremot har deras yrken offentliggjorts, men med samtycke från samtliga respondenter. Trots att respondenternas yrken har offentliggjorts i denna studie är det inget som går att spåra till vilken specifik individ det är, samma gäller respondentens ålder. Respondenterna fick även information om studien handlar om (informationskravet), samt vad syftet är vilket i detta fallet är examensarbete.

Respondenterna har även fått läsa igenom och gett godkänt till transkriberingen som har utförts efter att intervjun har genomförts. Av den anledning att intervjuerna utfördes med några dagars mellanrum transkriberades intervjun tämligen omgående efter att intervjun genomfördes, vilket ledde till att respondenten samt forskaren hade ett färskt minne av vad som sades under intervjuerna. Det innebar även att tidsåtgången mellan intervjun och transkribering tills dess godkännande var relativt knapp, vilket även hjälpte till i studiens förutbestämda tidsram.

Respondenterna informerades även om att deras medverkan gick att avbryta under hela forskningsprocessen, från dess början till slut (samtyckeskravet). Detta innebar även att respondenternas intervjusvar raderas omgående, vilket respondenterna fick information om i starten av intervjun, men även en påminnelse när intervjun var avklarad, för att upprepa respondentens rättigheter.

Den sista individsskyddskravet innebär att respondentens medverkan endast används till denna specifika studie, och kommer alltså inte att användas till något annat (nyttjandekravet). Även detta kravet går i enlighet med vad Vetenskapsrådet (2002) menar, vilket samtliga ovanstående individskyddskrav likaså.

# Referenser


Andronache, A., & Althonayan, A. (2018). Shifting From Information Security Towards A Cybersecurity Paradigm. *ICIME 2018, Proceedings of the 2018 10th International Conference on Information Management and Engineering* pp 68-79. DOI: 10.1145/3285957.3285971.

Bao, P., Pierce, J., Whittaker, S., & Zhai, S. (2011). Smart phone use by non-mobile business users. *MobileHCI'11 Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services,* ss. 445-454. DOI: 10.1145/2037373.2037440.

Berndtsson, M., Hansson, J., Olsson, B., & Lundell, B. (2008). Thesis Projects: A Guide for Students in Computer Science and Information Systems, 2nd ed. London: Springer Verlag.

Bhanushali, A., Mange, B., Vyas, H,. Bhanushali, H. & Bhogle, P. (2015). Comparison of Graphical Password Authentication Techniques. *International Journal of Computer Applications (0975 – 8887)* Vol 116, No. 1. DOI: 10.5120/20299-2332

Bhattacharyya, D., Ranjan, R., Alisherov, F. & Choi, M. (2009) Biometric Authentication: A Review. *International Journal of u- and e- Service, Science and Technology* Vol. 2, No. 3.

Burgbacher, U., Prätorius, M., & Hinrichs, K. (2014). A behavioral Biometric Challenge and Response Approach to User Authentication on Smartphones. *IEEE International Conference on Systems, Man, and Cybernetics (SMC)* ss. 3328-3335.

Buriro, A., Crispo, B., DelFrari, F. & Wrona F. (2016). Hold & Sign: A Novel Behavioral Biometrics for Smartphone User Authentication. *2016 IEEE Security and Privacy Workshops (SPW).* DOI: 10.1109/SPW.2016.20.

Choudhury, B., Then, P., Issac, B., Raman, V. & Haldar M, K. (2018). A Survey on Biometrics and Cancelable Biometrics Systems. *International Journal of Image and Graphics* Vol. 18, No. 01. DOI: 10.1142/S0219467818500067.

Dobos, L. (2018). Så lyckades forskare skapa falska avtryck som lurar fingeravtrycksläsare. *Techworld,* 26 november. https://techworld.idg.se/2.2524/1.710926/falska-fingeravtryck-forskare

Faundez-Zanuy, M. (2006). Biometric security technology. *IEEE Aerospace and Electronic Systems Magazine* vol. 21, no. 6, *pp*. 15-26.

Ferrag, M.A, Maglaras, L., & Derhab, A. (2019) Authentication and Authorization for Mobile IoT Devices using Bio-features: Recent Advances and Future Trends. *arXiv: 1901.09374[cs.CR]*

Harakannanavar, S. S., Renukamurthy, P. C., & Raja, K. B. (2019). Comprehensive Study of Biometric Authentication Systems, Challenges and Future Trends. *Int. J. Advanced Networking and Applications* Vol. 10, Issue 04, pp 3958-3968.

Matyas, V. & Riha Z. (2003) Toward Reliable User Authentication trough Biometrics. *IEEE Security & Privacy* Vol. 99, Issue: 3.

Mayron, L., Bahr, G.S., & Hausawi, Y. (2013). Secure, Usable Biometric Authentication Systems. *Universal Access in Human-Computer Interaction. Design Methods, Tools, and Interaction Techniques for eInclusion*, pp. 195-204. DOI: 10.1007/978-3-642-39188-0_21

Muller, I, E. (2017) Biometrics in Film: True or False. *Veridium,* 2 mars. https://www.veridiumid.com/blog/biometrics-in-film-true-or-false/

Myndigheten för samhällsskydd och beredskap (MSB) (2015). *Detta är informationssäkerhet.* https://www.informationssakerhet.se/Om-informationssakerhet-kon/vad_ar_informationssakerhet/ [2019-02-16]

Myndigheten för samhällsskydd och beredskap (MSB) (2015). *Informationssäkerhet som privatperson.* https://www.informationssakerhet.se/Om-informationssakerhet-kon/informationssakerhet-i-hemmet/ [2019-02-16]

Nguyen, T, A, T. , Dang, T, K. (2019). Privacy preserving biometric-based remote authentication with secure processing unit on untrusted server. *IET Biometrics*, vol 8, pp. 79-91. DOI:10.1049/iet-bmt.2018.5101.

Oates, B. J. (2006) *Researching Information Systems and Computing*. London: SAGE Publications Inc.

Patton, M. Q. (2015). *Qualitative Research & Evaluation Methods* (4 uppl.). USA: SAGE Publications Inc.

Pfleeger, C. P., Pfleeger, S. L., & Margulies, J. (2015). *Security in computing*. 5. Uppl., USA: Harlow: Prentice Hall.

Pocovnicu, A. (2009). Biometric Security for Cell Phones. *Informativa Economica* vol 3, No 1.

Prabhakar, S., Pankanti, S. & Jain, A. K. (2003) Biometric recognition: security and privacy concerns. IEEE Security & Privacy, vol 1, Issue 2, pp. 33-42. DOI: 10.1109/MSECP.2003.1193209

Rosenthal, M. (2016). Qualitative research methods: Why, when, and how to conduct interviews and focus groups in pharmacy research. *Currents in Pharmacy Teaching and Learning 8* pp 509-516.

Ryen, Anne & Håkansson, O (red.). (2004) *Kvalitativ Interjvu - från vetenskapsteori till fältstudier*. Malmö: Liber AB.

Solms, V,R., Niekerk, V,J. (2013). From information security to cyber security. *Computers & Security* vol 28, pp 97-102. DOI: 10.1016/j.cose.2013.04.004.

Swedish Standards Institute (SIS) (2015). Terminologi för informationssäkerhet 50:2015. Tillgänglig på internet: https://www.sis.se/api/document/preview/8014024/ [Hämtad 2019-04-10]

Trost, J. (2005). *Kvalitativa intervjuer*, 3.uppl., Lund: Studentlitteratur AB.

Tu, Z. & Yuan, Y. (2014). Critical Success Factors Analysis on Effective Information Security Management: A litteratur Review.

Tvrdíková, M. (2008). Information system integrated security. *7th Computer Information Systems and Industrial Management Applications.* DOI: 10.1109/CISIM.2008.41.

Vetenskapsrådet (2002). *Forskningsetiska principer inom humanistisk-samhällsvetenskaplig forskning.* http://www.codex.vr.se/texts/HSFR.pdf [2019-02-26].

Wollner, A. (2018) Bra med alternativ till lösenord – men långt kvar innan vi är helt säkra. *PC för Alla,* 20 januari. https://pcforalla.idg.se/2.1054/1.692722/bra-med-alternativ-till-losenord-men-jattarna-har-mycket-arbete-kvar?queryText=biometri

Åhlfeldt, R.-M., Spagnoletti, P., & Sindre, G. (2007) Improving the Information Security Model by using TFI. *New Approaches for Security, Privacy and Trust in Complex Environments* pp. 73-84. DOI: 10.1007/978-0-387-72367-9_7.

# Bilaga 1 - Anmälan av intresse för deltagande

**Hej!**

Jag studerar Systemvetenskapliga programmet på Högskolan i Skövde och håller just nu på att skriva mitt examensarbete. Jag har valt att inrikta mig mot Informationssäkerhet med en ytterligare inriktning mot autentisering, såsom traditionell samt biometri. Inriktningen har gjorts för att belysa de synvinklar som privatpersoner har kring användandet av dessa autentiseringsmetoder samt fånga upp olika aspekter kring hur dessa autentiseringsmetoder uppfattas och används av just privatpersoner.

Mitt examensarbete går ut på att göra en forskning, som en slags undersökningar jag har valt att använda den kvalitativa metoden för att kunna genomföra mitt arbete. Jag har valt att göra den kvalitativa metoden med hjälp av intervjuer, och är därför i behov av hjälp från just Er.

Min tanke är att ställa grundläggande frågor kring de utvalda autentiseringsmetoderna, hur Du använder dem, och vad du anser om just dessa metoder. Jag vill gärna intervjua er som har en smartphone som har ansiktsigenkänning, och har haft en telefon med fingeravtryckskläsare. Det går även bra att ha en telefon som har båda dessa funktioner.

Jag skulle vara väldigt tacksam om just Du vill hjälpa mig att genomföra mitt examensarbete, och anmäla ditt intresse i tabellen nedan om Du vill hjälpa mig. Den beräknade tidsåtgången är cirka en timme, och för att underlätta för Dig bestämmer vi en mötesplats som passar Dig bäst.

Jag hoppas på en positiv respons på denna förfrågan, och hoppas återigen att Du vill hjälpa mig med detta!

*Med vänliga hälsningar*
Josefin Johansson Telefonnummer: XXX XX XX XXX

| **Intresseanmälan** | | |
|---|---|---|
| **Namn** | **Ålder** | **Telefonnummer** |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

# Bilaga 2 - Intervjuguide

*- Introduktion och presentation av arbetet*
*- Förklara de etiska aspekterna för respondenten*

- **Allmänt**

- Vad har du för smartphone?
- Tycker du att det är viktigt att skydda den information som du har i din smartphone?
- Vad anser du vara den viktigaste informationen som du har i din smartphone, som du vill skydda?
- Har du köpt din smartphone på grund av dess säkerhetsfunktioner, eller de övriga nya funktionerna? Eller något annat?

- **Allmänt om autentisering**

- Vet du vad autentisering är?
- Vet du vad traditionell autentisering är? Kan du förklara med dina egna ord vad det är.
- Vet du vad biometrisk autentisering är? Kan du förklara med dina egna ord vad det är.
- Vad ser du för för- och nackdelar med dessa metoder inom autentisering?
  - Traditionella =
  - Biometriska =
- Har du någon gång blivit utsatt för någon slags attack på din smartphone?
- Använder du din smartphone i osäkra miljöer? Kopplar upp till okända nätverk etc.

- **Respondenternas användning av traditionell autentisering**

- Använder du någon gång traditionell autentisering på din smartphone?
  - På vilket sätt? När?
  - Hur många siffror/tecken använder du?
  - Tycker du att det känns som ett säkert sätt att skydda din smartphone med?

- **Respondenternas användning av biometrisk autentisering**

- Använder du den biometriska funktionen som finns på din smartphone?
  - Varför/Varför inte?
- Tycker du att den biometriska metoden är smidig? Fungerar bra? Fungerar dåligt? På vilket sätt, varför?
- När kan du känna att den biometriska metodens funktion brister?
- Tror du att de biometriska autentiseringsmetoderna är framtidens verifiering?
  - Varför/Varför inte?
  - Om du hade fått välja en av de biometriska metoderna, vilken hade du ansett vara den säkraste? (Fingeravtryck, röstigenkänning, iris-igenkänning, ansiktsigenkänning)
    - Varför tror du att den är säkrast?
- Du har använt både fingeravtryck & ansiktsigenkänning, vilken funktion tycker du har fungerat bäst?
- Vilken funktion kände du dig säkrast med?

- Varför?
- Tycker du att den biometriska metoderna underlättar eftersom du inte behöver komma ihåg något eller ha något med dig för att identifiera dig?

**Integritet och identitet**

- När du använder din traditionella autentiseringsmetod (pinkoden), är du någon gång rädd för att någon annan ser din kod?
- Anser du att de biometriska autentisieringen bryter mot din identitet eller liknande?
  - Varför/Varför inte?