Examensarbete

HÖGSKOLAN I SKÖVDE

VILKA ASPEKTER AV ETT SYSTEM FÖR DIGITALA ID-HANDLINGAR ÄR VIKTIGA FÖR SYSTEMETS EFFEKTIVITET, TILLGÄNGLIGHET OCH SÄKERHET?

WHICH ASPECTS ARE IMPORTANT FOR A DIGITAL ID-CARD SYSTEM'S EFFICIENCY, ACCESSIBILITY AND SECURITY?

Examensarbete inom huvudområdet
Informationsteknologi
Grundnivå 30 Högskolepoäng
Vårtermin 2025

Emil N. Florentsson

Handledare: Christian Lennerholt
Examinator: Mikael Berndtsson

Sammanfattning

Syftet med denna rapport är att kunna öka förståelsen för hur digitala id-handlingar kan användas för att förbättra effektivitet, tillgänglighet och säkerhet för alla medborgare. Studiens syfte är att hjälpa till i utvecklingsprocessen för digitala id-handlingar och se till att alla medborgare kan känna sig trygga i att använda ett digitalt system för id-handlingar.

Denna studie inkluderar intervjuer med flera personer, både i deras yrkesroll och som privatpersoner, för att få en övergripande bild av hur digitala legitimationer kan underlätta för olika grupper. Studien är baserad på en kvalitativ metodansats, vilket innebär att ett litet antal respondenter har valts ut för detaljerade och djupgående intervjuer. Trots det begränsade antalet intervjuer har många respondenter gett liknande svar på de flesta frågor, vilket indikerar att datamättnad har uppnåtts.

I studien framkom det fort att de aspekterna som betyder mest är kryptering, tillgänglighet, offlineanvändning, dataskydd och kostnad. Dessa faktorer identifierades redan i den första intervjun, däremot genomfördes flera intervjuer för att kunna motivera en datamättnad i intervjuerna. Studien är dock begränsad av att vara ett examensarbete, och det finns få relevanta forskningsartiklar på området. Den begränsade tiden för att genomföra rapporten innebär att vidare forskning med fler intervjuer och praktiska tester av en utvecklad applikation behövs.

Slutsatsen blev att alla dessa aspekter är viktiga att ta i beaktning för att systemet ska vara så effektivt, tillgängligt och säkert som möjligt.

Sökord: digitala id-handlingar, e-id, e-legitimation, effektivitet, tillgänglighet, säkerhet, användaracceptans, myndigheter, statliga e-tjänster, digitalisering

Abstract

The purpose of this report is to increase understanding of how digital identification documents can be used to increase efficiency, accessibility, and security for all citizens. The purpose of the study is to aid the development of digital identification documents, and to ensure all citizens can feel safe in using a digital system for identification documents.

This study includes interviews with multiple people, either as their professional role or as a citizen, this to get an wide understanding of how digital id-documents can aid different groups of people. The study is based on a qualitative research approach, which implies a low number of respondents have been selected for a more detailed and explorative interview. Despite the low number of interviews, a lot of people have given similar answers , indicating data saturation has been met.

In this study it was clear early that the aspects that matter most are encryption, accessibility, offline usage, data protection and cost. These aspects were identified in the first interview, although to motivate for data saturation multiple more interviews were made. The study is limited due to the fact that the study is a bachelor thesis article, there are not nearly enough relevant scientific papers in this scientific area. The limited time to research within this topic means that another study would have to be made with even more interviews and a practical test with an developed application.

The conclusion of this article is that it is important to take all of these aspects into consideration when developing a system to reach a good level of efficiency, accessibility and security.

1. Inledning

Denna uppsats handlar om en analys av flera olika aspekter inom digitala id-handlingar. Digitala id-handlingar handlar om plastkortet som finns idag och hur det ska behandlas när det digitaliseras i framtiden. Digitala id-handlingar kan lätt blandas ihop med e-id (e-legitimationer), dock handlar e-id om digitala signaturer och identifieringar, inte om fysisk legitimering med ett digitalt kort. EU håller just nu på med att undersöka hur de kan utveckla en applikation för att ha pass och nationell id-handling i, som ett tillägg till de fysiska som redan finns. (Europeiska kommissionen, 2021)

Inom ramen för denna uppsats fanns det inte tid för att utveckla en applikation för digitala id-handlingar samt genomföra en analys av befintliga och teoretiska system. Därför innehåller denna uppsats endast en analys av befintliga och teoretiska system.

Analysen innehåller tre olika aspekter: effektivitet, tillgänglighet och säkerhet. Dessa har analyserats genom tre olika metoder för datainsamling, en öppen intervju med olika legitimationskontrollanter (polis, passkontrollant, ordningsvakt, butikspersonal osv.). Målet med den öppna intervjun är att fånga en övergripande bild över situationen, men samtidigt få en mer detaljerad bild över hur digitala id-handlingar kan underlätta deras arbete. Sedan finns det även en studie som har genomförts genom google forms där respondenter helt anonymt svarar på frågor om hur digitala id-handlingar kan underlätta för dem i deras vardag. Studiens mål är att fånga en övergripande helhetsbild över situationen utan att gå in på för mycket detalj då personerna som svarar på studien varken arbetar med området eller är experter inom området. Till sist genomfördes en datainsamling genom en litteraturstudie där jag som författare går igenom många vetenskapliga och statliga rapporter om just digitala id-handlingar, eID och nära relaterade ämnen.

Till sist jämförs alla svaren från de olika data insamlingarna i kapitlen “analys” och “diskussion” för att sedan skriva ett relevant resultat. Avslutande på rapporten kommer en slutsats där forskningsfrågan kommer att besvaras. I slutsatsen kommer hela forskningsfrågan besvaras genom att skriva om varje delmoment i forskningsfrågan.

2. Bakgrund

2.1. Digitala ID-handlingar (legitimationer)

Med digitala id-handlingar i denna uppsats menas en applikation på en mobiltelefon, surfplatta eller PC där en användare kan legitimera sig för att kunna logga in på en webbtjänst eller visa upp för passkontrollanten i tullen för att verifiera ålder. Det finns ett annat begrepp som också kommer att användas i denna uppsats "e-id" (elektronisk identifiering), detta syftar däremot endast mot legitimationer som används för att logga in på webbtjänster eller köpa produkter / tjänster online. E-id erbjuder inte möjligheten för att användas vid fysisk legitimering. E-id kan även innebära att det finns ett digitalt chip på den fysiska legitimationen. Detta chip kan användas för att verifiera legitimationen och se att det är en riktig legitimation och inte förfalskat. (Siddhartha, 2008)

En legitimation kan utfärdas av både myndigheter och privata företag, medan en id-handling endast kan utfärdas av myndigheter. Några exempel på id-handlingar är: pass, nationellt id-kort, körkort m.m. Några exempel på legitimationer är: läkarlegitimation, lärarlegitimation m.m. (legitimation.se, n.d.). I denna uppsats görs däremot ingen skillnad på legitimation och id-handling, dessa begrepp används här som synonymer.

2.2. Effektivitet

Effektivitet kan mätas på många olika sätt, ett av dessa är kvalitet * volym / resurs (Sveriges Kommuner och Regioner, 2024). Där kvalitet innebär hur bra tjänsterna är, volym menar hur mycket tjänster som kan erbjudas och resurs innebär hur mycket pengar som läggs ned på området.

I denna rapport kommer effektivitet att mätas på följande sätt. Jämföra hur mycket resurser som går åt för att underhålla både digitala och fysiska legitimationer och hur mycket pengar som kommer att gå åt för att utveckla och underhålla systemet. Effektivitet innebär dock även tiden det tar att ta fram / kontrollera en legitimation, minimering av mänskliga fel och hur ett system kan underlätta för personer i deras privatliv och / eller deras yrkesroll.

2.3. Tillgänglighet

I denna uppsats kommer tillgängligheten handla om hur enkelt ett system är att använda. Idag är det väldigt många äldre som inte vill eller inte kan använda internet och / eller digitala ID-handlingar (Internetstiftelsen, 2023). Detta är något som måste förbättras i Sverige och i denna uppsats kommer det att diskuteras hur sådana system för digitala id-handlingar ska utvecklas för att alla ska kunna komma åt det. Detta skulle kunna ske genom ett enklare system, eller ett system som inte kräver internet, eller ett system som staten äger istället för att id-handlingen ska vara ägt av privata företag (såsom banker). Polismyndigheten eller Transportstyrelsen hade varit väldigt bra

kandidater för ett liknande system, där polisen tillhandahåller nationella id-kort, pass m.m. medan Transportstyrelsen tillhandahåller körkort som en digital legitimation.

2.4. Säkerhet

Säkerhet är något som många oroar sig över. Under en konferens 1986 presenterades en metod för digitala id-kort, digitala betalkort och så vidare (Siddhartha, 2008). Under den presentationen fanns det flera faktorer som var risker ifall olika länder inte började använda digitala id-kort och bankkort, dessa var bland annat följande; pass kan foto kopieras, kreditkortsnummer kan kopieras och att hackers och avlyssnare kan knäcka lösenord.

På senare tid har frågan om digitala id-kort drivits framåt av flera andra aspekter istället, dessa är till exempel; UN (United Nations) har drivit fram det som kallas för "nästa generation av pass" där passet har ett digitalt chip som integrerar biometrik och kan verifieras i passkontrollen med hjälp av en speciell läsare (Siddhartha, 2008). I Sverige just nu är det den sorts teknik som används, där passen och nationella id-handlingarna har digitala chip i sig för att verifiera legitimationen och kontrollera biometrik.

2.5. Mätning av framsteg inom digitalisering av offentlig verksamhet

Det går att mäta framsteg i digitalisering på många olika sätt, fem av dessa är olika index som olika myndigheter skapar årligen eller vartannat år. Dessa är EGDI (E-Government Development Index), DAI (Digital Adoption Index), Waseda-IAC, GODI (Global Open Data Index) och EPI (E-Participation Index). Dessa kan vara bra på sina egna sätt, däremot skriver Febiri & Hub (2021) om hur dessa är dåliga då de inte tar med hela bilden. Febiri & Hub (2021) tar istället fram 7 olika aspekter på hur det går att mäta framstegen inom digitalisering av offentlig verksamhet, Effektivitet, Användbarhet, Säkerhet, Tidlöshet, Dataanvändning, Framgång och Kostnadsfaktor och Digital kompetens. Alla dessa faktorer enskilt ger inte en speciellt bra bild på hur framstegen inom digitaliseringen ser ut, däremot ger dessa faktorer tillsammans en bra bild på det. (Febiri & Hub, 2021)

Effektivitet

När forskare undersöker digitalisering av offentlig verksamhet har de i åtanke den relativa moderniteten, detta skiljer sig från digitaliseringen av privat sektor då de inte tänker på den relativa moderniteten. Inom detta inkluderas mängder av olika saker: kvaliteten på back office-system, stora databaser, front office-mjukvara, datorerna, nätverkshastigheten, och många fler.

Det spelar ingen roll om ett system är helt nytt eller gammalt då det enda som övervägs är hur mycket som kan produceras av systemet, detta är varför mycket uppmärksamhet ska placeras på just effektivitet. Effektivitet innehåller flera olika aspekter. Effektivitet som ett digitalt system; här tänker forskare på tillförlitligheten på hårdvara, effektiviteten av mjukvara och ifall det finns tillräckligt med bandbredd. En annan aspekt som tas i åtanke är effektivitet som ett specifikt system; till exempel, ett skattesystem

som fokuserar på resultaten som en högre grad av skatteinsamling eller lägre mängd skattefusk (Febiri & Hub, 2021). Den sista aspekten som tas i beaktning är den dynamiska effektiviteten, här tänker forskare på teknologi-fria system då de vill framtidssäkra systemen för att se till att myndigheter inte blir beroende av ett system som endast ett företag i världen kan göra service på (Febiri & Hub, 2021).

Användbarhet

Användbarhet är ett välkänt begrepp och ett väldefinierat koncept inom människa-datorinteraktioner (MDI). Här fokuseras på hur bra en människa och en dator kan "kommunicera" med varandra. Användbarheten är det som definierar hur bra ett system är; det är den som kan skilja på system som faktiskt gör det som invånarna behöver och de system som bara finns där för att det ska se bra ut. (Febiri & Hub, 2021)

Säkerhet

Just nu håller oron över användarnas dataintegritet öka. Den övergripande säkerheten över användares data kommer att vara en aspekt i alla digitaliseringsprojekt inom offentlig verksamhet. Personer litar på staten med sin känsliga data, däremot skadar dataläckor detta förtroende, då viss data som läcks eller stjäls kan komma att skada ett lands stabilitet och säkerhet. Ökade säkerhetsstandarder och ökade hot mot datan har ökat behovet av en strategi för hur dataintegriteten ska behållas och risken för dataläckor och dataintrång ska reduceras. Ett annat exempel på ökad säkerhet kan vara kryptering, biometrisk inloggning, ett säkert statligt ID, flerfaktorsautentisering och mycket mer. (Febiri & Hub, 2021)

Aktualitet

Denna aspekt innebär statens kapacitet att förvandla en idé för ett projekt till ett faktiskt system som gör vad invånarna i landet vill inom en rimlig tidsram (Febiri & Hub, 2021). Tiden som ett projekt tar är en väldigt viktig aspekt för projekt inom offentlig verksamhet. Den här aspekten är ofta beroende på hur stort själva projektet är och hur mycket tidigare erfarenhet som den utvecklande avdelningen har sedan tidigare för att rensa bort problem som ofta uppstår redan i början. Denna kunskap kan vara både intern eller extern med en bra kontakt till beslutsfattare. (Febiri & Hub, 2021)

Dataanvändning

Den här mätpunkten innebär hur statliga institutioner använder data. Detta inkluderar hur de tar in data från invånarna och strukturerar upp den för att analysera hur det ser ut i landet. Datan kan också användas för att se insikter på företag som finns i området. Potentiella åtgärder åt dåligt värde på denna punkt skulle kunna vara, omorganisering inom en sektion, komma på strategier eller utveckla KPIer (Key Performance Indicator) runt vad invånarna eller företagen vill ha, istället för utbudsdrivna faktorer. (Febiri & Hub, 2021)

Framgångsfaktor och kostnad

Aspekterna framgångsfaktor och kostnad innebär många olika saker, det kan vara allt från kostnad av ett projekt till hur bra ett projekt går (Febiri & Hub, 2021). Dessa kan bli influerade av flera olika aspekter såsom: hur väl ledare och beslutsfattare kan säkra försvarbara priser "värde för pengarna", hur mycket som ges till externa konsulter istället för instansens egna resurser, hur relationen mellan företag och staten ser ut, företag som skriver kontraktsvillkor som skyddar dem från framtida marknadsförändringar, och långtidskontrakt som leder till att endast befintliga företag kan göra ändringar mitt i kontraktet. (Febiri & Hub, 2021)

Digital kompetens och färdigheter

Denna punkt inkluderar flera olika aspekter som alla är viktiga: hur mycket som spenderas på digital marknadsföring, märkes igenkänning, organisationen räckvidd på marknaden, digital mognad av de anställda (inklusive styrelse och högre chefer), hur mycket de tjänar på den digitala marknaden, och bidrag till digitala initiativ från varje avdelning. (Febiri & Hub, 2021)

2.6. Tidigare utveckling av ett digitalt körkort

Raj et al. (2016) skriver om ett sätt som digitala körkort kan utvecklas i deras rapport. De gjorde en applikation där en användare kunde logga in med användarnamn och lösenord för att komma åt sitt körkort. Därefter kunde polisen vid ett rutinmässigt stopp kontrollera och verifiera personens körkort direkt från appen. Polisen hade i detta fallet speciell inloggning där de kunde skriva in personnummer och verifiera körkort och vilka trafikbrott föraren hade lagrat i deras register. I undersökningen visade det sig att deras applikation var smidigare och snabbare än hur det gått till traditionellt. (Raj et al., 2016)

Applikationen utvecklades i flera olika teknologier, såsom PHP och MySQL, och kommunikationen mellan dessa sker i JSON (Raj et al., 2016). Detta är ett relativt säkert sätt att göra detta i fallet att ingen får tag på API nyckeln. Ifall en obehörig får tag på en API nyckel kan de komma åt den användarens användaruppgifter och logga in som den användaren, däremot ifall en obehörig får tag på en av polisernas API nyckel kan de ta sig in i systemet och kontrollera körkort, men också sätta ut böter på personer. Alla dessa kontroller skickas via HTTPS protokollet (Hypertext Transfer Protocol Secure) vilket är ett protokoll för att hemsidor och applikationer ska kunna skicka data mellan en enhet och en server säkert. (Raj et al., 2016)

Med denna applikationen skulle körkortsförfalskningar kunna minskas ordentligt då föraren av fordonet aldrig kan modifiera databasen med körkorten. (Raj et al., 2016) Föraren kan endast se sitt eget körkort och vilka behörigheter denne har. Polisen måste kunna verifiera körkort, däremot behöver inte polisen kunna ta ut en lista på personer som har körkort och därför kan det argumenteras för att denna applikation har bra informationssäkerhetsaspekter. Applikationen har dessutom endast överföringar av

textinformation och inga bilder eller andra “tunga” filer (filer som tar mycket plats på en enhet). (Raj et al., 2016)

Denna applikation är däremot i sitt första stadie och kommer därmed inte att publiceras till allmänheten, applikationen kan uppgraderas senare och inkludera flera andra aspekter såsom försäkring, skatt o.s.v. (Raj et al., 2016). På grund av att denna applikation är i första stadiet kommer applikationen endast att testas med interna tester istället för att testas med faktiska poliser och förare. Applikationen kan även generera en QR-kod vilken polisen kan skanna för att verifiera körkortets giltighet (Raj et al., 2016). Denna QR-kod hade även kunnat användas till flera andra uppgifter, till exempel när en person behöver visa legitimation för att köpa varor med åldersgräns eller att hämta ut paket från postutlämningen.

Genom sökning hos Google Scholar, diva-portalen och flera andra källor har inte många forskningsartiklar som handlar om digitala id-handlingar hittats. Däremot har flertalet forskningsartiklar och myndighetsrapporter om e-id hittats, detta är varför detta kapitel har mycket om e-id jämfört med mindre om digitala id-handlingar.

2.7. Digital identifiering och betalning i dagsläget

Bank-ID används av de flesta svenskar idag (Internetstiftelsen, 2023). Däremot finns det ändå många äldre som inte vill eller kan inte använda det. Detta kan vara av flera anledningar, att de inte har tillgång till en mobiltelefon, inte har tillgång till internet alls, eller saknar ett bankkonto som erbjuder det (Internetstiftelsen, 2023). Att äldre inte vill kan vara på grund av att Bank-ID idag är ägt av ett privat företag eller att de inte ser poängen i att ha Bank-ID när allt som går att göra digitalt fortfarande går att göra med papper.

Freja eID används inte av speciellt många då Bank-ID utvecklades först och blev populärt fort. Freja eID används endast av 3% av den svenska befolkningen, däremot främst av 00-talister (9%) (Internetstiftelsen, 2023). Freja eID har exakt samma problem som Bank-ID har, däremot större. Freja eID används inte av äldre, det ägs av ett privat företag och företaget lanserade produkten senare än Bank-ID. Bank-ID har även spridits väldigt mycket med hjälp av att det ägs av bankerna och bankerna har gjort det obligatoriskt för att kunna använda onlinebanken.

Idag används ofta den fysiska legitimationen i affären, på postutlämningen, på krogen och många fler platser. På krogen måste en person alltid kunna styrka sin identitet med hjälp av en giltig legitimation. Giltiga legitimationer i Sverige är körkort, pass, nationellt id-kort, SIS-märkt id-kort och identitetskort för folkbokförda i Sverige. Detta innebär att den legitimation som de flesta i Sverige har (Bank-ID) är inte giltig i affären, på postutlämningen eller på krogen. Detta är något som en digital legitimation skulle hjälpa med då svensken ofta har telefonen med sig.

Om en person är ute och kör bil och blir stoppad av polisen, då måste personen ha körkortet med sig för att kunna styrka sin identitet och att de har körkort för fordonet de

kör. Ifall personen inte har körkortet med sig kan polisen utfärda en böter och därmed även lägga in personen i brottsregistret. Allt detta bara för att personen inte har sitt körkort med sig. Detta är också något som en digital legitimation kan hjälpa till med då svensken oftast har telefonen med sig.

Idag har många sina betalkort på telefonen och betalar mycket med telefonen (Sveriges Riksbank, 2022). Många personer använder även hellre betalkortet än kontanter, då endast 34% av svenska folket hade använt kontanter under den senaste månaden (från intervjuns datum) och endast 8% hade använt kontanter för deras senaste köp. Jämförelsen mellan betalkort fysiskt och digitalt på mobiltelefonen slutade i att en av fyra personer i Sverige betalar med hjälp av telefonen medan ungefär tre av fyra personer har tillgång till swish (Sveriges Riksbank, 2022). Swish är en betallösning för att skicka pengar smidigt via mobiltelefonen till andra personer eller företag. Swish används istället för banköverföring då banköverföringar tar lång tid medan swish är direkt. Swish går även att implementera i butiker och det är väldigt smidigt att handla i butik med swish.

2.8. EUs digitala identitetsplånbok

För att digitala legitimationer ska vara så effektiva som möjligt måste flera olika aspekter kontrolleras, en av dessa kan vara hur snabbt en person kan legitimera sig när de visar upp legitimationen för legitimationskontrollanten (polis, ordningsvakt, passkontrollant, gränsvakt, kassapersonal, och många fler). Däremot måste denna uppsats begränsas där och denna aspekt kan tyvärr inte kontrolleras då detta tar för mycket tid då ett helt system hade behövt utvecklas. Istället kommer uppsatsen innehålla intervjuer med legitimationskontrollanter som frågar vilka aspekter som är viktigast.

Sverige behöver ha ett statligt e-id då alla de vi har idag är ägda av privata företag och det finns flera som inte vill använda e-id för att det inte ägs av staten (Internetstiftelsen, 2023. Sveriges Riksbank, 2022). Regeringen har gett detta uppdrag till myndigheten för digital förvaltning (DIGG) och de har publicerat en slutredovisning för detta uppdrag och i den skriver DIGG om hur sverige ligger bakom de flesta andra EU-länder då sverige inte har en statlig e-legitimation på den högsta tillitsnivån. Dessa tillitsnivåer finns i 4 olika stadier där det bestäms hur pålitligt ett system för e-legitimationer är. Ett system på nivå ett skulle vara ett system med användarnamn och lösenord som användaren skapat själv, ett system på nivå två hade varit ett system med användarnamn, lösenord och en form av tvåstegsverifiering. Ett system på nivå tre hade varit ett system vars konto skapande kräver ett fysiskt möte där användaren styrker sin identitet genom en fysisk legitimation. Ett system på nivå fyra hade varit ett system som vid skapandet av användarkontot kräver ett fysiskt möte och legitimering med en godkänd svensk legitimation, däremot kräver de även tvåstegsverifiering och dessutom förnyelse var 5e år med en giltig svensk id-handling.

Alla EU-länder har fått ett krav på sig att utveckla en statlig e-legitimation för att EU ska kunna införa en digital identitetsplånbok. Med detta menar EU att nationella

id-handlingar, (pass och nationellt id-kort) läkarintyg, yrkeskvalifikationer, betyg från skolan och mycket mer ska kunna vara digitala (Myndigheten för digital förvaltning, 2023. Europeiska kommissionen, 2021). Detta är en av anledningarna till att denna uppsats skrivs, dessa aspekter (effektivitet, tillgänglighet och säkerhet) behöver undersökas då det är väldigt känslig information som verkligen inte får läcka ut utanför korrekta system, informationen måste vara tillgänglig för alla då det är information som alla måste kunna komma åt och metoden att komma åt informationen måste vara effektiv då poängen med digitalisering är att effektivisera arbete.

Det finns många olika sätt att publicera denna identitesplånbok, ett av dessa sätt är en separat applikation som har olika legitimationer i sig och kan användas av alla i EU. En separat applikation är det som Raj et al. (2016) har skrivit om i deras rapport. En applikation som endast har ett körkort och inget annat. En annan metod kan vara såsom Swedbank har implementerat deras digitala "blipp" funktion. Att blippa innebär att en mobiltelefon har ett NFC-chip (Near Field Communication) vilket interagerar med kortläsarens NFC-läsare som skickar över kortinformationen och betalar i systemet. Swedbank har implementerat detta genom att användaren som har ett konto hos Swedbank och har ett betalkort utgivet av "Swedbank och Sparbanken". Då kan en användare lägga in kortuppgifterna i Apple eller Google pay (m.fl) vilket sedan kräver en verifieringskod från Swedbanks applikation. Efter att denna verifieringskod är inskriven i Apple eller Google pay (m.fl) kommer Apple eller Google pay (m.fl) lägga in kortet i en sorts digital plånbok som användaren sedan kan använda för att "blippa" i en butik.

3. Problemområde

Inom den svenska digitaliseringen är det viktigt att hålla sig till flera olika faktorer när en organisation håller på att digitalisera, spelar ingen roll ifall det är en myndighet eller ej. Dessa faktorer kan vara exempelvis: effektivitet, användbarhet och säkerhet (Febiri & Hub, 2021). Under effektiviteten skriver de om hur det är viktigt med stabil hårdvara, effektiviteten som ett specifikt system och dynamisk effektivitet. Stabil hårdvara är väldigt viktigt för att systemet aldrig ska gå offline. Effektiviteten som ett specifikt system kan vara exempelvis ett digitalt system för att deklarera skatt, i ett sådant system kan målen vara till exempel; lägre mängd skattefusk, högre grad av skatte-insamling eller lägre grad av penningtvätt. Den sista faktorn, dynamisk effektivitet handlar om hur man framtidssäkrar ett system genom att exempelvis inte binder upp sig till ett system och använder det väldigt länge. Händer detta riskeras det att systemet fastnar i gamla standarder och utvecklas väldigt sakta. (Febiri & Hub, 2021)

Användbarhet är ett väldefinierat begrepp inom människa-datorinteraktioner (MDI) undersökning, vilket menar hur bra användaren kan "kommunicera" med applikationen genom ett gränssnitt. De definierar användbarhet som hur bra e-tjänsten kan bli förstådd, lärd, hanterad och hur bra den ser ut för användarna. (Febiri & Hub, 2021)

Säkerheten för specifikt statlig data är extremt viktig med tanke på att ifall en dataläcka skulle ske skulle extremt känslig information kunna komma ut i fel händer (Febiri & Hub, 2021). Informationssäkerhet är fortfarande extremt viktigt när det kommer till informationssystem inom privata organisationer också, däremot sparar de oftast inte lika känslig data. Finlands släppte sin första cybersäkerhetsstrategi i januari 2013, strategin formades av försvars- och säkerhets-komiteen som en förebyggande strategi ifall de någon gång skulle utsättas för dataintrång eller liknande (Febiri & Hub, 2021). Människor litar på staten och deras strategier för att skydda människors data. Ifall ett dataintrång eller en dataläcka skulle ske skulle denna tillit försämras något extremt då läckt eller stulen data kan hota landets stabilitet och säkerhet. Ökade säkerhetsstandarder och ökade hot ökar behovet av en säkerhetsplan ifall det skulle hända något. Det finns flera faktorer som ökar säkerheten på dessa system och dessa kan vara till exempel, biometrisk inloggning, tvåfaktors autentisering, kryptering och ett säkert ID-system. (Febiri & Hub, 2021)

Svenskarna använder Bank-ID väldigt mycket, 92% av befolkningen 18 år eller äldre använder Bank-ID (Internetstiftelsen, 2023). Ungefär 69% av svenskar använder Bank-ID varje dag, Bank-ID används i störst utsträckning av de som är födda på 60-talet eller senare, där minst 71% av svenskarna använder Bank-ID varje dag. Internetstiftelsen (2023) skriver i sin rapport att flera äldre inte känner att Bank-ID är säkert nog och att "…Om staten hade ägt det hade det varit en annan sak…". De skriver även att många som inte använder Bank-ID har en okunskap om tekniken där många inte vet hur man gör eller att deras mobiltelefoner är för gamla för att installera appen Bank-ID. (Internetstiftelsen, 2023)

Enligt en studie gjord i Indonesien 2023 svarar 52% av respondenterna att de har använt digitala id-handlingar medan 48% av respondenterna svarar att de inte har använt digitala id-handlingar (Zahlimar et al., 2023). De 48% svarar att det finns problem med att tjänsten endast är tillgänglig på android-plattformen och inte på IOS-plattformen. Detta är något som begränsar tillgången till systemet då många använder IOS-plattformen. Med detta missar utvecklare många chanser att öka tillgängligheten och förlorar därmed många användare. Digitala id-handlingar har underlättat för många yngre medborgare då de ofta vill göra saker online istället för att gå till exempelvis ett passkontor eller göra pappersarbete för att skaffa ett bankkonto (Zahlimar et al., 2023). Digitala id-handlingar underlättar för den yngre generationen då de lätt kan ta fram ett digitalt id-kort istället för att ha med sig den fysiska legitimationen hela tiden. Svenskarna har ofta med sig sin mobiltelefon och plånbok, ifall digitala id-handlingar hade varit mer populärt hade svenskarna kunnat lämna plånboken hemma då svensken oftast inte betalar med kontanter (Sveriges Riksbank, 2022). Fysiska legitimationer kan lätt gå sönder eller tappas bort, och att ersätta dessa tar ofta lång tid och kräver att individen går till polisens reception och får ett nytt id-kort. Med digitala id-handlingar blir denna process mycket smidigare då en person aldrig behöver ersätta ett trasigt eller borttappat digitalt id-kort då det inte går att tappa bort en webbplats eller applikation. Det går alltid att tappa bort en mobiltelefon, däremot är mobiltelefonen lättare att ersätta än en legitimation då det bara är att gå in i närmsta elektronikbutik och köpa en ny. Den yngre generationen är generellt positiv kring digitala id-handlingar, däremot finns det många som väcker oro när det kommer till informationssäkerhet och tillgänglighet. (Zahlimar et al., 2023)

För att kunna analysera detta på bästa sätt inkluderar denna rapport inte bara de yngre generationer utan rapporten inkluderar även medelålders och äldre generationer för att kunna få en helhetsbild över hur situationen kring digitala id-handlingar ser ut. Dagens digitala utanförskap för den äldre generationen, dagens mobilanvändning bland den yngre generationen samt avsaknaden av en statlig e-legitimation är varför denna rapport behövs.

Det finns en trend inom olika digitaliseringsprojekt speciellt inom den offentliga sektorn, de flesta projekten blir helt enkelt en digital kopia på det som redan finns fysiskt vilket kan leda till att personer bara använder det som redan fungerar. Projekten blir endast digitala och har väldigt få eller inga vidareutvecklingar på det som redan finns. (Holgersson et al., 2017)

3.1. Problem/fråga

Svenskarna blir mer och mer digitaliserade för varje dag som går och därför använder svenskarna knappt kontanter längre, och istället använder svenskarna ett betalkort (fysiskt eller på mobiltelefonen) i hög utsträckning. Svenskarna använder däremot inte en digital id-handling då det inte finns en svensk statlig digital id-handling. Med avsaknaden av en statlig digital id-handling och den konstant ökande mobiltelefonanvändningen i åtanke formulerades forskningsfrågan enligt följande: *Vilka*

aspekter av ett system för digitala id-handlingar är viktiga för systemets effektivitet, tillgänglighet och säkerhet?

3.2. Avgränsningar

Inom denna studie kommer inte en utveckling av ett system att genomföras då studien inte kan omfatta utveckling av ett system då detta är något som måste göras av proffs och dessutom finns det inte tid inom ramen för examensarbetet.

4. Metod

När en forskare ska genomföra ett forskningsprojekt behöver forskaren välja hur den vill göra. Det finns två olika metodansatser, kvalitativa och den kvantitativa metodansatsen (härefter kallat kvalitativa och kvantitativa) (Berndtsson et al., 2008). Inom den kvantitativa skapar forskaren en hypotes och försöker därefter falsifiera den hypotesen genom undersökningar. Därefter sägs det att hypotesen är korrekt tills någon bevisar motsatsen (Berndtsson et al., 2008). Den andra, den kvalitativa, är istället en typ av forskning som istället för att direkt svara på frågan utökar vår förståelse för forskningsområdet. Den kvalitativa forskningen är ofta associerad med fältarbete och kan därför verka mer som ett arbete för ett företag än den kvantitativa forskningen. Människor förändras däremot hela tiden och därför kan den kvalitativa forskningen vara svårare än den kvantitativa att repetera (Berndtsson et al., 2008). Denna studien kommer att genomföras med kvalitativ forskning och kommer därmed inte direkt besvara frågan utan kommer istället utöka förståelsen för ämnet digitala id-handlingar. Denna studien är genomförd med den kvalitativa för att studien baseras på vetenskapliga artiklar, statliga myndigheters rapporter och intervjuer då detta är den typen av data som går att samla in smidigt utan att utveckla en hel applikation och sedan testa den på individer för att kunna genomföra en kvantitativ forskning.

4.1. Intervjuer

Intervjuer kan genomföras på flera olika sätt, Berndtsson et al. (2008) skriver om två av dem i deras bok. Där skriver de om öppna och stängda intervjuer och hur de metoderna fungerar. Öppna intervjuer är vanliga i kvalitativ forskning där forskaren har lite eller ingen kontroll över vilka problem som kommer på tal under intervjun, däremot har forskaren koll på de övergripande målen med intervjun (Berndtsson et al., 2008). Under öppna intervjuer är det viktigt att frågorna som forskaren har inte leder till enkla ja/nej svar utan de leder till en diskussion kring ämnet istället. Stängda intervjuer är en annan form av intervju där forskaren har frågor nedskrivna sedan innan intervjun som kan leda till kortare diskussioner eller enkla ja/nej svar. Den stängda intervjun kan dock ha frågor som respondenten tycker är helt irrelevanta och kan därför leda till väldigt tråkiga svar på frågorna.

I denna studien genomförs en öppen intervju med olika legitimationskontrollanter (polis, ordningsvakt, butikspersonal mm.). Detta för att få en djupgående förståelse för hur deras arbete går till och hur ett system för digitala id-handlingar kan hjälpa dem i deras arbete istället för att göra deras arbete svårare. Dessa intervjuer kommer sedan att anonymiseras helt och det enda som kommer att identifiera personerna som blivit intervjuade är ett fiktivt namn.

En undersökning är något som ofta genomförs ifall ett problem är välkänt och det finns många respondenter som har en övergripande bild på problemet. Däremot går det inte att analysera komplicerade problem då det inte finns någon tvåvägskommunikation. Ett annat problem med undersökningar är att det ofta kan vara stora problem med att få in

tillräckligt med respondenter till undersökningen då många inte har tid eller orkar inte svara på en undersökning. (Berndtsson et al., 2008)

En undersökning genomförs med respondenter som inte har en specifik inblick i problemet. Detta för att få en övergripande blick på hur personer vill ha sin legitimation för att underlätta i deras vardag. Intervjun kommer att helt anonymiseras och ett fiktivt namn kommer att användas i rapporten för att kunna identifiera personen. Det fiktiva namnet kommer inte heller att representera könet eller åldern på personen då vilket namn som helst kan väljas.

4.2. Litteraturstudie

Med litteraturstudier menas en systematisk genomgång av ett problem, med det menas en genomgång av olika vetenskapliga artiklar som publicerats i olika journaler och konferenser (Berndtsson et al., 2008). En litteraturstudie är också något som kommer att genomföras i denna rapport, detta för att kunna få en helhetsbild på hur liknande system har fungerat tidigare och hur olika aspekter av tillgänglighet, effektivitet och säkerhet som är viktiga och hur de aspekterna tidigare har mätts upp.

4.3. Vetenskapliga / forskningsetiska aspekter

Det finns 4 olika krav som måste behandlas när en forskare genomför en datainsamling med andra parter än forskaren själv (Vetenskapsrådet, 2002). Dessa delas däremot upp i 8 olika regler. Det första kravet är informationskravet, som innebär att den andra parten måste vara informerad om hur intervjun / studien kommer att genomföras, den andra parten måste vara informerad om vilka villkor som gäller för partens deltagande, exempelvis att intervjun / studien är helt frivillig och parten kan dra sig ut när den vill. Informationen som den andra parten får kan vara mer eller mindre omfattande, däremot måste informationen innehålla alla aspekter som kan förändra partens vilja att delta i intervjun / studien. (Vetenskapsrådet, 2002)

Den andra kravet (samtyckeskravet) innebär att den andra parten måste kunna själv bestämma över vilken information som behandlas, ifall parten är minderårig måste en vårdnadshavare godkänna intervjun / studien. Detta innebär att parten som intervjuas / deltar i studien måste lämna samtycke för att vara med i studien. (Vetenskapsrådet, 2002) I detta krav finns även regel 3 som innefattar hur en andra part alltid kan dra sig ur undersökningen när de vill och parten ska därmed inte få några som helst negativa följder för att parten dragit sig ur. Ifall en part skulle dra sig ur kan informationen som redan samlats in användas, däremot får ingen mer information samlas in. Däremot kan parten begära att all information som samlats in stryks helt ur undersökningen och då måste detta följas. Inom samtyckeskravet finns det ytterligare en regel, att parten inte får utsättas för påtryckning eller liknande för att försöka få tillbaka parten till undersökningen. (Vetenskapsrådet, 2002)

Därefter finns konfidentialitetskravet som innebär att alla personuppgifter måste hållas under sekretess och aldrig publiceras, detta innebär även att rapporten måste skrivas på

så sätt att ingen obehörig kan identifiera personen för att parten ska fortsätta vara anonym. (Vetenskapsrådet, 2002)

Det sista kravet handlar om att uppgifterna som samlats in från andra part ej får användas utanför studien och personuppgifter får ej användas för beslut eller åtgärder som direkt påverkar parten. Detta innebär att insamlade personuppgifter ej får användas av exempelvis myndigheter för att ta ett beslut om vård eller liknande. Vid planering måste dessa aspekter tas hänsyn till av projektledaren / forskaren för att minska risken för att något sådant händer. (Vetenskapsrådet, 2002)

Alla dessa krav är väldigt viktiga inom forskning för att forskningen ska genomföras på ett korrekt sätt, därför börjar intervjuerna med en genomgång av dessa rättigheter och en fråga ifall intervjun får spelas in.

4.4. Mål med rapporten

Målet med detta examensarbete är att samla in djupgående data kring vad personer som är mer insatta inom IT / IS system tycker kring digitala id-handlingar och EUs digitala identitetsplånbok. En kvalitativ metodansats samlar inte in information från många källor utan den kvalitativa metodansats samlar in djupgående information från ett färre antal källor. Detta är varför den kvalitativa metodansatsen fungerar bättre för denna studien än den kvantitativa metodansatsen, helt enkelt att det behövs mer djupgående information än den kvantitativa metodansatsen kan ge. Båda studierna (litteraturstudie och intervju) kommer att analyseras och dras slutsatser från i senare kapitel för att till slut få en bra idé om hur digitala id-handlingar påverkar människors privatliv / yrkesroll.

5. Materialpresentation

Intervjun genomfördes i två omgångar, en mot privatpersoner och en mot yrkesroller. De yrkesroller som här är inkluderade är: brevbärare och polis.

Intervjun är uppdelad i 5 kategorier;

- Användning av legitimation (introduktion)
    - För att säkerställa att personen faktiskt använder deras legitimation / kontrollerar legitimationer. Detta för att kunna säkerställa att personen faktiskt har erfarenhet och svaren på frågorna kan användas.
- Effektivitet
    - Denna kategori valdes då effektivitet är en väldigt bra aspekt att studera då ny teknik inte ska försämra det som redan finns utan ny teknik ska bara förbättra och lägga till funktioner. Det är väldigt lätt att ny teknik försvårar och hindrar personer istället för att förbättra.
- Tillgänglighet
    - Tillgänglighet är en väldigt viktig aspekt då många personer i samhället inte förstår sig på ny teknik eller inte kan hantera ny teknik, detta är varför denna aspekt valdes.
- Säkerhet
    - Världssituationen just nu är väldigt orolig och det finns hög sannolikhet att just ny teknik kan utvecklas på ett dåligt sätt och fel person kan få reda på ett “kryphål” eller en “bakdörr” och därför är säkerhet väldigt viktig. Däremot finns även en nackdel med säkerhet, ifall ett system är för säkert kommer effektivitet och tillgänglighet att minska rejält. Noggrant utvald säkerhetsnivå är varför denna aspekt valdes att studeras.
- EUs digitala identitetsplånbok
    - EUs digitala identitetsplånbok håller just nu på att utvecklas och därför behöver även denna vara med då den är aktuell till situationen för digitala id-handlingar.

Frågorna för de två olika intervjuerna är mindre modifierade för att bättre passa situationen, till exempel: Privatperson: "Hur tror du att digitala id-handlingar kan påverka ditt privata användande av id-handlingen?" Yrkesroll: "Hur tror du att digitala id-handlingar kan påverka ditt yrke / din yrkesroll?” Respondent nummer 2 är en intervju där respondenten intervjuades som både yrkesroll och privatperson, därför är denne respondenten uppdelad i 2.1 samt 2.2 när det är olika frågor och sammansatt när frågan är likadan. När respondenten svarat utifrån sin yrkesroll är detta markerat med “(yrkesroll)”, är det en respondent som svarat ut ett privat perspektiv är det markerat med “(privat)”.

5.1. Introduktion

Privatpersoner fråga 1.1: Hur ofta använder du din legitimation?

Yrkesroller fråga 1.2: Hur ofta kontrollerar du legitimationer i ditt arbete?

Respondent 1 (privat)	Jag använder min legitimation (Nationellt ID) ungefär en gång i veckan.
Respondent 2.1 (yrkesroll)	Jag kontrollerar legitimationer någon gång i månaden i mitt arbete. De legitimationer som jag ser mest är körkort och pass.
Respondent 2.2 (privat)	Jag använder min legitimation ungefär 1-3 gånger i veckan men Bank-ID är varje dag.
Respondent 3 (privat)	Jag använder min legitimation maximalt en gång i veckan
Respondent 4 (privat)	Jag använder min legitimation mellan en och tre gånger i veckan
Respondent 5 (yrkesroll)	Jag personligen kontrollerar nästan aldrig legitimationer idag, men när jag arbetade inom ingripandeverksamheten (IGV) var det flera gånger varje dag, detta för att säkerställa identiteten på personen vi pratar med. Inom IGV är det näst intill bara körkort som kontrolleras, däremot kan körkort vara både svenska och utländska vilket kan innebära problem.

Yrkesroller fråga 1.4: Har du stött på några utmaningar med att kontrollera fysiska legitimationer?

Respondent 2.1 (yrkesroll)	Inga större utmaningar så sett, flera som inte haft legitimationen på sig och behövt hämta den, eller någon som haft ett trasigt körkort och behövt legitimera sig på annat sätt
Respondent 5 (yrkesroll)	Körkort ser väldigt olika ut beroende på vilket land körkortet är utfärdat i, exempelvis är ett svenskt körkort det lättaste att kontrollera för oss medan vissa tyskar har en 40 år gammal papperslapp. Därför blir det väldigt svårt att veta ifall körkortet är förfalskat, polisen har experter men det blir endast ett ärende hos dem ifall den ingripande polisen har en misstanke.

Privatpersoner fråga 1.3 & yrkesroller fråga 1.5: Har du hört talas något om digitala id-handlingar?

Respondent 1 (privat)	Ja, jag har hört talas om BankID och Freja eID, däremot inget om exempelvis att ha körkort digitalt
Respondent 2 (yrkesroll)	Ja, BankID och freja eID men jag vet inte mycket om dem förutom att jag använder BankID varje dag.
Respondent 3 (privat)	Inte mycket alls
Respondent 4 (privat)	Inte jättemycket, endast om BankID och freja eID. Det jag vet är att de är applikationer som används för att säkerställa identiteten på personen som försöker genomföra ett ärende på en webbplats eller hos banken.
Respondent 5 (yrkesroll)	Jag har hört en del om exempelvis BankID men väldigt sparsamt om “fysiska gone digital”

Privatpersoner fråga 1.5 & yrkesroller fråga 1.7: Vad tror du om potentialen för digitala id-handlingar att ersätta fysiska legitimationer?

Respondent 1 (privat)	Fysiska kort går att förfalska ganska lätt, de metoder som används för att verifiera en fysisk legitimation är oftast visuella. Digitala kort går att verifiera med kryptologi, även när användaren är offline. Det går även att koppla en applikation med en internetuppkoppling för att kunna direkt i applikationen visa eventuella återkallningar eller andra viktiga saker.
Respondent 2 (yrkesroll)	Jag tror att digitala id-handlingar kommer att ersätta de fysiska legitimationerna inom en längre tidsperiod, däremot i nuläget tror jag det kommer att behövas en fysisk legitimation som "backup" ifall mobiltelefonen skulle ta slut på batteri eller internet skulle ligga nere.
Respondent 3 (privat)	Jag tror inte alls på digitala legitimationer då jag redan haft problem med bankkortet i mobiltelefonen.
Respondent 4 (privat)	Jag tror att digitala legitimationer kommer att helt ersätta de fysiska legitimationerna inom en längre tidsperiod. Däremot tror jag att digitala legitimationer kommer att slå igenom inom ca 10-20 år. Med slå igenom menar jag att de flesta använder den digitala legitimationen och det är mer och mer sällan man ser de fysiska legitimationerna.
Respondent 5 (yrkesroll)	Jag ser väldigt många både fördelar och nackdelar med digitala legitimationer. Det finns alltid en risk med att ha något digitalt, exempelvis hackning. Det digitala är alltid väldigt sårbart ifall ett krig eller en större kris skulle utbrista. Till exempel ifall det blir strömavbrott förlorar alla sina legitimationer förr eller senare järfört med de fysiska körkorten vi har idag som inte kan försvinna tillsammans med strömmen. Jag ser däremot många bra saker med det också, exempelvis att allt är samlat på samma ställe. Och ur en polisiär synvinkel måste jag säga att de digitala legitimationerna hade underlättat då det alltid går att tvinga till sig en inloggning genom olika polisiära metoder.

5.2. Effektivitet

Fråga 2.1: Vilka aspekter av ett system för digitala id-handlingar tror du är viktiga för att det ska vara effektivt?

Respondent 1 (privat)	Jag anser att det måste vara "lätt att få tag på", med det menar jag att legitimationen får inte ta längre tid att ta fram än det tar med de nuvarande fysiska legitimationerna
Respondent 2 (yrkesroll)	I min yrkesroll skulle jag säga att det behöver finnas något verktyg för att kunna verifiera de digitala legitimationerna, exempelvis i våra handdatorer. I privata tankar tänker jag på systemets säkerhet, det får inte vara för säkert så att legitimationen tar extremt lång tid att ta fram men samtidigt måste systemet vara så pass säkert att något dataintrång inte kan ske.
Respondent 3 (privat)	Jag är för osäker på detta för att kunna svara
Respondent 4 (privat)	Det måste gå snabbt att ta fram legitimationen, det får inte ta längre tid eller vara mycket krångligare än den nuvarande fysiska legitimationen.
Respondent 5 (yrkesroll)	Lätthanterligt, alla måste kunna hantera det utan större problem, men samtidigt krävs det att alla har tillräckligt modern utrustning. Systemet måste också vara tillräckligt säkert, ifall en väskryckning skulle ske är det en person som blir av med deras legitimation medan ifall ett dataintrång sker blir alla av med sina legitimationer.

Fråga 2.2: Hur tror du att digitala id-handlingar kan underlätta för dig i din vardag / ditt arbete?

Respondent 1 (privat)	Idag har alla med sig sin mobiltelefon i princip överallt, och man slipper ha med sig plånboken så länge som man inte har med sig kontanter. Den digitala legitimationen är det sista steget för att slippa ta med sig plånboken helt.
Respondent 2.1 (yrkesroll)	Jag tror att det som mest hade underlättat i mitt arbete är egentligen något sätt att verifiera legitimationer.
Respondent 2.2 (privat)	Exempelvis hade det underlättat genom att man slipper ha med sig plånboken när man ska iväg, däremot tror jag i alla fall till en början att man måste fortfarande ha en fysisk legitimation med sig ifall mobiltelefonen skulle ta slut på batteri
Respondent 3 (privat)	Jag tror det hade kunnat användas som en backup ifall man glömmer legitimationen hemma istället för en ersättare till fysiska legitimationer
Respondent 4 (privat)	Jag tror det underlättar genom att jag slipper ha med mig plånboken när jag är ute, jag tror absolut att man kommer kunna lämna plånboken hemma så länge som man håller mobiltelefonen laddad och inte behöver handla men kontanter.
Respondent 5 (yrkesroll)	Så länge tekniken fungerar så tror jag att det kommer fungera bra, däremot ifall mobiltelefonen skulle ha slut på batteri eller mobilnätet skulle ligga nere eller någon annan typ av händelse. Ifall detta skulle hända skulle det vara väldigt bra ifall polisen hade haft någon form av enhet som skulle kunna verifiera en persons identitet baserat på fingeravtryck eller liknande istället.

Fråga 2.3: Vilka typer av funktioner eller tjänster tror du är nödvändiga för att ett system för digitala id-handlingar ska vara effektivt?

Respondent 1 (privat)	Det måste kunna fungera offline, det är fördelaktigt att ha någon form av internetuppkoppling för att kunna bekräfta att körkortet inte är återkallat eller liknande men det är inte ett måste då detta går att arbeta runt redan idag. De digitala id-handlingarna måste kunna fungera även offline då det finns personer som inte har en internetuppkoppling.
Respondent 2 (yrkesroll)	Precis som jag sagt tidigare, något sätt att verifiera legitimationer hade underlättat väldigt mycket.
Respondent 3 (privat)	Det måste vara lättillgängligt, bankkortet i telefonen idag är en ganska smidig lösning och det hade varit väldigt bra ifall det går göra någon liknande lösning
Respondent 4 (privat)	Det hade varit bra ifall mobiltelefonen hade haft någon funktion så att legitimationen även fungerar offline då en användare inte alltid har uppkoppling med internet. Exempelvis kanske applikationen har någon form av krypteringsnyckel som kan verifieras med en server när mobiltelefonen väl har internetuppkoppling.
Respondent 5 (yrkesroll)	För att det ska vara effektivt måste det vara säkert. I dagsläget har polisen endast tillgång till sveriges databaser på vilka som har körkort och inte, ett system för digitala id-handlingar hade kunnat göra så den svenska polisen hade kunnat kontrollera körkort och id-handlingar från alla länder inom europa istället för endast inom sverige.

5.3. Tillgänglighet

Fråga 3.1: Vilka utmaningar ser du med att implementera och använda ett system för digitala id-handlingar för alla medborgare?

På denna fråga svarade alla respondenter nästan samma sak. Alla respondenter tror att äldre och funktionshindrade kommer att ha problem med en tjänst för digitala id-handlingar. Respondent 1 & 5 la utöver det tidigare nämnda till ett problem med mobiluppkopplingen som är väldigt dålig på många platser långt ut på landet.

Personer blir påtvingade en digital lösning när de kanske inte vill ha en digital id-handling, därför är det väldigt bra om de fysiska legitimationerna fortfarande finns att få tag i ifall en person skulle ha väldigt svårt med att hantera mobiltelefonen eller absolut inte kan av någon anledning. Allt kommer att kosta för både staten och privatpersoner men frågan är hur mycket det får kosta innan det blir för mycket. Även trots den yngre och medelålders generationen har relativt lätt för att anpassa sig till en ny lösning kanske inte de äldre eller funktionshindrade hade haft samma möjlighet att lätt anpassa sig till en digital lösning för id-handlingar. Olika personer har olika krav och kunskap, därför är det extremt svårt att utveckla en lösning som fungerar och passar för alla.

Fråga 3.2 och 3.3: Hur tror du att man kan säkerställa att alla medborgare, oavsett ålder, digitala färdigheter eller socioekonomisk bakgrund, har tillgång till och kan använda digitala id-handlingar?

Frågorna 3.2 och 3.3 är väldigt liknande svar på, därför är dessa grupperade i samma presentation.

Respondent 1 (privat)	Det måste fungera offline, på en väldigt stor variation av enheter, särskilt billiga enheter då många personer inte har råd att köpa det nyaste och det dyraste. Det kan komma att krävas utbildningar för hur man använder en digital id-handling och då kommer det att kosta, antingen för svenska staten eller för personen direkt.
Respondent 2 (yrkesroll)	Försöka underlätta för personer exempelvis genom en enhet som används endast för att uppvisa legitimationen, den enheten måste däremot alltid fungera oavsett mobiltäckning eller inte. Oavsett om personen har en smarttelefon eller inte måste legitimationsenheten fungera. Enheten måste också vara så pass enkel att den går använda för alla, inte bara gemene man.
Respondent 3 (privat)	Jag tror att det kommer att krävas utbildningar som visar speciellt utsatta grupper hur man ska använda den digitala id-handlingen, däremot tror jag att kostnaden för denna typen av utbildning kan vara ganska hög. Alla olika personer har olika krav på hur ett system behöver vara utformat, därför tror jag att det behövs olika utbildningar för olika personer och därmed behöver en sådan utbildning vara på plats för att alla ska förstå ordentligt.
Respondent 4 (privat)	Jag tror flertalet äldre och funktionshindrade hade haft större problem än gemene man med ett system för digitala id-handlingar, detta för att redan idag ser vi stora problem för många äldre som inte kan hantera mobiltelefonen eller en dator. Många hade förmodligen behövt ha en god man eller någon annan som kan hjälpa dem. Jag tror även att utbildningar är en väldigt bra satsning ifall utbildningarna utformas på en bra sätt, detta kan däremot bli väldigt dyrt för svenska staten eller personen själv.
Respondent 5 (yrkesroll)	Olika grupper har olika behov, man måste kunna hitta rätt metod för rätt målgrupp. I många kommuner har man arbetat med ungdomsgrupper som hjälper till att utbilda exempelvis äldre om hur man använder en mobiltelefon. Detta kanske hade varit en bra lösning då både äldre får veta från en ungdom hur man använder systemet och den yngre generationen får komma ut och träffa de äldre och skapa ett kontaktnätverk.

5.4. Säkerhet

Fråga 4.1: Vilka aspekter av ett system för digitala id-handlingar tror du är viktiga för att det ska vara säkert?

Respondent 1 (privat)	Jag tror att kryptografi är en viktig sak som skulle kunna integreras i systemet, användarens enhet genererar en nyckel som utgivaren ska signera. På så sätt blir det säkert med många olika modeller på smarttelefoner.
Respondent 2 (yrkesroll)	Att ha någon form av enhet som automatiskt kan kontrollera en legitimation genom att scanna exempelvis en qr-kod. Men inte bara det utan även ha bakgrundskontroller på alla som ska använda denna enhet och det ska vara svårt att skicka en verifieringsförfrågan, exempelvis att endast företag som är godkända ska kunna använda verifieringssystemet.
Respondent 3 (privat)	Jag är för osäker på detta för att kunna svara
Respondent 4 (privat)	Jag tror en krypteringsnyckel på användarens enhet men också en verifieringsnyckel på en server någonstans (molnet) som ska användas för att verifiera den lokalt sparade nyckeln.
Respondent 5 (yrkesroll)	Den som ansvarar för systemet måste “täppa till hålen” i systemet för att kunna minimera risken för att användare blir identitetskapade. Risken för identitetsstöld finns alltid och går inte minimera till 0 men risken måste vara minimal. I dagsläget är mycket fokus på “snabbt och enkelt” medan i framtiden måste fokus läggas mer på “tryggt och säkert”

Fråga 4.2: Vilka typer av säkerhetsrisker ser du med användningen av digitala id-handlingar?

Respondent 1 (privat)	Jag ser en stor risk med exempelvis dataintrång. Om fel person får tag i de nycklarna som signerar identiteter kan dessa användas för att förfalska nya identiteter. Därmed kan de härma en riktig identitet eller helt enkelt skapa en ny.
Respondent 2 (yrkesroll)	Finns alla möjliga risker med digitala id-handlingar, exempelvis bedrägerier, dataintrång eller datastölder. Information hamnar i fel händer eller att data säljs vidare.
Respondent 3 (privat)	Om man tar och jämför det med att ha bankkortet i telefonen så har jag hört att det är säkrare att ha bankkortet i telefonen än att ha det i plånboken.
Respondent 4 (privat)	Hackning, id-kapning, datastöld, egentligen alla traditionella metoder för att hacka en server går alltid att använda mot en ny server.
Respondent 5 (yrkesroll)	Det finns väldigt många säkerhetsrisker skulle jag säga, alla traditionella metoder fungerar fortfarande så där måste arbete göras för att minimera risken att en obehörig person tar sig in i dessa system.

Fråga 4.3: Hur tror du att man kan hantera dessa säkerhetsrisker och skydda användarnas integritet och data?

Respondent 1 (privat)	Jag tror att man måste spara så lite information som möjligt och aktivt förebygga attacker.
Respondent 2 (yrkesroll)	Någon typ av verifiering för att kunna kontrollera legitimationer, och bakgrundskontroller på personer och företag som skickar förfrågningar. Försöka ha någon form av dataspårning ifall datan skulle läcka ut.
Respondent 3 (privat)	Jag är för osäker på detta för att kunna svara
Respondent 4 (privat)	Jag tror att genom en krypteringsnyckel på den lokala enheten och en verifieringsnyckel på en server skulle vara tillräckligt säkert för att en obehörig inte skulle kunna ta sig in i systemet och skapa nya identiteter. Detta är däremot inte tillräckligt då en obehörig person kanske kan ta sig in i servern och skapa en ny identitet och så pass kunna bli en ny person. Detta måste systemet också skydda mot
Respondent 5 (yrkesroll)	Jag tror att mycket teknik i nuläget baseras på att allt ska vara så snabbt och enkelt som möjligt, jag tror däremot att i framtiden måste vi fokusera mer på tryggt och säkert istället för snabbt och enkelt.

Fråga 4.4: Vad tycker du om användningen av biometrisk autentisering i system för digitala id-handlingar?

Respondent 1 (privat)	Biometrisk autentisering på en mobiltelefon är ganska bra, eftersom att det är en “sluten enhet”. Om man startar om telefonen så måste användaren skriva in lösenordet för att biometrik ska gå att använda igen. Många telefoner har även den funktionen att efter X många timmar eller efter X många försök så måste användaren skriva in sin PIN-kod för att kunna låsa upp telefonen och biometriken igen.
Respondent 2 (yrkesroll)	Ganska bra, går väldigt snabbt och smidigt. Jag upplever inte att det händer ofta att den biometriska autentiseringen blir fel så jag upplever det som relativt säkert. Om man har både kod och någon form av biometrik så bör det vara tillräckligt säkert, men då kommer exakt samma problem som tidigare med personer som inte klarar av det.
Respondent 3 (privat)	Jag känner mig trygg i det vi har idag, jag tycker det känns säkrare än fysiska metoder.
Respondent 4 (privat)	Jag känner att en biometrisk autentisering är en väldigt bra metod för autentisering, i alla fall om det skapas på ett bra sätt. Ett sämre sätt är som många android telefoner har skapat ansiktsigenkänning, den går lura med en enkel bild av en person. Apple däremot har skapat en metod som sparar en 3d modell av en persons ansikte lokalt på telefonen och därmed behöver en hel 3d modell av en persons ansikte skrivas ut för att lura den telefonen.
Respondent 5 (yrkesroll)	Biometrisk autentisering är relativt bra, det har sina för och nackdelar. Exempelvis kan polisen tvinga en person att lägga sitt finger på fingeravtrycksläsaren men samtidigt kan en gärningsperson göra exakt samma sak. Men ifall man har någon variant av tvåstegsverifiering så tappar man lite det lättillgängliga med hela systemet.

5.5. EUs digitala identitetsplånbok

Fråga 5.1: Har du hört talas om EUs digitala identitetsplånbok?

På denna fråga var alla svar exakt samma sak, “Nej”. Det var ingen av respondenterna som hade hört talas om EUs digitala identitetsplånbok. Därmed presenterades denna lösning lite kort inom intervjun och därefter ställdes nästkommande fråga.

Fråga 5.3: Vad tror du om potentialen för EUs digitala identitetsplånbok att förenkla användningen av digitala id-handlingar i Europa?

Respondent 1 (privat)	Jag tror det finns väldigt stor potential med ett sådant system, men bara ifall det skapas på korrekt sätt. Exempelvis att det går att använda offline.
Respondent 2 (yrkesroll)	För resande personer tror jag det hade varit aktuellt, men för personer som bara stannar i samma land hade det inte varit lika viktigt att samla ihop hela EU. Som jag tidigare nämnt hade det förmodligen fortfarande behövts någon form av fysisk legitimation som kan användas istället för telefonen ifall mobiltelefonen tar slut på batteri eller man glömmer den hemma.
Respondent 3 (privat)	Jag tror egentligen att det bara kan användas som backup för en persons pass då de är ute och reser.
Respondent 4 (privat)	Jag tror absolut att den kan slå igenom på marknaden. Däremot tror jag inte den kommer helt ersätta pass körkort m.m. på ett antal år då vi fortfarande har den äldre generationen där många har väldigt svårt med ny teknik.
Respondent 5 (yrkesroll)	Om man går mot att det ska ersätta fysiska id-handlingar så måste ett gemensamt system för id-handlingar (i alla fall inom europa) finnas. Egentligen måste alla jordens länder finnas i det systemet men det vet jag inte hur man ska få med alla länder i detta systemet, speciellt med tanke på situationen i världen just nu samt att flertalet länder agerar helt emot våra svenska principer. Men ifall vi endast pratar om inom EU så hade det varit väldigt bra med ett system som enar hela europas pass, körkort och andra id-handlingar.

5.6. Avslutning

Fråga 6.1: Finns det något annat du vill lyfta fram om digitala id-handlingar?

Respondent 1 (privat)	De behöver bli mindre förlitliga på internet för att fungera.
Respondent 2 (yrkesroll)	Jag tror egentligen bara det är säkerheten som påverkar systemet väldigt mycket, ju fler som vill använda systemet desto högre säkerhet i systemet måste finnas.
Respondent 3 (privat)	Nej
Respondent 4 (privat)	Nej
Respondent 5 (yrkesroll)	Med tanke på hur Bank-ID utnyttjas redan idag, det är en av kriminella nätverks största inkomstkällor. Med det i åtanke blir jag lite orolig vad detta systemet skulle kunna användas till, men jag tror att ifall de som utvecklar systemet får tillräckligt med information och utbildning inom säkerhet så ska de lyckas göra systemet relativt säkert.

6. Analys

Nuvarande användning av Bank-ID och andra e-id tjänster

I dagsläget använder många den digitala lösningen för signaturer "Bank-ID" för signaturer på exempelvis bostadskontrakt, köp på internet eller inloggning för många internettjänster. Bank-ID är en väldigt enkel och snabb lösning att använda. Bank-ID fungerar väldigt smidigt med det som används idag, däremot går det inte att legitimera sig i butiken eller vid postutlämningen. Detta kan bero på flera olika anledningar, antingen att det är privatägt och att personer inte litar på det, eller att personer inte ännu är redo för att legitimera sig med hjälp av telefonen eller att Bank-ID inte är på en tillräckligt hög säkerhetsklass, eller någon helt annan anledning. Fyra av fem personer i intervjuerna tror att digitala id-handlingar skulle kunna vara en smidig lösning, däremot är det endast två av fem som tror att digitala id-handlingar skulle kunna ersätta de fysiska legitimationerna.

Sverige behöver ha en statlig e-legitimation för att i dagsläget litar vi på endast en privat aktör som delar ut e-legitimationer (Myndigheten för digital förvaltning, 2023). Ifall denna aktör skulle bli angripen av cyberkriminella kommer Sverige få väldigt stora problem och därför måste för det första, alla myndigheter acceptera flera olika digitala legitimationer, och för det andra måste Sverige ha en statlig e-legitimation på säkerhetsklass 4. Utöver säkerhetsklass måste även systemet ha stora krav på uppdatering för olika säkerhetsåtgärder som kan komma och bli aktuella inom en snar framtid. (Myndigheten för digital förvaltning, 2023)

En aspekt som går att följa väldigt lätt är hur villig en person är att acceptera ny teknologi, detta märks inte bara i intervjuerna utan även i litteraturen. Zahlimar et al., (2023) skriver att generation Z är väldigt teknikvana och därför mer villiga att acceptera ny teknologi. Detta märks tydligt i intervjuerna då de flesta var yngre och hade lättare att acceptera ny teknologi och var därför inte lika oroliga för vad som kan hända när allt blir digitalt.

Effektivitet

Effektiviteten beror på många olika aspekter, bland annat de aspekter som diskuteras här nedan, men även aspekter såsom kostnad, eller hur fort det går att ta fram legitimationen. Det finns två respondenter som uppmärksammar hur snabbt det går att verifiera legitimationen i fråga och där även upplyser om hur mänskliga fel kan minimeras. Någon metod för att kontrollera personens identitet utan att personen har legitimation med sig uppmärksammas av två respondenter. I fyra intervjuer nämns det att legitimationen skulle kunna vara sista steget till att helt kunna lämna plånboken hemma då det är det enda som inte redan finns digitalt. Denna rapports definition av effektivitet innefattar däremot inte tillgänglighet eller säkerhet, det diskuteras i respektive kapitel, däremot innefattar definitionen hur snabbt det går att ta fram,

kontrollera, minimera mänskliga fel och hur det kan underlätta för personer i deras privatliv och / eller yrkesroll.

Digg uppskattar ett e-id systems kostnad för utveckling och uppbyggnad till 80-100 miljoner kronor och de årliga underhållskostnaderna till ungefär 70 miljoner (Myndigheten för digital förvaltning, 2023). Samtidigt skriver de att de indentitetskontrollerande myndigheternas kostnad kommer att bli ungefär 30 miljoner kronor. Det kommer däremot inte bara behöva finnas en mobilapplikation utan det kommer även behöva finnas en datorapplikation som också behöver utvecklas, vilket gör systemet för e-id:n mer tillgängligt för alla medborgare (Myndigheten för digital förvaltning, 2023). Detta kapitel finns till för att öka förståelsen för hur mycket effektiviteten kan påverka en persons privatliv eller yrkesroll i tid och / eller pengar.

Zahlimar et al., (2023) skriver i deras artikel om hur e-tjänster ofta är smidigare än "analoga" tjänster då inom e-tjänster så sker allt digitalt medan "analoga" tjänster kräver att en individ skriver på papper. Detta är inte bara smidigare utan det sparar även både tid och miljö för både individen men också de som erbjuder tjänsten.

Tillgänglighet

I detta kapitel lyfts äldre och rörelsehindrade personer i alla intervjuer och hur ett system för digitala id-handlingar behöver utformas för att kunna anpassas till alla, inte bara gemene man. Idag finns det många problem med tillgänglighet kring digitala system då det finns några grupper i samhället som inte vill eller inte kan använda digitala system av olika anledningar. Däremot finns det även många åtgärder som kan tas för att få med så många som möjligt i systemet, exempelvis nämner respondent 5 att flera kommuner har arbetat med ungdomsgrupper för att utbilda äldre i hur de ska använda en smarttelefon, fyra av fem av respondenterna nämner detta som en lösning för vissa speciellt utsatta grupper. Tre av fem respondenter nämner att olika grupper har olika krav och därför måste detta tas i åtanke när detta system utformas. Dessutom finns det ett problem med internetuppkoppling för vissa, därför måste systemet kunna vara tillgängligt offline.

Sverige är idag ett av de länder som ligger i framkant med digitaliseringen, däremot har Sverige fortfarande problem med digitaliseringen för specifikt utsatta målgrupper, exempelvis äldre, personer med funktionsvariation eller personer utan svenskt personnummer (Myndigheten för digital förvaltning, 2023). Sverige har redan klarat många stora omställningar genom organisering, stora insatser och långsiktigt ansvar. Digitaliseringen har redan förändrat mycket i samhället men digitaliseringen kommer bara fortsätta förändra det svenska samhället. (Myndigheten för digital förvaltning, 2023)

Säkerhet

Respondent 5 nämner "Den som ansvarar för systemet måste 'täppa till hålen' i systemet för att kunna minimera risken för att användare blir identitetskapade. "..." I dagsläget är mycket

fokus på ‘snabbt och enkelt’ medan i framtiden måste fokus läggas mer på ‘tryggt och säkert’”. Precis som respondent 5 nämner finns det idag ett stort fokus på att Bank-ID och andra banktjänster ska vara snabba och enkla att använda, däremot finns det annat som står på kartan i framtiden. Istället för att ett system ska vara snabbt och enkelt kan systemet behöva vara tryggt och säkert, speciellt när det handlar om en persons identitet. En lösning på detta är kryptering. Kryptering gör systemet mer komplicerat i koden, däremot behöver inte kryptering göra systemet mycket svårare för individen att använda då kryptering används för att överföringar och lagring av data ska vara säkra. Med kryptering sparas inte datan i sin “råa” form utan datan går igenom ett form av lås som med hjälp av en publik nyckel krypteras och blir helt oläsbar som sedan skickas till en annan aktör som har en privat nyckel som kan “låsa upp” datan och gör datan läsbar. Denna publika nyckel kan lämnas ut till vem som helst då den endast kan användas för att låsa datan, den privata nyckeln eller som den ibland kallas hemliga nyckeln får aldrig lämnas ut till någon då den kan användas för att “låsa upp” all data som krypteras med den publika nyckeln. (Stine & Dang, n.d.) En annan aspekt som kan påverka systemet väldigt mycket är vilken aktör som är ansvarig för att utveckla och underhålla systemet. Exempelvis ifall systemet är privatägt av ett aktiebolag kommer aktieägarna försöka få så mycket vinst som möjligt från systemet, då kanske det kommer börja kosta att ha en e-legitimation. Medan ifall staten har ansvar för systemet kommer det inte kosta för individerna direkt utan kostnaden dras från pengarna som individerna betalar i skatt istället.

I Sverige finns det flera olika myndigheter som kan utfärda legitimationer, polismyndigheten, skatteverket m.fl. Detta gör att det finns ett väldigt stort utbud av legitimationer som personer kan ha, och därmed blir det svårare för legitimationskontrollanter att verifiera legitimationens giltighet. Även teknik för att förfalska legitimationer har blivit alltmer tillgänglig, som åtgärd för detta föreslogs 2017 att endast en myndighet ska vara behörig att utfärda legitimationer (Myndigheten för digital förvaltning, 2023). Efter pandemin har det kommit fram att det måste finnas en säker metod för att kunna identifiera en person digitalt, ifall en statlig e-legitimation endast ges ut vid ett personligt besök hos en identitetskontrollerande myndighet skapas stora möjligheter för en säker elektronisk identifiering. Detta ger även möjlighet för att kunna obehindrat identifiera personer elektroniskt. (Myndigheten för digital förvaltning, 2023)

Aspekten säkerhet var en spännande aspekt att följa genom intervjuerna, respondenterna som var yngre och mer teknikvana hade ett större förtroende till staten och deras möjlighet att utveckla e-tjänster. Detta matchar ganska bra med vad Zahlimar et al., (2023) skriver i deras artikel då de skriver om hur yngre personer är mer teknikvana och därmed har större förtroende för e-tjänster. Yngre personer vet även om att e-tjänster inte påverkar miljön lika mycket som de “analoga” tjänsterna, exempelvis kanske en individ som ska ta ett lås måste signera papper hos banken medan ifall en e-tjänst finns för detta är den yngre generationen mer trolig att använda den digitala tjänsten än den “analoga” tjänsten. Detta både för att digitala tjänster sparar på miljön

men också att e-tjänster ofta är smidigare att använda för en som är teknikvan sedan tidigare.

EU digitala identitetsplånbok

Bland respondenterna var det ingen som var emot idén med ett gemensamt sätt att legitimera sig runt om i hela EU, däremot var det två som var tveksamma angående hur stor utsträckning detta system skulle användas. Om det skulle vara ett system för hela världen så var det en person som var emot att koppla upp sig mot detta systemet med tanke på vilka länder som Sverige har konflikter med.

Även här nämns att Sverige måste ha ett digitalt e-id för att kunna delta i detta system. Detta e-id måste då vara på säkerhetsnivå 4 för att EU ska kunna godkänna det. Idag används ett privatägt system för e-id och det gör att Sverige är beroende av en privat aktör för att kunna identifiera Sveriges medborgare i statliga och bankärenden. EU menar att i den digitala identitetsplånboken ska allt ifrån körkort till betyg från skola kunna sparas, och på detta sätt kunna underlätta för alla i EU och göra legitimationskontroller mycket lättare och smidigare för både invånarna men också legitimationskontrollanterna då alla legitimationer kommer se likadana ut. EUs digitala identitetsplånbok måste inte bara kunna användas inom landet som invånaren är bosatt i utan den måste även kunna användas i alla andra medverkande länder också (Myndigheten för digital förvaltning, 2023). Inte bara identitetsplånboken behöver kunna användas utomlands men även e-id applikationen för annars begränsas samarbetet mellan olika EU länder. Digg bedömer att både ett fristående statligt e-id och en identitetsplånbok kommer att behövas. Det är tanken att identitetsplånboken kommer att integreras i personens smarttelefon, däremot leder detta till att många tekniska krav som ställs på smarttelefoner kommer att behöva ökas. Digg bedömer även att det är orimligt att medborgaren ska behöva gå till en identitetsutfärdande myndighet varje gång medborgaren skaffar en ny smarttelefon och därför görs bedömningen att medborgaren ska på distans med hjälp av den redan befintliga smarttelefonen med ett e-id på ska kunna utfärda ett nytt e-id för den nya smarttelefonen. (Myndigheten för digital förvaltning, 2023)

För att invånare ska använda ett digitalt system för körkort m.m finns det ett tydligt behov att tjänsten inte endast finns som en digital kopia av id-handlingen utan det vidareutvecklas på en sådan tjänst för att kunna erbjuda ett mervärde till landets invånare. (Holgersson et al., 2017) Ett digitalt system har väldigt stor potential att erbjuda ett mervärde för invånarna medan det samtidigt har en väldigt stor risk för att misslyckas ifall systemet inte erbjuder det invånarna vill ha.

Under tiden som detta examensarbete skrevs kom flertal regeringsbelut samt nyhetsartiklar ut. I Storbritannien kommer en digital identitetsplånbok att lanseras, troligtvis någon gång under 2025 (Wallenrud, 2025a). De nuvarande fysiska plastkorten kommer inte att sluta tillverkas utan den digitala varianten kommer vara ett frivilligt tillägg till plastkortet. Storbritannien är inte det första europeiska landet att införa

digitala id-handlingar utan det finns redan i flera länder, exempelvis Norge och Danmark. Alla EU-länder måste införa en typ av e-id senast år 2026 då EU håller på med utveckling av en plattform för digitala identitetshandlingar. (Wallenrud, 2025b) I hela EU kommer en digital identitetsplånbok att lanseras år 2030 och kommer vara ett komplement till det fysiska körkortet som finns idag. Den digitala identitetsplånboken kommer inte bara innehålla körkort utan ska även i framtiden ha stöd för att innehålla allt ifrån examensbevis till registreringsbevis för bilar. (Wallenrud, 2025b)

7. Resultat

Vilka aspekter av ett system för digitala id-handlingar är viktiga för systemets effektivitet, tillgänglighet och säkerhet?

Effektivitet: *De aspekter som är viktiga för systemets effektivitet är tiden det tar att visa upp / kontrollera legitimationen, kostnaden för systemets utveckling och underhållning, och hur mänskliga fel kan minimeras.*

Tillgänglighet: *De aspekter som är viktiga för systemets tillgänglighet är att systemet inte bara måste finnas på telefonen, det behöver även finnas på datorn. Systemet måste vara anpassningsbart mellan olika målgruppers krav, och att systemet måste vara tillgängligt att använda offline.*

Säkerhet: *De aspekter som är viktiga för systemets säkerhet är kryptering, flerstegsverifiering, dataskyddande åtgärder, begränsa antalet myndigheter involverade i utförandet av en legitimation.*

Inom intervjuerna och litteraturen har en aspekt stått ut extra mycket, nämligen säkerhet. Säkerhet verkar vara den aspekt som respondenterna oroar sig absolut mest över då ifall säkerheten skulle brista kan det leda till extrema konsekvenser för både stat och individ. Säkerheten är också den aspekten som påverkar absolut mest då ifall det är extremt bra säkerhet kommer systemet inte vara varken effektivt eller tillgängligt, den som utvecklar detta id-handlingssystem måste ta i beaktning hur bra säkerhet man kan ha på systemet för att fortfarande ha systemet både effektivt och tillgängligt.

I dagsläget finns dock fortfarande väldigt stort förtroende för digitala id-handlingar, fyra av fem respondenter som tror att ett sådant system kommer att öka effektivitet, tillgänglighet och säkerhet för alla medborgare. Idag används redan Bank-ID och Bank-ID är ett system som är tillräckligt säkert för nuläget, däremot finns flera problem med det fortfarande. Bank-ID är dessutom inte på en tillräckligt hög säkerhetsklass och därför behöver svenska staten utveckla en egen e-id tjänst som delas ut till de medborgare som vill ha den. Svenska staten behöver också utveckla en ny tjänst för att kunna delta i EUs digitala identitetsplånbok. Digg har tagit fram ett förslag på en statlig e-id tjänst som svenska staten behöver gå igenom och godkänna eller neka för att sedan gå vidare till utveckling av detta system. (Myndigheten för digital förvaltning, 2023)

7.1. Diskussion

7.2. Vald metod

En fallstudie tillsammans med en legitimationutförande myndighet hade varit optimalt, däremot fungerade inte detta i denna rapport då flera myndigheter kontaktades men dessvärre helt utan samarbetsvilja. Detta är något som en potentiell framtida studie får ta i beaktning. Denna rapport däremot har baserats på en intervjustudie och jämförts med litteraturen genom en litteraturstudie. Utmaningarna som är identifierade i denna studie baseras endast på intervjuer och litteratur, inget problem som är specifikt för ett specifikt fall. I ett fall som använder en fallstudie kan denna rapport användas som en källa för att komma igång med en bra bakgrund. En fallstudie tillsammans med en myndighet som har legitimationskontroller och / eller legitimationsutfärdande i myndighetens vardag hade varit helt optimalt för ett fortsättande arbete. Författaren till denna studie anser däremot att denna studie ger en bra övergripande bild över situationen.

7.3. Samhälleliga aspekter

Denna studie bidrar till samhället med en undersökning på hur olika aspekter påverkar effektivitet, tillgänglighet och säkerhet. Däremot är inget test genomfört då tiden för denna studien varit begränsad och därmed behövs vidare forskning inom området. Genom att identifiera hinder och utmaningar för användaracceptans kan forskningen hjälpa till att skapa mer användarvänliga och inkluderande identitetssystem. Genom en belysning på specifika betydelsen hur digitala id-handlingar kan påverka samhället. Genom ett säkert och effektivt digitalt identifieringssystem kan samhället dra nytta av ökad tillgänglighet och effektivitet i olika sammanhang, allt ifrån offentliga tjänster till privata transaktioner.

7.4. Vetenskapliga aspekter

En jämförelse mellan en intervjustudie och en litteraturstudie ger en väldigt djupgående förståelse för forskningsområdet. Detta tillvägagångssätt ger en mångsidig syn på problemet och tillåter en jämförelse mellan insamlad data och teoretiska insikter. Studien fyller en lucka inom forskningen genom att ett identifierat problem är besvarat, problemet blev identifierat genom väldigt mycket undersökning inom området effektivitet, säkerhet och tillgänglighet inom just digitala id-handlingar och andra statliga applikationer. Då hittades en lucka då ingen gjort någon som helst undersökning på vad det faktiskt är som är viktigt med dessa områden inom statliga applikationer. Denna undersökning behöver inte bara användas för statliga applikationer utan undersökningen kan även användas för undersökning inom den privata sektorn och är därmed generell. Denna undersökning kanske är väldigt specifik, däremot går denna studie att använda för mycket mer generella områden, som exempelvis andra statliga e-tjänster och mycket mer. Resultatet efter denna studie blev att säkerheten är den absolut viktigaste aspekten och säkerheten påverkar de andra aspekterna något extremt. Säkerheten kan vara den absolut viktigaste aspekten, däremot måste en utvecklare utöver

säkerhet ta andra aspekter i beaktning. Det är lätt att utveckla ett säkert system, däremot är det väldigt svårt att utveckla ett system som är både tillgängligt, effektivt och säkert.

7.5. Etiska aspekter

De etiska aspekter som beskrivits i tidigare kapitel är följda då hela intervjun är anonym med endast ett fiktivt namn. Alla deltagare har blivit informerade om frågorna direkt efter de tackat ja till intervjun, minst en dag innan intervjun. Informationen är sparad i ett separat dokument som sparas lokalt på samma dator som används för skrivningen av detta arbete. På detta sätt kommer ingen information att läcka ut på någon annan plats än författarens egen dator. Dessutom är alla svar på intervjuerna endast använda till denna studie och ingen information har givits ut till extern part. Alla respondenter är även informerade direkt innan intervjun att de är helt anonyma, vart svaren kommer att användas, vart svaren lagras och att varje deltagare kan dra sig ur intervjun ifall de känner att det är nödvändigt, i det fallet att en respondent dragit sig ur hade endast de svar som redan samlats in använts, inget mer hade samlats in.

7.6. Begränsningar och framtida forskning

Precis som det är nämnt tidigare i denna rapport finns det flera begränsningar med denna studie. En av dem är att det inte har kunnat utvecklas och testas ett system för digitala id-handlingar. En annan begränsning är att det inte har skett något samarbete med någon annan aktör för att kunna jämföra forskningen med ett aktuellt fall. Istället har ett problem identifierats genom intervjuer och en litteraturstudie. För framtida forskning skulle författaren av denna rapport rekommendera att en fallstudie tillsammans med någon myndighet och jurister för att få en bild över hur ett system kan fungera i den riktiga världen. Denna rapports resultat öppnar upp en möjlighet för en framtida forskningsartikel inom digitala id-handlingar.

Referenser

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

Europeiska kommissionen. (2021, Juni 3). *om ändring av förordning (EU) nr 910/2014 vad gäller inrättandet av en ram för europeisk digital identitet*. EUR-Lex. Retrieved February 12, 2024, from https://eur-lex.europa.eu/legal-content/SV/TXT/HTML/?uri=CELEX:52021PC0281

Febiri, F., & Hub, M. (2021). Digitalization of Global Economy: A Qualitative Study Exploring Key Indicators use to Measure Digital Progress in the Public Sector. *92*(SHS Web of Conferences). https://doi.org/10.1051/shsconf/20219205006

Holgersson, J., Lindgren, I., Melin, U., & Axelsson, K. (2017, 10 6). Not another wine in the same old bottles - motivators and innovation in local government e-service development. *AIS Electronic Library*. https://core.ac.uk/download/pdf/301372302.pdf

Internetstiftelsen. (2023, 10). Svenskarna och internet. https://svenskarnaochinternet.se/app/uploads/2023/10/internetstiftelsen-svenskarna-och-internet-2023.pdf

legitimation.se. (n.d.). *Legitimation och Id kort – Legitimation.se*. Legitimation.se. Retrieved February 16, 2024, from https://legitimation.se/legitimation-och-id-kort/

Myndigheten för digital förvaltning. (2023, January 30). *En säker och tillgänglig statlig e-legitimation*. Digg – Myndigheten för digital förvaltning. Retrieved February 11, 2024, from https://www.digg.se/download/18.5b30ce7218475cd9ed3ee0e/1675088054155/en-saker-och-tillganglig-statlig-e-legitimation.pdf

Raj, R. T., Sanjay, S., & Sivakumar, S. (2016, September 15). Digital License mv. *International Conference on Wireless Communications, Signal Processing and Networking*. 10.1109/WiSPNET.2016.7566342

Siddhartha, A. (2008, Maj 1). National e-ID card schemes: A European overview. *Information Security Technical Report*, *13*(2), 46-53. https://doi.org/10.1016/j.istr.2008.08.002

Stine, K., & Dang, Q. (n.d.). Encryption Basics. *Journal of AHIMA (American Health Information Management Association)*. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=908084

Sveriges Kommuner och Regioner. (2024, Januari 8). *Effektivitet*. SKR. Retrieved February 6, 2024, from https://skr.se/skr/demokratiledningstyrning/styrningledning/styrledningssystemarbetssatt/styraforresultat/effektivitet.55563.html

Sveriges Riksbank. (2022, December 15). Betalningsrapport 2022. *Riksbanken*. https://www.riksbank.se/globalassets/media/rapporter/betalningsrapport/2022/svensk/betalningsrapport-2022.pdf

Vetenskapsrådet. (2002). *Forskningsetiska principer inom humanistisk-samhällsvetenskaplig forskning*. Vetenskapsrådet.

https://www.vr.se/download/18.68c009f71769c7698a41df/1610103120390/Forskningsetiska_principer_VR_2002.pdf
Wallenrud, Å. (2025a, January 23). Nu slopas plasten: Digitala körkort blir verklighet. *Dagens PS*. https://www.dagensps.se/motor/nu-slopas-plasten-digitala-korkort-blir-verklighet/
Wallenrud, Å. (2025b, April 8). *Så här fungerar det digitala körkortet*. Dagens PS. Retrieved April 25, 2025, from https://www.dagensps.se/motor/sa-har-fungerar-det-digitala-korkortet/
Zahlimar, Abu Bakar, Ipik Permana, Mukarto Siswoyo, & Hamirul. (2023). Analysis and Study of the Use of Digital National Identity Card Services in Generation Z. *Open Access Indonesia Journal of Social Sciences*, *6*(5), 1061-1068. https://doi.org/10.37275/oaijss.v6i5.172