Linköpings universitet | Institutionen för ekonomisk och industriell utveckling
Masteruppsats, 30 hp | IT & Management
Vårterminen 2023 | LIU-IEI-FIL-A--23/04328--SE

Statlig elektronisk identifiering i en marknadsdriven försörjningsmodell

– om dess förutsättningar och utmaningar i Sverige

Government electronic identification in a private driven model

– about its conditions and challenges in Sweden

Linus Blomgren

Hubert Czekierda

Handledare: Fredrik Söderström & Maria Booth

Examinator: Björn Johansson

Linköpings universitet
SE-581 83 Linköping, Sverige
013-28 10 00, www.liu.se

Abstract

In Sweden, a government eID has long been a concept that has not been realized. The development of government eID in both Sweden and around the world has been problematic. Even if a government eID is developed, adoption of this can also be problematic. Therefore, this study examines the current situation in Sweden with eID and discusses the conditions needed and challenges with a government eID. This study resulted in three relationships that we believe are of great importance for eID in general and for Swedish government eID: 1) relationship between an individual and IT, 2) relationship between individual and organization and 3) inter-organizational relationships. These three relationships create conditions for continuous operation of the current eID in Sweden, but also discuss possible challenges within those relations and challenges a government eID can meet.

Keywords: electronic identification (eID), swedish eID, digitalization, e-government, digital divide

Sammanfattning

I Sverige har statlig eID länge varit ett koncept som inte har realiserats. Utvecklingen av statlig eID i både Sverige och runt omkring i världen har varit problematisk. Även om en statlig eID utvecklas kan adoption av detta också vara problematisk. Därför granskar denna undersökning nuläget i Sverige med eID för att sedan diskutera förutsättningar och utmaningar med en statlig eID. Diskussionen om förutsättningar och utmaningar resulterade i tre relationer som vi anser är av stor vikt för eID generellt och för statligt eID i Sverige: 1) relation mellan en individ och IT, 2) relation mellan individ och organisation och 3) interorganisatoriska relationer. Dessa tre relationer skapar förutsättningar för kontinuerlig drift av nuvarande eID i Sverige men diskuterar också möjliga utmaningar inom dessa relationer och som en statlig eID kan bemöta.

Nyckelord: elektronisk identifiering (eID), svensk eID, digitalisering, e-förvaltning, digital klyfta

Innehållsförteckning

1. Introduktion

1.1 Bakgrund

Elektronisk identifiering (eID) har blivit en teknisk lösning som i Sverige adopterats av både institutioner och invånare för att säkerställa identifiering och autentisering i en digital miljö, något som ersätter fysisk identifiering (Söderström, 2016). Orsaken till det kan anses vara att samhället som stort har digitaliserats, där institutioner har integrerats allt mer med IT (informationsteknik) sedan 80-talet (Goldkuhl, 1996); med en tydlig styrning mot det digitala har även invånaren kommit att integreras och organiseras med IT i form av bland annat offentliga tjänster.

Allt eftersom institutioner, och likaså samhället som stort, digitiserar data (gör analog data digital), digitaliserar processer (ändrar processer att inkludera digitiserad data för att effektivisera arbetsflödet), och genomgår digitala transformationer (digitalisering på bred skala, genomsyrar hela systemet) så förnyas tillvägagångssätt till att ta sig an problem med hjälp av digital teknologi (Gobble, 2018; Parida et al., 2019). Digitalisering innebär flerfaldiga möjligheter till värdeskapande på en individuell-, industriell-, och samhällelig nivå (Parida, 2018) och är den drivande faktorn när det kommer till intern effektivisering inom organisationer och att erbjuda externa möjligheter i form av nya tjänster eller produkter till kunder, något som bedriver förändringar i roller, arbetssätt, och tjänste- eller produktutbud som ett resultat av digital teknik (Parviainen et al., 2017).

E-förvaltning som effekt av en samhällelig digital transformation är ett brett studerat ämne (Bannister & Connolly 2012; Dawes, 2008; Saxena, 2005; m.fl.) med hög praktisk relevans. E-förvaltning avser framförallt hur institutioner inom offentlig sektor brukar IT för att digitalt transformera sig själva och sina tjänster (Lenk, 2002), framförallt i form av webbaserade applikationer som förenklar tillgången till myndighetsinformation och tjänster för medborgaren, företag, och andra myndigheter (McClure, 2000). Offentlig verksamhet enligt traditionella byråkratiska värden syftar till att tjäna invånarna och stödja samhället genom att fokusera på att leverera offentligt värde där de opartiskt ska tjäna alla invånare (Dobel, 2007).

Allt eftersom digitalisering transformerar offentlig sektor och myndigheters tjänsteutbud erbjuds i form av e-tjänster så har behovet av att kunna identifiera individer digitalt ökat (Beynon-Davies, 2006). Elektronisk identifiering krävs för att institutioner på ett trovärdigt sätt ska kunna identifiera en individ elektroniskt eller för att en individ ska kunna utföra olika

statliga-, bank-, betalning- och inloggningprocedurer genom att elektronisk identifiera sig själv. Olika teknologiska lösningar har anammats i samband med dessa digitala tjänster, BankID (Finansiell ID-Teknik BID AB, 2023a) är en av de applikationer som möjliggör autentisering vid elektronisk identifiering för invånare i Sverige och är den allra största aktören på marknaden. Vid identifiering av användare digitalt samarbetar institutioner med eID utfärdare där autentiseringen sker utanför institutionen där de förlitar sig på det kryptologiska beviset för identifikation från denna.

1.2 Problemformulering

Tillgång till information har gått och blivit ett krav för social inkludering och ekonomiskt deltagande, detta har i och med digitaliseringen ökat den digitala klyftan mellan de digitalt inkluderade och digitalt exkluderade (Powell et al., 2010). Eftersom eID är ett krav för att ta del av den offentliga sektorns tjänsteutbud riskerar individer som saknar tillgång att gå miste om social deltagning och hamna i ett digitalt utanförskap som kan innebära konsekvenser i form av avsaknad av information, risker vad gäller hälsa och välbefinnande, eller exkludering från sociala förmåner och strukturer (Friemel, 2016). Sett utifrån myndigheternas perspektiv kan det innebära att institutionernas möjligheter till organisatorisk effektivisering, digital säkerhet och trovärdighet försämras eftersom de inte tjänar alla. Sett utifrån ett invånarperspektiv så kan det innebära att svenska invånare får komplikationer kring samhälleliga tjänster och dessa procedurer på grund av exkludering, där ett direkt resultat blir utvidgandet av den digitala klyftan (Scheerder et al., 2017; Sparks, 2013).

BankID är den mest spridda IT lösningen som brukas i kontext med eID, där organisering av identifiering och autentisering till stor del har centraliserat sig kring BankID (Myndigheten för digital förvaltning, 2021). Enligt oss finns det ett problem då flertalet myndigheter numera kräver digitala autentiseringar i sina e-tjänster där de förlitar sig på privata leverantörer av eID. Här finns en överhängande risk om dessa leverantörer i framtiden väljer att inte längre erbjuda offentlig sektor sina tjänster. Dessa problem resulterar i risker för den samhällskritiska infrastruktur som vi som samhälle och eID användare blivit beroende av där tillgänglighet till olika e-tjänster kan drabbas (Myndigheten för digital förvaltning, 2021). Alternativa lösningar som Freja eID och AB Svenska Pass finns redan på marknaden där privatpersoner har möjlighet ansöka om tillgång; Freja eID kan argumenteras vara ett bättre alternativ till BankID i flera aspekter som interoperabilitet inom EU, en högre grad

transparens där användare kan spåra samtliga utförda transaktioner, och ID-växling med flera (Consid, 2018) men brukas i mycket mindre utsträckning. Vi har som samhälle "låst oss" till BankID, något vi ser i deras användarbas om åtta miljoner användare (Myndigheten för digital förvaltning, 2021). Rådande situation av eID i Sverige kan ses som en konsekvens av statens beslut att gå med en försörjningsmodell som bygger på att privata aktörer tillhandahåller e-legitimationslösningar vid första adoption, något som har inneburit att vi i vissa fall har fastnat kring BankID som enda lösning att avgöra hur flertalet av vardagliga procedurer för organisation och invånare hanteras. Elektronisk identifiering anses som en samhällskritisk infrastruktur som numera är omöjlig att se bortom (Myndigheten för digital förvaltning, 2021). Ett statligt försök till elektronisk identifiering är nu på väg som inkluderar ett fysiskt identifieringskort; Digg (Myndigheten för digital förvaltning) lämnade in ett förslag till Finansdepartementet för hur de tänker sig att en potentiell lösning skulle kunna se ut den 30 januari 2023. Blickar vi bortom Sveriges gränser så har redan mer än hälften av alla länder i Europa kort för eID men dessa och statlig eID överlag har haft liten eller begränsad framgång (Aichholzer & Strauß, 2010; Goodstadt et al., 2015; Lai et al., 2011) vilket potentiellt också kan bli fallet i Sverige.

1.3 Syfte och frågeställningar

Syftet är att undersöka rådande situation med eID i Sverige utifrån myndigheternas perspektiv, där BankID har varit den ledande aktören de senaste tjugo åren (Finansiell ID-Teknik BID AB, 2023b). Denna analys och problematisering kommer att lägga fram diverse utmaningar som statlig eID kan bemöta. Dessa utmaningar undersöks både från myndigheternas perspektiv som presenteras i vår empiri, dokumentation om statlig eID men också med hjälp av relevant akademisk litteratur som berör bland annat digitalisering, e-förvaltning, digital klyfta, hur statlig eID har sett ut utomlands inom EU samt möjliga drivande faktorer bakom adoption av eID.

Därför har nedan frågeställningar formulerats där rådande situation först undersöks i kontext med eID i Sverige (fråga 1) för att sedan framställa möjliga utmaningar som den statliga eID kan bemöta (fråga 2).

1) Hur ser den rådande situationen med eID och statlig eID ut i Sverige?
2) Vilka är de möjliga utmaningar som en svensk statlig eID kan komma att bemöta?

1.4 Avgränsningar och målgrupp

Studien är avgränsad till att innefatta rådande situation och utmaningar för statlig eID för att ge organisationer möjliga konceptualiseringar inför e-tjänster som kräver elektroniska autentiseringar. Elektronisk identifiering av individer kan beröra allt ifrån en ung målgrupp till en äldre målgrupp och därmed blir avgränsningen av individer på en väldigt generell nivå. Vi kommer inte att gå in på och beröra de olika strategiska och ekonomiska förutsättningar som krävs för projektet eller specifika tekniska kravspecifikationer för tekniken som möjliggör eID.

Den avsedda målgruppen för studien är framförallt IS-forskare, potentiellt inom området e-förvaltning eller kring elektronisk identifiering. Eftersom invånare och myndigheter som användare av tekniken diskuteras finns det även ett potentiellt intresse för dem i studiens slutresultat.

1.5 Kunskapsbidrag

Studiens tänkta kunskapsbidrag är att upplysa problematiken kring personlig identifiering i en digital miljö och tekniken som möjliggör detta. Problematiken syftar till att utpeka tekniken som mycket tas för given. Vidare är kunskapsbidraget ytterligare att presentera ett mer lämpligt tillvägagångssätt, handling och drift kring elektronisk identifiering som kan vara av intresse främst för institutioner. Generellt handlar det om att framställa en kritisk granskning av fenomenen kring elektronisk identifiering och teknisk monopol samt hur den förhåller sig till såväl praktik som till teori.

2. Metod

Interpretivismen som antar att verkligheten endast kan upplevas på ett subjektivt sätt har varit den generella filosofin och utgångspunkten för studien. Studien genomfördes enligt kvalitativ forskningstradition och är grundad i hermeneutisk teori. Den övergripande ansatsen och olika resonemang grundades i abduktion eftersom processen var en blandning av deduktiva och induktiva tillvägagångssätt. Fallstudie har använts för studien där tre olika myndigheter utgjorde kontexten för den valda forskningsstrategin. Datainsamlingen skedde i en tvärsnittsstudie och undersökte ett fenomen vid en specifik tidpunkt. Datainsamlingen har skett genom intervjuer av myndighetsanställda med relevant kunskap och erfarenheter för forskningsfrågan. Tematisk analys har tillämpats på den insamlade empirin från studien för att analysera och tolka datan. Forskningsfrågan grundades induktivt i ett praktiskt fenomen medan intervjuer och den slutliga analysen påverkades både induktivt och deduktivt.

2.1 Ontologi och dess konceptualisering

Ontologi är filosofiskt grundad och är läran om vad som finns; det som finns kan anta olika former av fenomen som exempelvis processer, relationer, typer av strukturer, objekt eller egenskaper (Introna & Ilharco, 2004; Smith, 2003). Då vi tycker att det kan finnas många, om inte oändligt många ontologiska kontexter och konceptualiseringar blir de ontologiska avgränsningarna viktiga (vilket beror på vem det är som observerar, vilket fenomen som observeras och vilka teoretiska tillämpningar som görs), något som kräver antaganden och är pluralistiskt i grunden (Becker & Niehaves, 2007; Smith, 2003).

De generella konceptualiseringar av ontologi som vi anser är mest relevanta för studien är av en social och en teknisk dimension. Kärnan i den sociala dimensionen är den subjektiva och intersubjektiva meningen samt det socialt konstruerade (Giddens, 1984; Orlikowski & Baroudi, 1991). Om det subjektiva består av personliga upplevelser, känslor, tankar och intentioner behandlar intersubjektivitet gemensamma uppfattningar av de olika fenomenen som exempelvis manifesteras med social handling och intersubjektiv kunskap som stöds av språk (Goldkuhl, 2022). Sociala konstruktioner som kan bestå bland annat av sociala mönster i form av samhälle, myndigheter, politik, ekonomi, maktstrukturer, lag, resurs och dess organisation är dynamiska som formas av yttre omständigheter, koncept och sociala mål i en miljö som begränsar men också möjliggör fenomen och handlingar där rekursiva handlingar antingen resulterar i reproduktion eller produktion av (nya) strukturer (Adler et al, 2022;

Kompella, 2017). Det konstruktivistiska perspektivet som främst kan användas till att analysera det kontextuella, maktstrukturer och vad makt gör (Guzzini, 2005), ger oss grundläggande antaganden och abstraktioner till vår analys. Fortsättningsvis ger det konstruktivistiska perspektivet och konceptet av relationen mellan agens och struktur grova antaganden i det kontextuella och en utgångspunkt i diskussionen för analysen; där individens agens är av vikt och ses som något värdefullt men också kontrasteras och påverkas av sociala strukturer och organisationer.

Den tekniska dimensionen där data stödjer information, kunskap, och IT system är till för att iterativt och framväxande uppfylla sociala krav och kopplar samman heterogena aktörer i digitala miljöer i allt snabbare takt (Lee, 2003; Yoo et al., 2010a). IT har en mångfald konceptualiseringar där det kan antas att IT är en behandlare och leverantör av information, ett verktyg eller en ersättare av ett arbete eller som en struktur för sociala handlingar och organisationer med ambivalent karaktär då den ständigt förändras (Kallinikos et al., 2013; Orlikowski, 1992; Orlikowski & Iacono, 2001). Generellt möjliggör IT mediering av representationer av sociala verkligheter men det kan också anses att IT skapar en förväntad framtid och därmed formar den sociala dimensionen (Baskerville et al., 2019). Då vi ser IT både som ett verktyg och som en struktur för social handling eller organisation, resulterade det i en analys som diskuterar IT på en subjektiv och individuell nivå (när en individ blir en användare av IT) samt på en strukturell nivå (där IT upprätthåller samhällskritiska infrastrukturer som eID).

Våra ontologiska konceptualiseringar kan ses som ett perspektiv och utgångspunkt i vår analys av litteratur, empiri och diverse relationer mellan individen, tekniken och organisation; däremot anser vi att fenomenen av eID i Sverige kräver en mångfald av (mer kontextuella) teorier utöver det konstruktivistiska perspektivet (Mir & Watson, 2000).

2.2 Epistemologi: interpretivism och hermeneutik

Epistemologi behandlar bland annat läran om kunskapsbildning (Becker & Niehaves, 2007). Eftersom våra ontologiska antaganden och avgränsningar är grundade i subjektiv mening och sociala strukturer anser vi att interpretivism är ett lämpligt och relevant epistemologiskt tillvägagångssätt som just fokuserar på förståelse av en social dimension; förståelsen kan bildas genom att tolka subjektiv och intersubjektiv mening (Goldkuhl, 2012; Klein & Myers, 1999). Detta kräver att se, anta och engagera sig i kontextuella verkligheter av sociala

grupper och deras deltagande i processer som något meningsfullt för att sedan uppvisa hur mening och intentioner ger upphov till social handling i syfte att på ett intersubjektivt sätt förklara varför personer, handlingar och processer bedrivs på det sättet som de görs (Orlikowski & Baroudi, 1991; Mathiassen, 2017).

Insamling av kvalitativ data sker vid interaktionen mellan forskare och utomstående parter där den kvalitativa datan konstrueras och tolkas subjektivt; processen kräver dialog, reflektion samt mottaglighet åt bias eller förvrängning i form av metaforer (Jahnke, 2012; Klein & Myers, 1999). Den tolkade och kontextuella meningen av sociala grupper används sedan som byggstenar inför kunskapsbildning (Goldkuhl, 2012) där ett dialogiskt resonemang förs mellan forskarens förutfattade meningar och studiens fynd (Klein & Myers, 1999).

Vanligtvis komplementeras interpretivismen med hermeneutik (Goldkuhl, 2012; Klein & Myers, 1999). Från ett historisk perspektiv behandlar hermeneutik studien av tolkning av text vilket utvecklades till orala utsägelser och anses lämplig även för studien av handling och tekniska interaktioner (Rennie, 2012; Myers, 2004). Syftet med hermeneutik är att tydliggöra och förstå det som studeras. Detta börjar med att inse vikten av historicitet vilket utpekar att sociala kontexten, språket, vanor och handlingar är formade av historiska omständigheter. Då tidigare kunskaper, fördomar och bias kan bli av vikt och stråla från både forskaren och det som studeras, blir detta något som kräver medvetenhet men också är nödvändigt att inneha för att förstå språket (Myers, 2004).

Den hermeneutiska cirkeln är ett koncept som utpekar en cirkulär och iterativ relation och process mellan de kontextuella och de övergripande fenomenen; kontextuella fragment upplyser om de övergripande fenomenen men likaså upplyser de övergripande fenomenen kontextuella fragment (Rennie, 2012; Myers, 2004). Insamling av kvalitativ data kräver dialog och reflektion vilket kan stödjas av en dialektisk process med aktivt frågande och bevarande som börjar med tidigare kunskaper för att nå förståelse av det som studeras (Jahnke, 2012).

I vårt sammanhang har den cirkulära processen applicerats både på litteraturgranskning och de fenomen som studerats. Litteraturgranskning behandlar sökning, identifiering, och anskaffning av det som anses relevant för att sedan analysera och tolka inför argumentationer (Boell & Cecez-Kecmanovic, 2014). Hermeneutiska cirkeln i vår studie innebär att vi ser intervjuer och tolkning av litteratur som en del av den övergripliga helheten i syfte att upplysa organisatoriska strukturer bakom eID (Myers, 2004). Hermeneutik anser vi är en

teori som stödjer vår tolkning av litteratur till att anskaffa förståelse av relevanta fenomen men också såväl subjektiv som intersubjektiv mening samt sociala strukturer.

2.2.1 Generalisering av interpretivistisk tillvägagångssätt

Klein och Myers (1999) trycker på vikten av generalisering och har det listat som en av sina sju principer inom interpretativ forskning. En teori som saknar validitet i en kontext utanför där den empiriskt testats saknar användbarhet (Lee & Baskerville, 2003). IS-fältet består inte bara av forskare, utan även praktiker, som dagligen arbetar inom området. Detta innebär att möjligheten till generalisering inte bara är av akademisk relevans utan även av praktisk relevans där resultatet kan komma till nytta inom olika organisatoriska kontexter ute i praktiken (Lee & Baskerville, 2003). På grund av Humes truism så kan inte en teori generaliseras till en kontext där den ännu inte empiriskt testats; att öka antalet respondenter hjälper inte heller för att styrka dess generaliserbarhet (Lee & Baskerville, 2003). Det enda sättet att bekräfta en teoris generaliserbarhet till en ny kontext är att testa teorin i en ny kontext (Lee & Baskerville, 2003). Denna studie ämnar att bidra med vad vi kallar generaliserbar kunskap, det vill säga kunskap som framtida forskare eller praktiker kan använda för att formulera uppfattningar om vad de potentiellt kan komma att förvänta sig i andra fall. Utifrån vår empiri formulerar vi teoretiska påståenden som forskare och praktiker kan generalisera till kunskap, eller lärdomar, i andra kontexter.

2.3 Övergripande tillvägagångssätt och resonemang

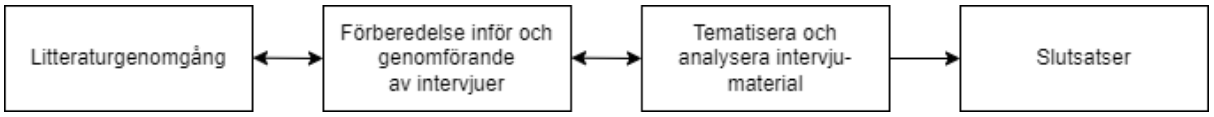
På ett sätt anser vi att abduktion är den ärligaste benämningen av resonemangen i en akademisk procedur trots att viss forskning lutar sig mer åt det deduktiva eller induktiva. Studiens ontologi som är det (inter)subjektiva och det konstruktivistiska har inneboende komplexitet som kräver tolkning och förståelse; detta “grävs ut” med hjälp av hermeneutisk teori om delar och helheten. Den första tolkningen som skapas av text och tal är endast en första gissning som behöver prövas och kritiseras i kontext med det som är runtomkring (Rennie, 2012).

Studiens abduktion, utöver tolkning av mening, sker också genom kontextualisering, litteratursamling och semistrukturerade intervjuer. Det kontextuella utpekar ett visst fenomen som bedriver några antaganden och kan därmed benämnas som en induktiv process. Tidigare forskning kontrasteras med fenomen som skapar ytterligare alternativa antaganden, något vi ser som deduktivt i grunden. Under de semistrukturerade intervjuerna sker både en

utforskning av det kontextuella (induktion) men som också kompletteras med en fot i tidigare forskning (deduktion). Både det induktiva och deduktiva är som stöd och resulterar i en iterativ och engagerad forskning som är nära knuten till en praktisk kontext (Mathiassen, 2017). Överlag handlar det om studier av individer som interagerar i varierande organisatoriska och professionella kontexter som stöds av ontologiska fenomen som diskuteras (både oralt men också genom akademisk litteratur) och resulterar i lingvistiska och relationella påståenden (Goldkuhl, 2023). För att på bästa sätt besvara våra forskningsfrågor togs en undersökningsstrategi fram. Studien bedrevs med en kvalitativ ansats och av interpretivistisk natur för att få en djupgående förståelse för problemet utifrån olika subjektiva och intersubjektiva upplevelser och processer. Urvalet av litteratur för studien har varit en iterativ process, men inte strukturerad. Sökningar har gjorts efter nyckelord och fraser som ansågs relevanta för studiens ändamål, huvudsakligen i Google Scholar. Under läsning har källor som refererats till nedtecknats om av potentiellt intresse för vidare läsning, något som kan efterlikna en snöbollseffekt där en artikel kunde ge inspiration till ytterligare flera intressanta artiklar.

Figur 1

Forskningsprocess för studien



2.4 Fallstudie

Fallstudie innebär en intensiv analys av en individuell enhet (som en person eller en organisation) och trycker på utvecklande faktorer i relation till sin kontext (Merriam-Webster, 2023). Ser vi bildligt till det engelska namnet “case study” så är det en kontextuellt inramad studie där fodralet utgör ramarna för studien. På så sätt kan en fallstudie anses vara en kontextuell avgränsning för studien. Flyvbjerg (2011) beskriver att en fallstudie inte är ett metodologiskt val, utan snarare ett fenomenologiskt val av vad som är tänkt att studeras. Fallstudier studerar system, och system utvecklas ofta över tid. Den här studien kommer inte bedrivas longitudinellt vilket begränsar fallstudiens potential delvis, där fallens händelseförlopp eller “utvecklande faktorer” över tid inte kan fångas.

Fallstudien har gått och blivit en väldigt populär forskningsstrategi inom kvalitativ forskning (George & Bennett, 2005) men att en forskningsstrategi är populär är dock inte en anledning till att använda den, anledningen bör vara kopplad till studiens syfte (Flyvbjerg, 2011). Likt alla forskningsstrategier är fallstudien inget undantag till att ha styrkor såväl som svagheter. Det är en strategi som har potential att gå på djupet och vara rik på detaljer, däremot är det en mindre effektiv metod om något vill studeras på bredden där statistiska metoder är att föredra (Flyvbjerg, 2011). Genom att bedriva en fallstudie och samla in flera olika myndigheters tankar och åsikter kring samma fenomen fick vi oss en överblick över nuläget kring eID i Sverige, de olika myndigheterna bidrog på så sätt med delar av den större helheten.

Vår fallstudie har innefattat att studera eID och dess bruk inom svenska myndigheter, men även att undersöka olika förutsättningar och utmaningar inför utvecklingen och implementeringen av en statlig eID. Vi valde att analysera varierande svenska myndigheter eftersom vi anser att de utgör en kritisk samhällelig struktur och därmed är centrala entiteter för olika utomstående privatpersoner. Eftersom myndigheternas syfte bland annat är att inkludera så många människor som möjligt och att eID är ett viktigt moment inom olika myndigheters e-tjänster ger det oss en kontext som är av praktisk relevans eftersom frågor kring identifiering inom offentlig sektor är av stor vikt.

2.5 Tvärsnittsstudie

Eftersom studien har haft en klar tidsbegränsning i kalendertid om endast ett fåtal månader saknades möjligheten till en longitudinell studie. Denna avgränsning präglade därmed starkt forskningsfrågan och resulterade i en tvärsnittsstudie som syftar till att undersöka ett fenomen vid en given tidpunkt (Kesmodel, 2018). För att verkligen definiera vad en given tidpunkt innebär så behöver vi se till studiens omfattning om fyra till fem kalendermånader. Studien har syftat till att bedriva en nulägesanalys av den rådande situationen kring eID i Sverige, utifrån det kan argumentet föras att en undersökning av fenomenet vid en specifik tidpunkt snarare än över en längre tidsperiod även har fångat syftet för studien bättre.

2.6 Datainsamling och analys

2.6.1 Datainsamlingsmetoder

Insamlingen av empiri av god kvalitet har varit av yttersta vikt för studiens slutresultat; detta då empirin är i direkt relation till analysen, desto bättre empiri desto bättre grund för analys

av hög kvalitet. Empirin som samlats in för studien har gjorts med hjälp av semistrukturerade intervjuer med erfarna praktiker från olika myndigheter som är berörda av eID, utöver det har även Diggs nya förslag för en statlig eID (Myndigheten för digital förvaltning, 2023), deras rapport kring utvecklingen av det svenska e-legitimationssystemet (Myndigheten för digital förvaltning, 2021) samt lagrådsremissen om auktorisationssystem (Regeringskansliet, 2023) granskats i studien. Urvalet av myndigheter har inte gjorts slumpmässigt utan med så kallad avsiktligt valda element, där de tre valda myndigheterna ansågs besitta betydelsefull information för studien. Clark et al. (2021) menar att ett sådant urval görs just på grund av att de anses besitta rätt typ av kunskap som kan leda studien till att besvara sin forskningsfråga. Urvalet av respondenter var dock inget vi styrde själva, utan gjordes huvudsakligen av myndigheterna själva. Ett undantag till den regeln gjordes dock där en av myndigheterna vid första kontakt inte ville ställa upp på intervju, något som tvingade oss att kontakta anställda personligen istället för att gå via deras offentliga kanal för kommunikation.

Både inom sociala studier (Clark et al., 2021) och inom IS studier (Myers, 1997) anses intervjuer vara centrala för att generera kvalitativt empirisk data. Den semistrukturerade intervjun, som var intervjumetoden för empiriinsamlingen, används brett inom kvalitativ forskning för att förstå varför människor beter sig som de gör genom att utforska deras uppfattningar, erfarenheter och attityder (Harvey-Jordan & Long, 2001). Likt alla metoder kommer den kvalitativa intervjun med för- och nackdelar. Det är en metod som tillåter forskaren att generera data från respondenternas vardagliga miljö, som när intervjun genomförs på arbetsplatsen hos respondenten (Goldkuhl, 2019). Det innebär dock en del utmaningar som att behöva förlita sig på att respondenten både förmedlar korrekt information samt besitter förmågan att uttrycka sig själv ordentligt (Hodder, 1994). Det är genom respondentens förmåga att förmedla sig själv korrekt som forskaren får tillgång till respondentens verklighet (Becker & Geer, 1957). Vad respondenten förmedlar är deras subjektiva uppfattning av verkligheten, formad av tidigare erfarenheter och det mänskliga medvetandet (Orlikowski & Baroudi, 1991) där syfte, tro, och intention kan komma att påverka (Goldkuhl, 2012). Det är forskarens uppgift att begripa sig på och konstruera datan på bästa sätt utan att förvränga den, allt medan denne förblir medveten om att det speglar respondentens subjektiva verklighet (Goldkuhl, 2012). Intervjuer kan vara av olika karaktär beroende på vilken intervjumetod som väljs. En semistrukturerad intervju är en strukturerad intervjumetod som lämnar ett visst utrymme för frihet att röra sig utanför ramarna av en intervjuguide och fördjupa sig i inte sedan tidigare förutbestämda teman. Den

semistrukturerade intervjun är kapabel till att fånga olika aspekter av mänskligt och organisatoriska beteende (Qu & Dumay, 2011), och ses ofta som den mest effektiva och behändiga metoden för att samla in information (Kvale & Brinkmann, 2009).

Institutionella dokument har varit objekt för granskning i kvalitativ forskning under många år (Bowen, 2009). Dokument är en viktig datakälla för kvalitativ forskning där dokumenten innehåller information som tecknats ned utan forskarens påverkan (Clark et al., 2021; Bowen, 2006). Dokumentanalys används ofta tillsammans med andra kvalitativa metoder där den kvalitativa forskaren beräknas använda åtminstone två källor för bevis och att eftersträva konvergens och bekräftelse mellan dessa (Bowen, 2009). Bowen (2009) fortsätter att det är en tidsmässigt effektiv metod där datan redan är insamlad och bara behöver utvärderas. Det är även ofta en väldigt tillgänglig metod, speciellt sedan tillgången av internet. En av nackdelarna med dokument är att de sällan innehåller tillräckligt med information men fungerar som ett bra komplement.

Eftersom fallstudiens kontext är svenska myndigheter är våra respondenter en variation av tjänstemän som är nära kopplade till lagliga och tekniska aspekter av implementering och bruk av eID i myndigheter. Dessa respondenter anses relevanta eftersom de besitter insyn kring såväl konsekvenser som mål med eID i olika sociala och strukturella sammanhang.

Det empiriska materialet har samlats in genom semistrukturerade intervjuer med tjänstemän från olika svenska myndigheter. Totalt har fyra respondenter intervjuats från tre olika myndigheter över tre intervjutillfällen. Dessa respondenter benämns som Respondent A, B, C och D. Samtliga respondenter har flera års erfarenhet inom både offentlig sektor och elektronisk identifiering. Alla fyra respondenter innehar idag en roll där de på strategisk nivå arbetar med frågor som berör elektronisk identifiering. De semistrukturerade intervjuer kompletteras med relevant innehåll från Diggs och Regeringskansliet utskrifter om statlig eID där dessa ger oss insyn i olika utmaningar och krav som finns kring en statlig eID och ger en god inblick över den rådande situationen. I och med att den statliga eID lösningen är tänkt att bland annat appliceras inom myndigheter ger insatta respondenter från olika myndigheter och dokumenten från Digg två olika perspektiv på en och samma utmaning som komplementeras med lagrådsremissen för auktorisationssystem för en bättre inblick kring hur infrastrukturen för eID ser ut praktiskt.

1) “Utveckling av det svenska e-legitimationssystem” (Myndigheten för digital förvaltning, 2021) som ger en bild av nuläget och en översikt av nuvarande e-legitimationssystem.

2) “En säker och tillgänglig statlig e-legitimation” (Myndigheten för digital förvaltning, 2023) som behandlar förslaget till statlig e-legitimation.

3) “Auktorisationssystem för elektronisk identifiering och för digital post” (Regeringskansliet, 2023) som föreslår att valfrihetssystem i fråga om elektronisk identifiering ska ersättas av auktorisationssystem.

2.6.2 Analysmetoder

För att analysera empirin har tematisk analys använts. Tematisk analys har en lägre ingångströskel än andra analysmetoder som exempelvis dataanalys eller korrespondensanalys och är på så sätt ett bra analysverktyg för forskare med bristfällig erfarenhet inom kvalitativa forskningstekniker (Braun & Clarke, 2006). Tematisk analys är vanligt använd och erkänd för sin mångsidighet och flexibilitet (Kiger & Varpio, 2020). Tematisk analys är en metod för kvalitativ analys (Braun & Clarke, 2006) och en metod om sex steg för tematisk analys framtagen av Braun och Clarke (2006) har använts för studien, där rå intervju data gradvis blir mer och mer definierad.

1. Bekanta sig med datan: Transkribera data verbatim (i detta fall intervjuer), läsa och läsa om datan, anteckna initiala idéer.
2. Generera ett första utkast av koder: Koda intressanta stycken bland datan, koppla an data till varje kod.
3. Temasökning: Likt tidigare steg fast koppla nu an koder till potentiella bredare teman.
4. Temagenomgång: Gå igenom och säkerställ att alla teman fungerar både i relation till koderna men även till datan.
5. Definiera och namnge teman: Förfina varje specifikt tema och analysen, generera konkreta definitioner för varje enskilt tema.
6. Producera rapporten: Slutgiltig analys, relatera tillbaka från analys till forskningsfrågor och det teoretiska ramverket, och formge en komplett akademisk rapport.

2.6.3 Etiska överväganden och kvalitetskriterier

Forskningsstudien har valt att avstå från att benämna respondenter och organisationer med deras formella namn; detta i syfte att bevara respondenternas och organisationernas integritet. För att garantera deras säkerhet har de istället pseudonymiserats. Det är god tradition att praktisera diskretion när det kommer till forskningsdata, speciellt när den innehåller information om människor eller organisationer (Jansson, 2015). Det är av högsta vikt att respektera integriteten hos respondenter och att inte möjliggöra för återidentifiering bakom anonymiserad data (ACM, 2018). Våra respondenter har begärt att förbli anonyma, både på en individuell nivå men även den myndighet de representerar. Detta ställdes som krav utifrån ett säkerhetsperspektiv inför intervjuerna då de innehar känsliga befattningar inom sina respektive organisationer.

Interpretivistisk forskning kan hjälpa IS forskare att förstå mänskliga tankeströmningar och handlingar i olika sociala kontexter (Klein & Myers, 1999). I utvärderande syften har vi kvalitetssäkrat studien med Klein och Myers (1999) sju principer för interpretivistisk forskning, dessa har diskuterats i kapitel 2.2 och 2.2.1; den hermeneutiska cirkeln, kontextualisering, data som en social konstruktion utifrån interaktionen mellan forskare och respondent, dialogiskt resonemang mellan förutfattade meningar och studiens fynd, subjektiva tolkningar som kan innebära olika beskrivningar av samma fenomen, och uppmärksamhet till olika bias från respondenterna.

3. Forskningsöversikt- Analytiskt ramverk

3.1 Digitalisering

Det moderna samhället har utvecklats, och fortsätter att utvecklas, att bli allt mer beroende av olika digitala teknologier. Skalan till vilken digitala teknologier integrerats i samhället är enorm (Igolkin et al., 2020). Digitalisering har identifierats som en av de större drivande faktorerna som förändrar samhälle och företag, både på kort och lång sikt (Tihinen & Kääriäinen, 2016). Trenden runtom i världen påpekar otvivelaktigen på att den digitala transformationen av samhället kommer påverka samtliga länder och grenar av världsekonomin där en förändring av decentralisering av maktstrukturer och kontroll kan ske då värde distribueras över en stor mängd aktörer (Igolkin et al., 2020, Yoo et al., 2010b). Innovation och utveckling av digitala teknologier är en förutsättning för digital transformation och kräver bland annat nya tekniska kombinationer, homogenisering och interoperabilitet av data och teknik samt interorganisatorisk praktik som har möjlighet att resultera i teknisk och praktisk konvergens inom organisationer där teknik och praktik blir likformig (Pardo & Tayi, 2007; Yoo et al., 2010a, 2010b).

En konsekvens av digital infrastruktur, teknisk innovation och utveckling är att teknik kräver självreferering (*eng. self-reference*), det vill säga en teknisk rekursiv cirkel; ny teknik är bunden till redan befintlig teknik vilket minskar krav för introduktion av ny teknik, minskar kunskapskraven för nästa teknik och möjliggör på så sätt en större grad adoption (Yoo et al., 2010a). Samtidigt som digitalisering ofta berör digitalisering av organisationer förändrar det också livet utanför organisationen. Ännu en konsekvens är att digitalisering och att enskilda individer integreras med diverse tekniska artefakter vilket möjliggör globala observationer, insamling av stora mängder av data om beteende i digitala miljöer och profilering av individer (Aichholzer & Strauß, 2010; Yoo et al., 2010b).

Fortsättningsvis krävs det ansträngningar att optimera användandet av digitala tekniker och data, och att på nya sätt både fånga och skapa värde genom digitalisering. Detta innefattar nya organisationsformer och omarbetade processer för att bättre kunna dra nytta av möjligheterna som digitala teknologier innebär (Björkdahl, 2020). Digitalisering innebär på så sätt mer än endast digital teknik och data (Björkdahl, 2020) utan är en process baserad på effekterna av användandet och integreringen av digitala teknologier som påverkar samtliga

nivåer av företag och samhälle (Igolkin et al., 2020). Parviainen et al. (2017) talar om fyra olika nivåer där digitalisering påverkar oss: process-, organisations-, verksamhetsområdes-, och samhällelig nivå. Digitalisering innefattar mer än att bara omvandla existerande processer till digitala, det handlar om att tänka om vad gäller nuvarande verksamhet med ett nytt perspektiv möjliggjort genom digitala teknologier (Parviainen et al., 2017).

Observationer kring digitaliseringens effekter visar primärt på att organisationer använt det som ett sätt att effektivisera verksamhets- och produktionsprocesser samt för att förbättra produkter eller tjänster med ökad funktionalitet (Björkdahl, 2020). Digitalisering har enligt Parviainen et al. (2017) haft en klar och tydlig påverkan på och möjliggjort för myndigheter att operera med effektivitet och transparens, och för de allra flesta underlätta invånares tillgång till offentliga tjänster. Digitaliseringens påverkan är mångfacetterad och kan ses på från tre olika perspektiv (Parviainen et al, 2017):

1. Intern effektivisering – effektiviseringar i arbetssätt genom digitala medel
2. Externa möjligheter – nya möjligheter i existerande verksamhetsområde, exempelvis i form av nya tjänster eller nya kunder
3. Disruptiv förändring – mer disruptiva förändringar genom digitalisering som nya verksamhetsroller eller nytt verksamhetsområde

Allt eftersom organisationer digitaliserar sina verksamheter blir det lätt att en myriad av olika system anskaffas för att bemöta olika verksamhetsbehov eller i effektiviseringssyften (Henfridsson & Bygstad, 2013). Dessa system blir en del av institutionernas digitala infrastrukturer. En av de mekanismer Henfridsson och Bygstad (2013) identifierade som möjliggör och ligger bakom utvecklingen av digitala infrastrukturer är adoption. Adoption innefattar hur fler användare adopterar tekniken allt eftersom mer resurser investeras och användbarheten ökar.

3.2 E-förvaltning

Adoptionen av IT och dess användning inom den kommersiella sektorn i samband med spridningen av internet bland den generella populationen gav upphov till dels en ökad familjaritet med elektroniska tjänster men även därigenom en stigande förväntan på bekvämlighet. Denna förväntan sträcker sig bortom den kommersiella sektorn där medborgare även förväntar sig liknande tjänster med samma effektivitet av organisationer i offentlig sektor (Ebrahim & Irani, 2006). Oakley (2010) har definierat e-förvaltning som en

tekniskt medierad tjänst som främjar en transformation i relationen mellan medborgare och offentlig sektor. Brett talat så innebär e-förvaltning digitaliserade förvaltningsärenden som är tänkt att vara tillgängliga dygnet runt utan att behöva besöka ett fysiskt kontor, möjliggjorda genom involverandet av IT. Genom en integrerad webbplatser kan medborgare få tillgång till offentliga tjänster och utföra ärenden med offentlig sektor (Ebrahim & Irani, 2006).

Allt mer och mer ser vi en ökande insikt hos utvalda representanter i riksdag och tjänstemän kring den potentiella nyttan med e-förvaltning i syfte att effektivisera verksamhet och att möjliggöra förmåner till medborgare och olika verksamhetspartners (Ebrahim & Irani, 2006). Jakten efter offentligt värde går långt bortom privata sektorns ekonomiska intresse, där e-förvaltningsstrategin behöver ta hänsyn till såväl politiska som sociala mål. Att uppnå offentligt värde inom e-förvaltning innebär att kunna leverera effektiv förvaltning, förbättrade tjänster till medborgare och företag, och att sociala värden som inkludering, transparens, och deltagande tas hänsyn till (Twizeyimana & Andersson, 2019). Hirst och Norton (1998) beskriver tre förändringsområden som e-förvaltning möjliggör internt, externt, och relationellt. Dessa tre områden går att jämföra med de tre områden Parviainen et al. (2017) menar att digitalisering påverkar inom. E-förvaltning har möjlighet att påverka interna processer och funktioner, att externt öppna upp och bli mer transparent mot medborgare och företag, och att fundamentalt påverka relationen mellan medborgare och staten, men även mot andra stater, med potentiella implikationer på demokratiska processer och strukturer inom offentlig sektor.

E-förvaltning är ett fenomen som sträcker sig över samhällen och organisationer vilket tyder på att interorganisatoriska aspekter, där strukturer, praktik och koncept bedrivs mellan organisationer och med hjälp av homogen och interoperativ IT (Yoo et al., 2010). Konceptet av interorganisation påverkas av en mängd faktorer som organisationers syfte, sociala trender, teknik, information, interaktion, innovativitet och är överlag något heterogent, asymmetriskt eller helt enkelt olika i grunden (Kompella, 2017). Interorganisatoriska relationer kräver mänskliga relationer, förhandlingar, tillit och engagemang samt kan leda till konflikter, resursdelning eller beroenden av varandra (Pardo & Tayi, 2007). En drivare av resursdelning tar form av teknisk interoperativitet där IT samlar, centraliserar och distribuerar data. Data kräver hög kvalitet, precision och fullständighet samt information i syfte att effektivisera manuellt arbete och bedriva automatisering. Det kan uppstå påtryck på organisationer av yttre sociala och fysiska omständigheter, tekniska innovationer, interna eller externa intressenter, formella eller informella påtryck som kan bedriva inkrementell eller radikal förändring eller

uppleva påtryck för en viss utvecklingsväg. Utveckling av e-förvaltning kan ses som en interaktiv utveckling där radikala mål uppnås med inkrementella förändringar inom och mellan organisationer som i slutändan bedriver radikala strukturella och beteende förändringar (Kompella, 2017; Pardo & Tayi, 2007).

3.2.1 Digital klyfta

I västvärlden påbörjade den digitala klyftan i och med bristfällig tillgång till digitala enheter för personer; sedan ansågs att brist i kunskapsanvändning av tekniken är ännu en faktor som bedriver fenomen (Sparks, 2013). Överlag utpekar digital klyfta sociala skillnader gällande olika ojämlikheter av teknisk tillgång, adoption, användning, användarkompetens och av fördelar när datorer och internet används (Friemel, 2016; Scheerder et al., 2017; Sparks, 2013). Brist i personens medvetandet av data och algoritmisk användning, tillgång till relevant information eller helt enkelt personens motivationsbrist för teknisk användning är flera anledningar till en digital klyfta (Lythreatis et al., 2021).

Den digitala klyftan kan innebära konsekvenser för den enstaka individen som exempelvis brist på eller avsaknad av politisk information och deltagning, bedriva olika risker för hälsa och välbefinnande, eller bli exkluderade från sociala förmåner och strukturer (Friemel, 2016).

Klyftan är inte enbart grundad i teknologiska konsekvenser men också i något individuellt, socialt, ekonomiskt och politiskt (Friemel, 2016; Sparks, 2013). Diverse funktionshinder för det sensoriska, fysiska eller kognitiva kan vara anledningar som skapar digital klyfta; webbplatser tar sällan i åtanke kognitiva eller språkliga funktionshinder vilket leder till att generell internethantering, användning av lösenord, informationssökning och förståelse kan vara problematiska (Johansson et al., 2020).

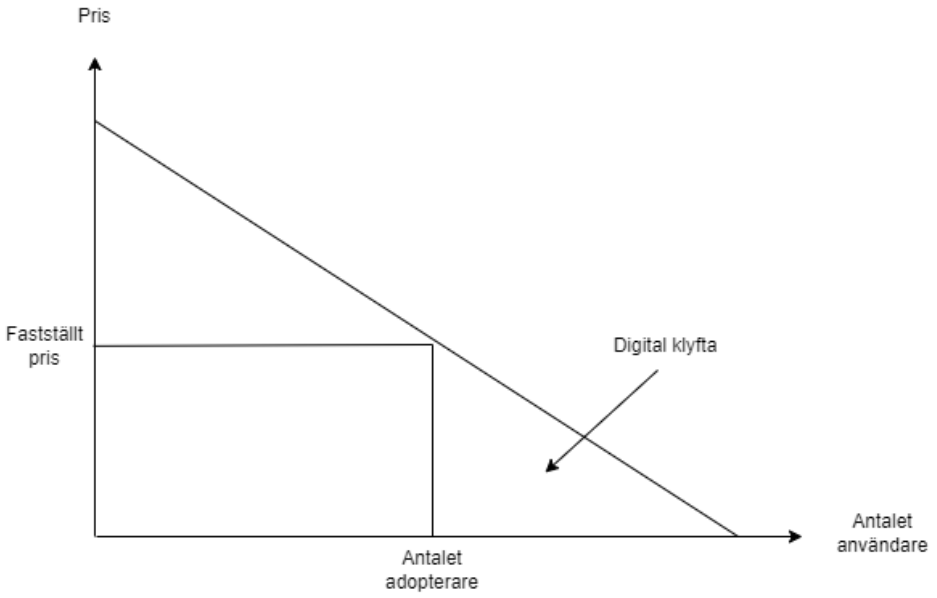
Utbildning som en person besitter är en av faktorerna som påverkar klyftan där det anses att digital utbildning av tjänster som tillhandahålls i och med e-förvaltning kan vara ett viktigt moment för att minska teknisk ojämlikhet (Lythreatis et al., 2021). Den äldre generationen som vanligtvis hamnar utanför digitaliseringen kan istället bli övertalade samt få stöd av familj eller vänner till adoption av olika digitala procedurer och därmed bli inkluderade (Friemel, 2016).

Den ekonomiska aspekten kan kopplas an till Martens (2018) och visualiseras i figur 2 där det fastställda priset blir en förutsättning för storleken på den högra triangeln som av

ekonomiska skäl inte väljer att adoptera tekniken, antalet adopterare på x-axeln blir en direkt konsekvens av var organisationen fastställer priset på y-axeln.

Figur 2

Digital klyfta utifrån ekonomiska förutsättningar, omarbetad modell av Martens (2018, s.12)



Den digitala klyftan riktar sig oftast åt den enskilde personen. Enligt Shakina et al. (2021) kan fenomenen även observeras inom organisationer där klyftan främst bedrivs av brist på teknisk adoption och användning. I dessa fall är det viktigt att återigen investera i teknisk utbildning parallellt med teknisk adoption och bedriva politik som främjar adoption av ny teknik (Shakina et al., 2021).

3.3 Om identifieringsprocessen; från identifiering till autentisering

Elektronisk identifiering spelar en stor roll inom infrastrukturer för e-förvaltning och e-handel. En privatperson anskaffar sig en mängd olika identifieringar i syfte att delta i olika tjänster och för att representera sig själv symboliskt (Beynon-Davies, 2006). Denna mångfald manifesteras när identifikation genomförts med analoga medier som exempelvis ett pass, ett nationellt ID-kort, eller körkort (Polisen, 2020) och kompenseras i Sverige med elektronisk identifiering som exempelvis BankID (Finansiell ID-Teknik BID AB, 2023a). En konsekvens av detta blir när den privata personen interagerar med offentlig sektor och tar nytta av privat sektor; identifieringen möjliggör tillgång till social handling och tjänster (Beynon-Davies,

2006). Identifiering krävs exempelvis vid olika offentliga registreringar och procedurer hos myndigheter och olika betalningar i webbaserade lösningar kräver numera BankID eller liknande alternativ i Sverige.

Processen av identifiering konceptualiseras enligt Beynon-Davies (2006) genom en modell som består av tre relaterade faktorer som är autentisering, identifikation och deltagning (eng. enrolment) som kopplar samman IT och mänskliga aktiviteter i sociala kontexter.

Autentisering besvarar frågan "är jag den jag påstår att vara?" som resulterar i en identifiering och bekräftelse av personens identitet; detta är möjligt genom att jämföra relationen mellan identifierare och person. Identitet (förutom att utpeka en form av en persons individualism) tar form av en mångfald av identifierare som utpekar egenskaper som observeras eller tilldelas till en viss person eller entitet. Identifierare kan ta form av den naturliga/biometriska eller artificiella typen och överlag ses som känslig information (Ohm, 2015). Fysiskt utseende, beteende eller mer specifika fysiologiska beståndsdelar (fingeravtryck, iris) är av den naturliga/biometriska typen medan koder eller övrigt bevis (serienummer, pass, email adress) är av artificiell typ (Beynon-Davies, 2006). Identifiering besvaras genom praktiska tillvägagångssätt av förbestämda processer för hur en identitet bör identifieras med identifierare. Om identifieringen lyckas resulterar processen i att en person deltar i olika sociala sammanhang för olika syften.

Den generella identifieringsprocessen behandlas genom att först identifiera personen med hjälp av identifierare som autentiseras och resulterar i att personen deltar i ett större socialt sammanhang. Skapande av identifiering sker istället genom att först autentisera en identitet för att sedan bilda identifierare (Beynon-Davies, 2006); alltså i många fall behöver personen redan inneha konstruerade och giltiga identifierare.

3.3.1 Delning av känslig information

En av konsekvenserna när en medborgare elektroniskt identifierar sig är att individen avslöjar känslig information och att det skapar integritetsdilemman (Naumann & Hogben, 2008; Taddei & Contena, 2013). Avslöjande som fenomen i en digital miljö kan argumenteras vara en nutida norm eftersom det delas frivilligt känslig information som exempelvis realtid, situation och plats på sociala medier, bankkontonummer och bostadsplats ges ut vid elektroniska betalningar och är obligatoriskt inom offentliga tjänster och processer (Lee et al., 2013; Taddei & Contena, 2013). Avslöjningen har att göra med hur mycket information som

delas och informationens känslighet i form av olika typer av identifierare (Beynon-Davies, 2006; Taddei & Contena, 2013). Definitionen av känslig information är nära kopplad till de olika konsekvenserna som kan ske när informationen hamnar i "fel händer" och har en informell konnotation inom olika organisatoriska sammanhang; om informationen hamnar i fel händer och det riskerar att uppstå negativa konsekvenser är det känslig information. Informationens känslighet kan ses som något kontextuellt; vid konventionella elektroniska betalningar av varor kan en identifierare som ett serienummer av ett pass anses mycket sensitivt men inte vid köp av flygbiljetter (Ohm, 2015).

Konceptualisering och kategorisering av känslig information är problematiskt eftersom det inte finns tydliga ramverk för vad som klassificeras som känslig information; generellt är det ett resultat av olika styrande konstruktioner, lagar eller är underhållen av sociala relationer (Thompson & Kaarst-Brown, 2005). Övergripande konsekvenser av avslöjningen av känslig information bortom kontexten som den är avslöjad i är att det kan leda till vinst eller förlust av tillgångar och fördelar för olika intressenter alternativt leda till att en individ blir generad, stigmatiserad eller innebära livsförändringar (Thompson & Kaarst-Brown, 2005).

Behovet av avslöjandet behandlar en process där risk och vinst uppvägs av användare inom olika e-tjänster vilket resulterar i att användare ofta avslöjar information trots uppfattad risk i kontexten (Gerber et al., 2018; Robinson, 2017). Anledningen till att användaren avslöjar känslig information har olika förklaringar och kan förklaras utifrån olika perspektiv. Från ett ekonomiskt perspektiv kan det förklaras att användaren kan inneha en uppfattning om att förmåner ökar och maximeras vilket överväger potentiella integritetsdilemman (Gerber et al., 2018); medan från ett psykologiskt perspektiv kan det förklaras att användaren bedrivs av kognitiva fördomar och kontextuell rationalisering där den över- eller underskattar fördelarna eller konsekvenserna då individen bearbetar en begränsad mängd av information och har (eller har brist på) personliga erfarenheter (Gerber et al., 2018). Vidare förklaringar kan vara att individen är påtryckt av sociala faktorer (bekanta, kulturella eller att att andra människor gör det helt enkelt) till att handla enligt givna normer eller att avslöjandet av känslig information sker när det uppfattas kontroll över informationen genom att exempelvis bestämma hur den publiceras (Gerber et al., 2018). Vidare kontextuella faktorer som nationalitet och utbildningsnivå spelar störst roll om en individ avslöjar känslig information där de med lägre utbildningsnivå är mer villiga att avslöja känslig information (Robinson, 2017).

3.4 Elektronisk identifiering internationellt

På grund av nya utmaningar med elektronisk digital handel och säkerhet har allt fler länder valt att byta ut sina pappersbaserade ID-kort mot elektroniska (De Cock et al., 2006). Introduktionen av nationella elektroniska identifieringar har vuxit fram som trend runt om i världen, mer än hälften av medlemsstaterna i EU har redan, eller håller på, att introducera elektroniska ID-kort (Aichholzer & Strauß, 2010; Goodstadt et al., 2015) men även länder i Mellanöstern och Asien har börjat investera i elektronisk identifiering (Castro, 2011). Spridningen är inte heltäckande; vissa länder har inte ID-kort överhuvudtaget och bland de länder som har ID-kort så har inte alla elektroniska ID-kort (Goodstadt et al., 2015).

De flesta länders försök att introducera en nationell elektronisk identifiering faller dock inom kategorin mindre lyckade, alternativt misslyckade projekt (Goodstadt et al., 2015). Storbritanniens försök till en statlig elektronisk identifiering blev ett stort och kostligt projekt som inte ledde någonstans, internationella samarbetsinitiativ som D5 med syfte att lära av varandra etablerades dock som ett direkt resultat av misslyckandet (Anthes, 2015). Det har varit problematiskt att uppnå en komplett täckning av sina invånare med elektronisk identifiering där Estland kan anses vara en ledstjärna inom området där de sedan Sovjetunionens fall byggt upp ett digitaliserat samhälle (Anthes, 2015; Castro, 2011) men även andra länder såsom Hong Kong anses ha introducerat en lyckad elektronisk identifiering (Goodstadt et al., 2015). I Estland har medborgare till och med möjligheten att med hjälp av elektronisk identifiering deltaga i demokratiska processer som folkomröstningar (Castro, 2011).

Hur mottagliga befolkningen är till elektronisk identifiering skiljer sig från land till land. I Hong Kong har invånarna haft krav på att bära id-kort som ett bevis på att de var rättmätiga invånare sedan 1980-talet, övergången till en elektronisk identifiering i form av ett fysiskt kort ansågs på så sätt ganska naturligt (Goodstadt et al., 2015). I andra länder som Storbritannien har ID-kort använts under krigstider, något regeringen försökt fortsätta med även under fredstider men som inte har haft offentligt stöd då befolkningen starkt satte sig emot id-kort. Denna offentliga fientlighet mot ID-kort kan potentiellt kopplas an till Frankrikes historia där register tänkta att att minska ojämnställdheter i samhället istället kom att innebära svårigheter för invånarna att byta arbete (Goodstadt et al., 2015). Arbetarpartiet försökte i Storbritannien år 2006 att införa ett biometriskt elektroniskt ID-kort, något som resulterade i en diskussion om inte detta var en överträdelse av personliga rättigheter och

invånarnas frihet. Detta projektet lades ned fyra år senare vid ny regeringsbildning trots att biometri har möjlighet till att förenkla autentiseringsprocessen (Goodstadt et al., 2015; Lai et al., 2011). Österrike påbörjade år 1999 sitt projekt om elektronisk identifiering. Det var ett projekt i fyra faser som pågick fram till 2008; initiering, utveckling och policyutformning, implementering, samt utvärdering och användning (Aichholzer & Strauß, 2010). Österrikes lösning har lidit av en låg användningsgrad, något som Aichholzer och Strauß (2010) har brutit ned i tre delar. För det första var det aldrig något krav på användning, andra alternativ existerade parallellt och detta blev ytterligare ett alternativ i mängden. För det andra så var behovet till användning generellt ganska lågt; Österrikes invånare var sällan i behov av att identifiera sig digitalt. Anskaffning av elektronisk identifiering för att sedan knappt använda den är ett ofta återkommande mönster (Goodstadt et al., 2015). För det tredje så ställde lösningen ytterligare krav på användaren jämfört med andra alternativ med fler artefakter och moment i autentiseringsprocessen. Inför tillverkningen av sina kort gjorde de ett aktivt val att inkludera fler än en utfärdare i syfte att undvika en potentiell monopolsituation (Aichholzer & Strauß, 2010). Ser vi till vår egen historia med elektronisk identifiering i Sverige så har vi använt oss av elektronisk identifiering vid autentisering i olika myndighets- eller bankprocesser (Grönlund, 2010). Nedladdningsbar elektronisk identifiering på fil har varit mer populärt än den fysiska representationen på kort och är enligt Grönlund (2010) även något vi kan förvänta oss i framtiden.

Historiskt sett kan olika länders elektroniska identifieringssystem inom Europa karaktäriseras av att de besuttit en hög grad av diversitet, den ena var inte den andra lik (Aichholzer & Strauß, 2010). Flertalet länder har byggt upp en nationell infrastruktur för elektronisk identifiering för att stödja tjänster inom e-förvaltning och e-handel, dessa initiativ har vuxit fram på en nationell nivå utan att ha gränsöverskridande samarbete i åtanke och har resulterat i barriärer som bedriver dilemman som brist på interoperativa modeller, olika implikationer av samma modeller, lagstiftning som inte stödjer mål eller diverse kommunikationsbarriärer (Leitold, 2010; Ribeiro et al., 2018). Ett IT-system projekt som möjliggör internationella autentiseringar är STORK som utvecklades mellan Spanien och Österrike (Leitold, 2010; Ribeiro et al., 2018). Trots att STORK inte löser problematiken med lagliga barriärer som kan uppstå internationellt, gav projektet värdefull insyn i interoperativa och internationella modeller för nationer med personlig statlig eID. Modellen går ut på att inte bedriva nationella förändringar i infrastrukturen för eID; däremot krävs det centraliserade identifierare på en nationell nivå som uppnår diverse säkerhet och kvalitet över data för att sedan möjliggöra

tillgång till proxytjänster (eller PEPS, *eng.* Pan-European Proxy Service) (Leitold, 2010). Då STORK projektet bedriver säkerhet nationellt, menar vissa att det krävs en centraliserad infrastruktur för eID, medan andra att decentraliserade infrastrukturer för eID och e-förvaltning är säkrare (Anthes, 2015; Leitold, 2010). Trots att det kan finnas olika anledningar till varför de olika systemen skiljer sig så mycket åt är det en utmaning som inneburit problem vad gäller interoperabilitet mellan länderna (Aichholzer & Strauß, 2010).

Sedan september 2018 har eIDAS (electronic identification and trust services) förordningen varit obligatorisk för samtliga medlemsstater i EU, ett stort initiativ tänkt att ge nationella krav på internationella elektroniska identifieringar och förbättra interoperabiliteten mellan olika länders IT-system som hanterar elektroniska identifieringar (Lips et al., 2020; Tsakalakis et al., 2019). När offentlig likväl privat sektor erbjuder sina tjänster online och över landsgränser blir interoperabilitet av allra högsta vikt där en pålitlig digital autentisering är nödvändig. Trots att eIDAS är ett initiativ tänkt att förbättra interoperabiliteten mellan medlemsstaterna i EU är inte allt i förordningen självklart och det finns flera utmaningar ur olika perspektiv. Utifrån Nederländernas och Estlands implementeringar har ett flertal utmaningar kunnat identifieras vad gäller efterlevnad och tolkning av förordningen, olika praktiker hos olika medlemsstater, samarbete, samt hur juridiska personer företräds (Lips et al., 2020).

GDPR (eng. general data protection regulation) är en förordning av EU vars syfte är att både facilitera informationsutbyte av personlig data internationellt och säkerställa säkerheten av informationsägaren. Enligt Tsakalakis et al. (2019) erbjuder varken GDPR eller eIDAS någon specifik vägledning hur säkerheten ska säkerställas vilket lämnar rum för tolkning åt de som kontrollerar data.

3.6 Faktorer inför adoption av elektronisk identifiering för invånare

Generella faktorer som påverkar invånarnas och användares adoption av eID kan bland annat vara 1) enkel användning, 2) funktionalitet, 3) komplexitet, 4) kännedom (eng. awareness), 5) transparens, 6) integritet, 7) säkerhet och 8) kontroll och egenmakt (Tsap et al., 2019; Tsap et al., 2020).

Enkel användning som vidare kan konceptualiseras som bekvämlighet, användarvänlighet, användbarhet eller komfort (Tsap et al., 2019) är en faktor med bakgrund i TAM (technology

acceptance model) och berör användarens uppfattning av teknikens användbarhet och om den är enkel att bruka (Davis, 1989). Vidare handlar det om att e-förvaltning möjliggör och erbjuder tjänster som är grundade i medborgarens behov; där exempelvis offentliga tjänster är snabbare att utföra genom digitala medel, möjliggöra tjänster dygnet runt och att applikationer innehar lämplig struktur, navigering och effektiv processtruktur (Andermatt & Göldi, 2018).

Funktionalitet, nära knuten till uppfattning av användbarhet från TAM som berör tron att ett system förbättrar tillståndet (Davis, 1989), behandlar bland annat de olika möjligheter en applikation har att erbjuda som exempelvis typer av autentiseringsmetoder samt applikationernas tillgänglighet för medborgare (Tsap et al., 2020).

Komplexitet kontrasteras med enkel användning och utpekar att användare kan uppleva en procedur i en applikation och autentisering som något svårt att förstå och utföra, något som i sin tur kan resultera i uppfattning av tappad kontroll, förminskad motivation till att adoptera teknik och klagomål på användarens sida (Harbach et al., 2013). Mycket beror på användarens digitala kunnighet.

Kännedom och dess kontextuella synonymer som förståelse, uppfattning av applikationens syfte och funktioner eller kännedom av användning eller leverantör beror mycket på hur väl användare är informerad och kan ses som en temporär faktor som kan försvinna med tiden efter uppdateringar och förändringar som en applikation kan genomgå (Tiits et al., 2014; Tsap et al., 2019; Tsap et al., 2020).

Transparens enligt ett medborgarcentriskt perspektiv behandlar behovet av att data som skickas av medborgare för att samlas och bearbetas av en IT leverantör ska bli tillgänglig för medborgaren i syfte att medborgaren ska få medvetenhet av vad som händer med sin data (Tsap et al., 2019). Transparens innebär insikt för externa intressenter till tjänsterna och deras processer, hur data behandlas, och att göra olika datainsamlingar tillgängliga för att uppnå ansvarighet kring e-tjänsterna (Tsap et al., 2020; Twizeyimana & Andersson, 2019).

Integritet utpekar e-tjänsternas möjlighet till att erbjuda pålitlighet, tillit och säkerhet av data samt mjuk- och hårdvara (Tsap et al., 2019). Osäkerheten som uppstår på medborgarnas sida är i form av uppfattade risker samt rädslor och hot mot deras digitala identifikation (Tsap et al., 2020).

Kontroll och egenmakt innebär bland att medborgare har valmöjlighet att använda eID, vilken data som tillhandahålls åt en e-tjänst, datans status i e-tjänsten samt möjlighet till att återkalla data och till inkludering och deltagning som möjliggörs genom att informera medborgare och upprätthålla öppna och transparenta processer (Tsap et al., 2019; Twizeyimana & Andersson, 2019). Enligt Cuijpers & Schroers (2014) är det en avgörande faktor för medborgarnas egenmakt att kunna minimera data i processer inom e-tjänster och eID; enbart data som är nödvändig, lämplig och relevant bör efterfrågas och bearbetas.

E-förvaltning står framför många nyanserade och beroende av varandra faktorer som påverkar medborgarnas adoption av eID och därmed integrerar medborgare i digitala processer, och enligt Tsap et al. (2019) är tillit den mest framstående förutsättningen och kan argumenteras vara beroende av problematiken kring integritet, transparens och säkerhet. Övriga faktorer som anses bedriva adoption av eID och därmed som positiva karaktärsdrag av e-tjänster var enkel användning, funktionalitet, kännedom, kontroll och egenmakt, och transparens.

3.7 Sammanfattning av litteraturgenomgång

Sammanfattningsvis behandlar forskningsöversikten olika fenomen som digitalisering, e-förvaltning, digital klyfta, processen bakom autentisering, hur statlig eID har sett ut utomlands i EU och möjliga faktorer som bedriver adoption av eID. Digitalisering berör förändringar på individuell, social och industriell nivå och kräver homogenisering av teknik för att skapa värde för organisationer och samhälle. E-förvaltning som främst fokuserar på att skapa värde för den enskilda individen med hjälp av e-tjänster kan ses som ett politiskt drivet fenomen och kräver interorganisatorisk praktik och teknik. Både digitalisering och e-förvaltning ger oss en övergripande översikt av vad som bedriver förändringar och vilket syfte tekniken har för både enskilda individer och organisationer.

Den digitala klyftan lyfter upp att det kan finnas problematik till adoption av teknik på individuell nivå som bland annat är grundat i ekonomiska, politiska och subjektiva aspekter vilket ger oss möjliga utmaningar som en svensk statlig eID kan bemöta. Statlig eID utomlands har överlag haft liten framgång gällande utveckling och adoption när den väl försökt att introduceras vilket kan ge oss inblick i vidare utmaningar som en svensk statlig eID kan stå inför. De övergripande faktorer som möjligt bedriver adoption av eID är vidare

grundade i teknologiska och subjektiva aspekter och ger oss potentiella konceptualiseringar för vilka förutsättningar eID behöver inneha.

4. Empiri

4.1 Empirisk kontext; privata leverantörer till eIDAS

Elektronisk identifiering syftar till “en process inom vilken personidentifieringsuppgifter i elektronisk form, som unikt avser en fysisk eller juridisk person eller en fysisk person som företräder en juridisk person, används” enligt EU förordning 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och upphävande av direktiv 1993/93/EG; där personidentifieringsuppgifter definieras som “en uppsättning uppgifter som gör det möjligt att fastställa identiteten på en fysisk eller juridisk person eller en fysisk person som företräder en juridisk person”. Infrastrukturen i Sverige, likt EU förordningen om elektronisk identifiering, bygger på standarden ISO/IEC 29115 (Regeringskansliet, 2023).

Istället för att ha en statlig e-legitmationsutfärdare valde Sverige i början av 2000-talet en försörjningsmodell som bygger på att privata aktörer tillhandahåller e-legitimationslösningar (Myndigheten för digital förvaltning, 2021, 2023). I Sverige är tjänsten för eID, dess process och integration beroende av interorganisatoriskt samarbete där olika utfärdare av eID tillhandahåller tjänsten åt andra organisationer (myndigheter i vår kontext) till att bli integrerade i deras IT lösningar; exempelvis i en webbaserad lösning. År 2011 introducerades en avtalsmodell kallad valfrihetsystemet där offentlig sektor kan sluta avtal med flera leverantörer och låta användaren styra vilken av leverantörerna som används och får betalt utifrån de villkor som den ansvariga myndigheten har fastställt (E-delegationen, 2009; Myndigheten för digital förvaltning, 2023). Valfrihetssystemet möjliggjorde för enklare tillämpningar av fler e-legitimationslösningar i myndighetskontexter, detta då offentlig sektor på grund av ändringar i lagstiftning om offentlig upphandling inte får upphandla samma tjänst från olika leverantörer (Myndigheten för digital förvaltning, 2023; Utredningen om bildande av en e-legitimationsnämnd, 2010). I dagsläget har Digg ett ansvar att administrera så att e-legitimationsutfärdare och offentliga aktörer kan sluta avtal om e-legitimationstjänster; det pågår även lagförändringar som potentiellt är tänkt att ersätta lagen om valfrihetssystem med en ny lag om auktorisationssystem för e-legitimering och elektroniska meddelanden där den praktiska skillnaden för e-legitimering inte förväntas blir särskilt stor men nu även ska tillämpas på marknaden för digitala brevlådor mellan individen och en organisation (Myndigheten för digital förvaltning, 2021, 2023).

Trots att privata aktörer levererar e-legitimationslösningar som fungerar väl i dagsläget finns det ett behov av ett statligt ägt alternativ; flertalet statliga myndigheter samt Sveriges Kommuner och Regioner (SKR) har i över tio år påtalat avsaknaden av en e-legitimation på den högsta tillitsnivån (Myndigheten för digital förvaltning, 2023). Digg fick den 16 juni 2022 i regeringsuppdrag att ta fram ett förslag om en statlig e-legitimation (I2022/01335) och skriver i sitt förslag till regeringen att valet om privata aktörer anses ha haft god effekt och är en modell som är tänkt att fortsättas med även efter lansering av en statligt ägd eID lösning (Myndigheten för digital förvaltning, 2023). Förslaget om den statliga e-legitimationen är tänkt att vara ett komplement till redan existerande lösningar på marknaden och det främsta argumentet som lyfts genom åren är robusthetsperspektivet där den statliga lösningen ska vara tillgänglig även om andra alternativ inte är det (Myndigheten för digital förvaltning, 2023). Detta förslaget har sina rötter i ett slutbetänkande som lämnades in till Regeringskansliet av Utredningen om effektiv styrning av nationella digitala tjänster i december 2017, där vissa förslag kring en statlig e-legitimation har tagits vidare (Regeringskansliet, 2023).

En statlig eID kommer behöva möjliggöra för och stödja internationella identifieringar, där svensk statlig eID och utländska eID kan brukas internt nationellt och bortom Sveriges gränser (Myndigheten för digital förvaltning, 2021). Visionen är att dessa identifieringar ska möjliggöra olika transaktioner mellan länderna vilket är ett initiativ av EU-kommissionen och benämns under eIDAS förordningen. I Sverige samordnar och stödjer Digg elektronisk identifiering, ansvarar för infrastrukturen som möjliggör den och har i mål att främja användning av eID (Myndigheten för digital förvaltning, 2021). Samordningen, stödjandet och ansvaret sker genom att tillåta relevanta aktörer tillgång till infrastruktur och metadataregister som i sig behandlas först av Sweden Connect (styrs av Digg) men också delvis och i framtiden av eIDAS. Fortsättningsvis bedrivs olika kontinuerliga granskningsprocesser av eID utfärdare eftersom offentliga myndigheter själva ansvarar för sina egna e-tjänster, identifieringar och e-underskrifter som stöds av avtal med Digg. De utfärdare som uppfyller kraven och blir godkända av Digg får använda kvalitetsmärket “Svensk e-legitimation” och ses som en förutsättning för att delta i eIDAS-förordningen (Myndigheten för digital förvaltning, 2021). Processer för elektroniska identifieringar som granskas är ansökan om eID, dess utgivning och autentiseringar.

4.2 Förslag till svensk statlig eID; ID-kort och digital plånbok

Förslaget som Digg kom med angående en statlig eID är tvådelad, det är tänkt att du använder ett fysiskt identitetskort tillsammans med en digital enhet (Myndigheten för digital förvaltning, 2023). Förslaget som sådant innebär inte att användarna behöver låsa sig till en enhet på så sätt att den endast fungerar med en specifik enhet, utan är tänkt att vara enhetsoberoende där identifiering kan ske med vilken digital enhet som helst (Myndigheten för digital förvaltning, 2023). Respondent A nämner hur en sådan lösning har en styrka i att identifiering är möjligt även om en skulle förlora sin digitala enhet och har möjlighet att identifiera sig med en annan enhet, det ger fler möjligheter till användning. Kortet kommer till skillnad från andra aktörer på marknaden komma med en anskaffningskostnad, likt hur ett pass eller ID-kort har en anskaffningskostnad, men något pris är ännu inte fastställt (Myndigheten för digital förvaltning, 2023).

Parallellt med ID-kortet är också målet att utveckla en digital plånbok där en person kan samla sina dokument och attesteringar på ett och samma ställe. Detta är i syfte att skapa kontroll över informationsflödet inom varierande e-tjänster och samtidigt minska datainsamlingen av en person.

> Det här ska ske utan kontakt med utfärdaren. I dagens e-legitimation, när du loggar in i en e-tjänst med hjälp av din e-legitimation så loggar du egentligen in hos legitimationsutfärdaren. .... Plånboken kommer att fungera direkt mellan plånboken och e-tjänsten så att, så att legitimationsutfärdaren inte är inblandad i det där operativa skedet. (Respondent A)

> Det är du som avgör vilka attribut du släpper. .... Om du ska hyra en bil, så kanske det räcker med att släppa att du har körkort klass B. Att du har både A, B, C och D också, det har inte den där biluthyrningen med att göra. .... Du ska sätta användaren i förarsätet och den avgör vad den vill släppa. (Respondent A)

Med fokus på säkerhetsdimensionen möjliggör en digital plånbok att användaren bestämmer över vilken data som delges mottagaren, samt att kommunikationen kommer gå direkt mellan plånboken och tillhandahållaren av tjänsten där mellanparter som eID utfärdaren tas bort ur ekvationen helt och hållet. Utvecklingen av en digital identitetsplånbok sker nu i EU där en eID av högsta tillitsnivå kommer att vara ett krav för tillgång, Digg har föreslagit att den statliga e-legitimationen ska kunna användas till detta och har begärt att få i uppdrag att

påbörja utvecklingen för att kunna möta EU:s tidsplan (Myndigheten för digital förvaltning, 2023).

4.3 Myndigheternas perspektiv på eID och statlig eID

Anledning till det organisatoriska påtrycket till att externa personer adopterar och brukar eID är att myndigheter ser värde i att enskilda individen kan initiera behandlingar av ärenden, att den ska se hela sin kundbild vilket också möjliggör större kontroll av tjänsternas processer.

Myndigheter som adopterar eID tjänster från externa utfärdare har möjlighet att påverka hur deras användare tar sig till och från autentiseringsprocessen som eID erbjuder men påverkar inte processen inom själva eID eftersom den är utvecklad, driven och därmed är determinerad av eID utförare som i dagsläget är externa privata aktörer (Respondent D).

Organisationer som adopterar eID lösningar brukar det till en mångfald av syften där den främsta är att autentisera den rätta personen i en digital miljö för att sedan möjliggöra inloggningar som tillåter tillgång till individuella konton, till att signera sig för olika avtal och utföra varierande procedurer och tjänster. Generellt upplevs det från respondenterna att digitalisering och eID effektiviserar interna procedurer, att interna organisatoriska processer är beroende av eID till att hantera invånarnas ärenden och att det finns ett stort tryck till att bibehålla, vidare bruka, och att personer i Sverige adopterar eID.

Trots att många myndigheter i dagsläget erbjuder inloggning med flera olika alternativa eID sker 92% av inloggningarna till en av myndigheterna via Mobilt BankID (Respondent B); därmed kan vi anta att övriga processer som signering och generellt bruk av myndighetstjänster också huvudsakligen realiseras med hjälp av Mobilt BankID.

Alla respondenter som intervjuades nämnde att BankID brukas av sina användare inom deras respektive verksamheter. Anledningarna bakom den höga graden av användning av BankID är mångfaldiga. En organisation nämnde att privata aktörer (banker i detta fallet) utvecklar IT snabbare än den offentliga sektor (Respondent A) och övriga nämnde att just BankID var en av de första applikationerna på marknaden som ansågs lämplig för adoption inom den offentliga sfären. En respondent diskuterade att en möjlig anledning till den breda adoptionen och det vardagliga bruket av BankID är att det är den enda lösningen som möjliggör användning av andra applikationer som Swish och Kivra (Respondent B). Användarna blir därmed låsta till BankID för att bruka tjänster som dessa.

Anledningarna till varför en statlig eID inte ännu finns på marknaden diskuterades och reflekterades över tillsammans med respondenterna under intervjuerna. Det förekom under intervjuerna att det inte upplevs finnas ett behov av en statlig eID bland myndigheterna. Från ett myndighetsperspektiv anses inte en statlig eID som något akut, respondenterna argumenterar att de nuvarande eID lösningar från de privata utfärdarna anses tillräckliga. Däremot argumenteras av Respondent A och B att en statlig eID kan vara en möjlig lösning till att minska den digitala klyftan eftersom kraven på utgivningsprocessen av en eID blir bestämd av statlig entitet och att de därmed kan formalisera krav som är mer inkluderande. Ett nuvarande problem vid utgivningsprocessen av eID är att personer behöver redan befintliga identifierare som säkerställer deras identitet, något som kan anses problematiskt när vissa privata eID utfärdare inte anser att identifierare som samordningsnummer är tillräckliga och har krav på identifierare som exkluderar användare; där anser Respondent D att en statlig utfärdare kan lösa problemet och ha fler inkluderade krav som även är säkra för utgivningen av eID. Respondent B är av åsikt att Freja eID och AB Svenska Pass är bättre på att inkludera kunder än BankID, främst för att personen i fråga inte behöver vara en bankkund och Respondent D lyfter även hur Freja eID börjat med att erbjuda eID till kunder med styrkt samordningsnummer.

Avsaknaden av en statlig eID innebär för myndigheterna en ständigt överhängande risk när eID anses vara en samhällskritisk struktur som måste fungera dygnet runt, årets alla dagar. Att myndigheter och invånare är beroende av privata aktörer som kan säga upp sina avtal med staten, alternativt råka ut för problem som kan påverka dess tillgänglighet anses inte vara hållbart och gör sårbart (Myndigheten för digital förvaltning, 2023).

> Ur ett robusthetsperspektiv, att hela samhället bygger på att BankID fungerar, är inte heller OK. Vi måste liksom ha ett alternativ som man kan falla tillbaka till om, om nu BankID skulle få problem eller fattar ett affärsmässigt beslut om att nej, vi levererar inte längre till staten. (Respondent A)

Bakom dessa eID lösningar står privata utfärdare som drivs av sina respektive affärsintressen, något som ligger utanför statens kontroll. Dessa företag prioriterar inte alltid samhällets behov och har ingen plikt att fortsätta erbjuda sina tjänster i syfte att stödja samhällets olika myndighetstjänster, detta ansvaret ligger på staten.

Ett annat problem från ett myndighetsperspektiv gällande statlig eID är dess potentiella värde eftersom den riskerar att bli ytterligare ett alternativ i mängden som sällan kommer till bruk. Respondent B anser att det kan finnas problematik i att implementera en statlig eID på grund av låg användning från externa intressenter och brist på behov. Respondent A menar istället att en låg användning av statlig eID inte behöver vara något större problem eftersom den kan riktas åt de som exkluderas idag. Vidare påstår Respondent A att en statlig eID inte behöver konkurrera bort privata utfärdare eller har målsättningen att göra det, det finns värde i att ha kvar ett utbud av alternativ att välja mellan. Digg har sedan tidigare lämnat som förslag att samtliga enligt Digg godkända e-legitimationer ska kunna användas inom offentlig sektor och är av likartad åsikt att en statlig e-legitimation måste erbjudas som inloggningsalternativ inom offentlig sektor (Myndigheten för digital förvaltning, 2023); detta utreds även nu som en del av en större utredning kring säker och tillgänglig digital identitet (Dir. 2022:142).

Den statliga eID lösningen innebär en möjlighet för myndigheter att vara med och deltaga i utformningen av slutprodukten. Via remissförfarande har myndigheter möjlighet att lämna åsikter och tankar, men även via dialog med den statligt utsedda särskilda utredaren och via kontakt- och samarbetsytor tillsammans med Digg.

> Själva möjligheten att lämna synpunkter, den får vi ju formellt som myndighet utifrån det vanliga remissförfarandet. .... Sen är det så naturligtvis att vi alltid kan ha en underhållsdialog med utredaren. .... Vi har ju även som myndighet löpande dialog med myndigheten för digital förvaltning Digg ... där vi lämnar våra synpunkter via både samverkansforum och via kontaktytor som vi har. (Respondent C)

4.4 Diverse utmaningar

4.4.1 Säkerhet

Utvecklingen av en statlig eID måste sätta säkerhetsfrågor i fokus, Digg har dock inte i sitt förslag hunnit genomfört några fördjupade analyser avseende säkerhet. Säkerhetsfrågorna anses vara av yttersta vikt och i nästa steg bör detta tittas på (Myndigheten för digital förvaltning, 2023). Utöver säkerheten så är en av de allra största utmaningarna med elektronisk identifiering i dagsläget den digitala klyftan. Det nya statliga förslaget förväntas kunna bedriva en högre grad inkludering än nuvarande lösningar och minska den digitala klyftan, något som beräknas innebära en ökad användning av digitala tjänster inom såväl offentlig som privat sektor (Myndigheten för digital förvaltning, 2023).

Respondent B beskrev eID som en mycket kritisk process för både organisationer och för invånare samt påpekar att vissa invånare inte inser hur viktigt det är att kunna bruka eID för inloggningar och signeringar. Överlag anser respondenten att en person är mer sårbar under en digital autentisering än under en fysisk identifiering. Respondent B argumenterar att distansautentisering prioriteras och det fysiska mötet mellan person och myndighet blir av mindre intresse, något som har medfört att digitala bedrägerier numera har blivit normen över fysiska. En samhällelig förändring av digitaliseringen är försvinnandet av specifika myndighetskontor; istället uppkom det nationellt täckande initiativet Statens Servicecenter med servicecenter runtom i Sverige där diverse myndigheter centraliseras på en enda plats. I servicecenter är det möjligt att genomföra enklare kundprocedurer, som att ställa frågor och lämna åsikter åt de specifika myndigheterna där kundernas åsikter medieras vidare. Respondent B menar på att medborgare ska kunna besöka ett servicecenter för att få hjälp med sina ärenden och gjorde jämförelsen med ett smörgåsbord där allt finns serverat.

En av respondenterna diskuterade att graden av säkerhet som erbjuds av de olika utfärdarna av eID kan komma att påverka behörigheten och möjligheten till att utföra olika myndighetstjänster. Som det ser ut idag har behovet att överväga behörighetskrav om tillitsnivå (eng. Level of Assurance, förkortat LoA) bland svenska eID aktörer inte behövts göras eftersom samtliga uppnår tillitsnivå tre.

> Det är ju ett val vi inte har behövt göra, för det är ju liksom det enda alternativet som i praktiken har funnits på menyn. Tittar man istället framåt ... där folk på allvar kommer kunna använda LoA4 … och det är mina egna gissningar … det kanske ändå gör att vissa lite känsligare tjänster börjar överväga att ja, för att komma åt våran tjänst kanske det är relevant att kräva LoA4. (Respondent D)

Vissa tjänster och procedurer kan i framtiden komma att kräva en högre grad av säkerhet vid autentisering vilket gör det kritiskt att målsättningen kring tillitsnivåer när det gäller eID är så hög som möjligt så att den kan brukas till en stor variation av myndighetstjänster och inte bedriva en variation av digital klyfta.

Ett viktigt moment för utfärdandet av en e-legitimation är grundidentifieringen som sker i utgivningsprocessen av en eID, denna måste ske på ett noggrant och säkert sätt (Myndigheten för digital förvaltning, 2023). Grundidentifiering ska bland annat kräva behandling av biometriska personuppgifter såsom jämförelser av ansiktsbild och fingeravtryck med hjälp av teknik till att kontrollera identiteten hos den som ansöker om statlig eID. Förutom att

grundidentifieringsprocessen är ett förslag för Statens servicecenter är övriga förutsättningar som krävs för denna process ännu oklart.

4.4.2 Digital klyfta

Det är tydligt att myndigheter har som mål att inkludera så många individer som möjligt i deras tjänster. Alla myndigheter rapporterade problematiken med den digitala klyftan och att det finns personer som exkluderas på grund av att de inte adopterar eller har möjlighet att adoptera eID vilket beror på olika faktorer. I dagsläget, och generellt, krävs att personer i Sverige har personnummer för att kunna adoptera och bruka eID inom myndighetstjänster. BankID kräver även att en invånare är en bankkund vilket anses vidare bedriva en digital klyfta. Trots att det är möjligt att adoptera alternativa eID med ett samordningsnummer istället för ett personnummer (Freja eID möjliggör det) är många av myndigheternas olika system och processer konstruerade med personnummer i åtanke som ett resultat av tekniska och historiska orsaker. Det finns därmed fall där trots att en person som innehar en eID tack vare ett samordningsnummer fortfarande kan sakna tillgång till vissa offentliga tjänster. Att personer är folkbokförda och fått personnummer i Sverige (eller alternativt innehar ett samordningsnummer i vissa fall) är därmed en determinerande faktor till adoption av eID och bruk av myndighetstjänster. Övriga anledningar till exkludering är att det finns äldre målgrupper som inte är tekniskt kunniga, det kan röra sig om olika funktionsnedsättningar hos personer som problematiserar bruket av eID eller att användare brukar tjänsterna så sällan att de saknar kunskap att bruka dem. Fotandet av en QR-kod i samband med inloggning är ett exempel som innebar utmaningar för vissa användare då detta var något de inte stött på tidigare (Respondent C). Det finns idag över en miljon människor i Sverige som lever i ett digitalt utanförskap på grund av att de är digitalt exkluderade i sin avsaknad av e-legitimation (Myndigheten för digital förvaltning, 2023).

> Det finns ju en hel flora av tjänster hos oss som inte fungerar för någon annan än en person som har ett svenskt personnummer. .... Ett praktiskt hinder som skulle göra att en person med samordningsnummer är helt utan svensk identitet. De skulle ändå inte kunna använda den tjänsten, även om de faktiskt hade fått ett BankID. (Respondent D)

Det har etablerats en standardiserad infrastruktur för tillhandahållandet av e-underskrifter och eID tjänster med syfte att underlätta för de olika offentliga myndigheterna (Myndigheten för

digital förvaltning, 2021) men det saknas förvaltningsgemensamma digitala lösningar inom den offentliga sektorn, något som har lett till myndighetsspecifika lösningar som skiljer sig åt från varandra (Regeringskansliet, 2023). Avsaknaden av homogena lösningar kan anses vara en annan orsak till exkludering, speciellt bland sällananvändare eller målgrupper som inte är tekniskt kunniga.

Möjliga fördelar som myndigheterna ser med statlig eID är just större möjlighet till att inkludera de som tidigare haft problem med utfärdandet av eID. Respondent B talar även positivt till inkluderingen med en statlig eID på grund av möjligheten regeringen har att tvinga aktörer till att inkludera lösningen i deras standarduppsättning, något Digg även har med i sitt förslag att alla enligt Digg godkända e-legitimationslösningar ska erbjudas i valfrihetssystemet (Myndigheten för digital förvaltning, 2023). Det nya lagförslaget om auktorisationssystem hade inneburit att Digg tar över och sluter avtal med utfärdare om att ingå i valfrihetssystem istället för att varje enskilt upphandlande myndighet gör detta individuellt (Regeringskansliet, 2023), något som hade gett dem direkt kontroll att inkludera den statliga lösningen.

5. Analys

5.1 Överblick av rådande situation och utmaningar

Teman som identifierades från vårt givna analytiska ramverk och insamlade empiri är i form av olika relationer. Relationer kan ses som ett ontologiskt fenomen (Smith, 2003) vilket vidare kan ta form som ett socialt koncept av fenomen; exempelvis av en relation mellan agens, struktur och teknik (Giddens, 1984, Orlikowski, 1992). Då digitalisering är ett fenomen som påverkar många nivåer av processer, organisationer och samhällen (Introna & Ilharco, 2004; Klein & Myers, 1999; Parviainen et al, 2017; Smith, 2003) anser vi att det är lämpligt att urskilja och koncentrera oss på vissa avgränsningar av helheten; dessa aspekter är just olika relationer och fenomen mellan entiteter. Relationer som vi anser av vikt är relationer mellan 1) individ och IT (då den digitala klyftan var ett återkommande tema), 2) individ och organisation (eID medierar den enskilda individen i e-tjänster som möjliggör statliga och övriga procedurer) och 3) interorganisatoriska relationer (eID är reglerad av Digg och utvecklingen av statlig eID påverkas av eIDAS) (se tabell 1). Dessa relationer kan ses som de främsta förutsättningar till att eID bör användas och bedrivas. Inom dessa relationer kan det diskuteras fler förutsättningar som är kontextuella för relationen men också utmaningar inför eID och den statliga eID.

Tabell 1

Identifierade relationer

Relationer	**Konceptuellt klargörande**
Individ och IT	En individ adopterar och använder digitala infrastrukturer och digitala enheter
Individ och organisation	Individ och organisation interagerar åt diverse syfte
Interorganisatorisk relation	Privat och offentlig sektor samarbetar och tekniskt integreras

5.2 Individ och IT

Det första identifierade temat är en relation mellan en individ och IT. Denna relation kan anses central i kontext med eID eftersom 1) eID är bunden till IT och 2) syftet med processen

av eID är att den enskilde individen självständigt ska digitalt autentisera sig i e-tjänster (Myndigheten för digital förvaltning, 2021, 2023; Regeringskansliet, 2023). Relationen kan även ses som en dualitet mellan agens och resurs där resurs är i form av IT och eID (Giddens, 1984; Orlikowski, 1992). Vidare kan IT resursen ses som ett medium mellan den enskilda individen och organisationen som skapar värde genom digitaliserad interaktion samt informationsutbyte i kontext med myndigheternas e-tjänster (Björkdahl, 2020). Myndigheter rapporterade problematiken i denna relation vilket är att en minoritet inte använder, har svårt att använda eller ser inte "poängen" med eID. Denna problematik kan vidare kopplas till digital klyfta (Friemel, 2016; Oakley 2010; Sparks, 2013; Tsap et al., 2019).

5.2.1 Adoption och användning av IT

En viktig förutsättning för individ och IT relationen (och att en eID används och autentisering realiseras) är att en individ adopterar teknik; detta kan ses som en konsekvens av digitalisering av offentlig förvaltning och att teknik kräver självreferering (Ebrahim & Irani, 2006; Henfridsson & Bygstad, 2013; Kaminski, 2011; Yoo et al., 2010a). Adoptionen av IT behöver ske både av en IT-enhet (hårdvara exempelvis i form av en mobiltelefon) men också av en applikation (mjukvara som exempelvis BankID-tjänsten). Samtidigt behöver individen befinna sig i en miljö med ytterligare digital infrastruktur i form av nätverk som möjliggör tillgång till internet. En ekonomisk förutsättning blir bland annat viktig eftersom den möjliggör anskaffning av IT-enheter och möjligtvis den framtida statliga eID-kortet (Friemel, 2016; Myndigheten för digital förvaltning, 2023). Det kan argumenteras att adoption av en IT-enhet är första steget för användning av eID eftersom IT-enheter skapar tillgång till IT-applikationer, leder till användning av e-tjänster och vidare till social deltagning (Beynon-Davies, 2006).

Utöver adoption av teknik och digital infrastruktur är värdefull användning av IT kritisk för relationen mellan individen och IT. Kunskap och medvetenhet om hur IT ska användas blir ett kritiskt moment för att uppnå fördelar som eID och e-tjänster möjliggör och erbjuder (Ebrahim & Irani, 2006; Lythreatis et al., 2021). En myndighet rapporterade att det kan vara brist på medvetenhet hos individer kring hur viktig eID är i deras e-tjänster och att brist på teknisk kompetens kan uppstå vid exempelvis användning av en QR-kod. Detta kan vara en konsekvens av att IT kan uppfattas och upplevas som komplex istället för något som är enkelt att använda (Davis, 1989; Harbach et al., 2013).

Därmed anser vi att teknisk adoption, användning och teknisk kompetens är viktiga förutsättningar inför bruk av eID i Sverige. Det kan vara problematiskt att på en bred skala säkerställa förutsättningar på en individuell nivå till att anskaffa och adoptera diverse teknik men också säkerställa kompetens av IT användning. Det kan ses som en kontinuerlig utmaning då individuella förutsättningar kan förändras och IT också generellt förändras över tid. Ekonomisk problematik kan förhindra anskaffning av IT-enheter som vidare förhindrar tillgång till IT-applikationer, autentisering och bruk av e-tjänster. Fortsättningsvis brist på teknisk kompetens, funktionsnedsättningar som försvårar bruk, hur IT används och en mer generell kunskap kring hur en individ kan uppnå fördelarna av IT och e-tjänster är vidare möjliga hinder.

5.2.2 IT-säkerhet och kontroll över informationsflöde

Säkerhetsfrågor är enligt Digg något som behöver sättas i fokus (Myndigheten för digital förvaltning, 2023), något vi även ser i flertalet tidigare studier kring elektronisk identifiering och integritet (Naumann & Hogben, 2008; Taddei & Contena, 2013; Tsap et al., 2020). En förutsättning för att kunna nyttja den digitala plånboken som är under utveckling i EU är en elektronisk identifiering av högsta tillitsnivå (Myndigheten för digital förvaltning, 2023), här har en statlig eID ett potentiellt användningsområde då de mest använda eID på marknaden idag inte uppfyller kravet om högsta tillitsnivå.

En förutsättning för adoption av eID är enskilda individens tillit och integritet för tekniken (Naumann & Hogben, 2008; Taddei & Contena, 2013; Tsap et al., 2019). För att uppnå tilliten kan det argumenteras att den digitala plånboken som är tänkt att minimera antalet aktör i informationsutbyte mellan plånboken och e-tjänsten omöjliggör för aktörer som exempelvis BankID att kartlägga användarbeteende genom att samla användarinformation vid bruk. Detta kan anses öka transparensen i informationsutbytet där individen får en bättre insikt i vilka aktörer som tar del av informationen och kan förminska organisationers möjligheter till att profilera individer då insamling av känslig information minimeras och individens integritet värderas (Aichholzer & Strauß, 2010; Cuijpers & Schroers, 2014; Yoo et al., 2010b). Utöver att användaren får en bättre insikt i vilken den mottagande parten är i informationsutbytet så främjar plånboken även agens och egenmakt genom att enskilde individen blir den drivande aktören i processer inom e-tjänster där denne själv väljer vilken data som delas och på så sätt kan anses vara i kontroll av informationsutbytet (Tsap et al., 2019). En risk i den digitala plånboken är att informationsutbytet kan komplicera processer i

e-tjänster vilken kan vara en utmaning att handskas med vid konstruktionen av den digitala plånboken (Andermatt & Göldi, 2018; Tsap et al., 2019).

Utmaningen är att på en subjektiv och individuell nivå inse värdet i den digitala plånboken för den enskilde individen (Parviainen et al., 2017). Kännedom av applikationens process för informationsutbyte kan ses som både en förutsättning och utmaning. Det elektroniska ID-kortet och den digitala plånboken kan resultera i en autentiserings- och informationsutbyteprocess som är mer komplex och som utifrån ett användarperspektiv upplevs som något komplicerat blir vidare utmaningar att fysiska artefakter och mjukvara är formade på ett som upplevs enkelt i användning. Samtidigt kan plånboken skapa en centralisering av känslig information vilket vidare kan bedriva utmaningar kring säkerhet.

En digital plånbok låst bakom en elektronisk identifiering av högsta tillitsnivå innebär ett ytterligare lager säkerhet som en fysisk plånbok saknar, om plånboken heller inte är enhetsberoende innebär det att stöld, borttappande, eller att ha glömt den digitala enheten inte omöjliggör åtkomst förutsatt att användaren har tillgång till en annan enhet. Även om en digital plånbok, likt en fysisk plånbok, är utsatt för fara så ser hotbilden och utmaningen med nya digitala säkerhetshot annorlunda ut, något som kommer att behöva analyseras noggrant för att utveckla en säker teknik. Den digitala plånboken är tänkt att centralisera och samla olika dokument och övrig information som kan ses känsligt på ett och samma ställe kopplade till en enskild individ; något som kan anses öka tillgängligheten för användaren inom e-tjänster men även potentiellt bli en säkerhetsfråga med all information på ett och samma ställe. Exakt hur en slutgiltig plånbok kommer att se ut återstår att se ut men frågor som dessa blir viktiga vid utveckling och en förutsättning för adoption och vidare användning.

5.2.3 Ekonomiska hinder

Att den digitala plånboken är låst bakom en elektronisk identifiering av högsta tillitsnivå innebär indirekt en ekonomisk tröskel för att ta del av och bruka tekniken. Om den statliga elektroniska identifieringen inte går att tillskansa sig gratis så kommer det att bedrivas en viss digital klyfta där antingen vissa människor inte anser sig ha råd att adoptera tekniken, medan andra inte är villiga att betala vad prissättningen för statlig elektronisk identifiering landar på. Digg har föreslagit att en avgift ska tas ut i samband med ansökan, någon exakt kostnad är varken föreslagen eller fastställd men de lyfter däremot att en lämplig utgångspunkt kan vara prissättningen för pass och id-kort (Myndigheten för digital förvaltning, 2023). I och med att målsättningen är en hög adoption riskerar ett för högt pris att avskräcka potentiella

användare, därav blir prissättningen en direkt konsekvens av efterfrågan. Användarnas betalningsvilja samt betalningsförmåga behöver därmed tas i beaktning vid fastställandet av avgiften. I och med ett fast pris så bedrivs en digital exkludering som en konsekvens av prissättningen; se figur 2. Genom att ta ut en avgift i samband med anskaffning så får kortet ett monetärt värde för användaren, något som bör resultera i att försiktighet vid hantering av kortet (Myndigheten för digital förvaltning, 2023). Utöver en avgift för anskaffning av den elektroniska identifieringen är ingenting sagt kring huruvida den digitala plånboken i sig kan komma att kosta något. Då det även finns ett hårdvarukrav i form av en digital enhet finns det klara ekonomiska förutsättningar för att kunna ta del av och bruka tekniken, något som onekligen kan anses bedriva den digitala klyfta (Friemel, 2016; Sparks, 2013).

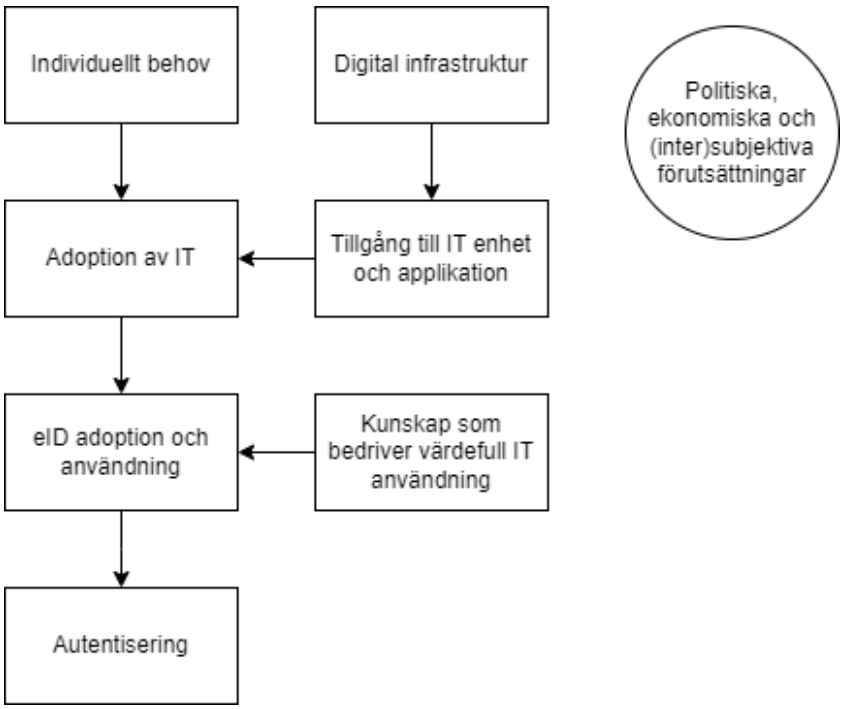
5.2.4 Potentiellt motstånd till det statliga förslaget

Genom att blicka utomlands och lära från andra nationers insatser vad gäller statlig eID så kan vi bland annat se att historisk kontext spelar roll och påverkar inställning till och adoption av elektronisk identifiering bland befolkningen. Ser vi till vår egen historia så har kortlösningar inte fått särskilt stor spridning i Sverige, majoriteten har föredragit alternativa enhetsberoende lösningar som BankID på fil och på senare år mobilt BankID (Grönlund, 2010). Att mobilt BankID fick så stor spridning anser vi potentiellt kan komma att förklaras genom att den påminner om BankID på fil med skillnaden att den digitala enheten gått från en personlig dator till en mobiltelefon. Den föreslagna lösningen kan anses som en radikal förändring (Kompella, 2017; Pardo & Tayi, 2007) på så sätt att den 1) går ifrån en marknadsdriven lösning, och 2) att den går emot vad som historiskt tycks ha föredragits i och med en kortbaserad lösning. Lik den digitala plånboken kan ID-kortet komplicera processer i e-tjänster och innebära något som inte är enkelt i användning (Davis, 1989; Tsap et al., 2019) Däremot att den kommer att kunna användas via mobiltelefon kan anses positivt. Österrikes förutsättningar i form av både ID-korts historia och populationsmängd kan anses vara likvärdig med Sverige. Jämför vi Diggs förslag mot Österrike som led av en låg användningsgrad så kan vi se stora likheter där de likt oss inte har något krav på användning och att andra alternativ finns tillgängliga parallellt, samt att ytterligare krav eller moment ställs på användaren i autentiseringsprocessen där ytterligare artefakter som ett fysiskt kort involveras. Den stora skillnaden här är att behovet för autentisering är större och att elektronisk identifiering sker mer ofta i Sverige jämfört med fallet i Österrike, något vi kan se i antalet transaktioner som genomförs med hjälp av bland annat BankID (Finansiell

ID-Teknik BID AB, 2023c). Utmaningen med ID-kortet och plånboken är därmed att på en individuell nivå skapa ett behov av adoption och användning.

Figur 3

Förutsättningar och utmaningar för relationen mellan individ och IT



5.3 Individ och organisation

De olika respondenterna delgav insikt kring problematiken när en individ inte adopterar eller inte kan använda IT och att det generellt är problematisk att bearbeta en individ utanför ett IT-system; därför kan det argumenteras att relationen mellan individ och IT är en viktig förutsättning till en fungerande relation mellan individ och organisation.

5.3.1 Organisation i en dynamisk miljö

Utifrån valfrihetssystemet, auktorisationssystemet och myndigheter att identifiering och autentisering är en kritisk procedur som kräver hög säkerhet för att minska bedrägerier; detta kan argumenteras kräva en hög grad av regulationer och standard. Då både IT och den sociala dimensionen dynamiskt förändras kan utmaningen hos utfärdare av eID, organisationer som adopterar eID i sina interna processer och myndigheter som reglerar detta vara att bedriva en viss adaption till förändrade omständigheter där IT standarder är tillåtna att bli omformade; särskilt när lag främjar individens åsikter (Regeringskansliet, 2023). I slutändan kan

utmaningen för organisationer och myndigheter vara att balansera strukturell standard och adoptiv praktik till sociala omständigheter.

5.3.2 Inkluderings- och integritetspolitik

Eftersom relationen mellan individ och organisation har digitaliserats blir generellt bruk av IT och eID en resurs som underhåller och möjliggör relationen i dagsläget (Björkdahl, 2020). Förutsättningar som realiserar detta är bland annat lag och politik där myndigheter bedriver och påtrycker till att utveckla IT-resurser för att sedan integrerar individen med IT, bedriver inkludering och möjliggör social deltagning för individen (Myndigheten för digital förvaltning, 2021, 2023; Regeringskansliet, 2023). Däremot kan det i praktiken bli utmanande att realisera lag och politik med tanke på den digitala klyftan och att det krävs diverse förutsättningar på individuell nivå till att adoptera och använda IT (Friemel, 2016; Sparks, 2013). Det kan finnas organisatoriska skäl till exkludering på grund av politiska och intersubjektiva koncept (Goodstadt et al., 2015). Politik som bedriver inkludering är en viktig förutsättning men också utmaning då dessa fenomen kan ses som dynamiska och ändrar sig över tid (Giddens, 1984; Orlikowski, 1992). Kontinuerlig politik som inkluderar diverse enskilda individer är av stor vikt vilket i sig kan skapa vidare utmaningar med att organisationer ska säkerställa kontinuerlig kännedom och medvetenhet av eID och e-tjänster för individer (Tiits et al., 2014; Tsap et al., 2019). Den främsta utmaningen är möjligtvis att relationen mellan individ och organisation behöver ha i åtanke båda parters förutsättningar och behov för en fungerande relation, vilket inte alltid fungerar i och med individens situation, politik eller organisatoriska påtryck.

Utöver inkluderingspolitik blir integritetspolitik av vikt. Trots att problematik kring individens integritet inte var något som lyftes fram under våra intervjuer är insamling av känslig information och dess organisatoriska bruk en förutsättning som möjliggör eID, övriga processer i e-tjänster och något som kan öka extern effektivitet mellan individ och organisation (Pardo & Tayi, 2007). Möjliga utmaningar med integritetsdilemman är att på en organisatorisk nivå skapa tillit hos enskilda individer som tar del av e-tjänster (Taddei & Contena, 2013; Tsap et al., 2019) vilket vidare kan kräva transparens kring hur känslig information hanteras och vad som händer med den efter avslöjandet (Tsap et al., 2020; Twizeyimana & Andersson, 2019). Detta kan vidare skapa utmaningar kring hur eID och e-tjänster ska kommunicera vad som har hänt med känslig information. En riktig transparens av känslig information kräver enligt oss lagstiftning och e-tjänster som stödjer transparens av

hur känslig information hanteras på den organisatoriska nivån för att skapa tillit för organisationer på individuell nivå.

Den organisatoriska medvetenheten kring att bedriva transparent hantering av känslig information verkar inte finnas på plats då detta inte går att explicit utläsas utifrån Diggs rapporter för den statliga eID trots att den digitala plånboken konceptuellt har möjlighet till en högre grad av individuell integritet (Myndigheten för digital förvaltning, 2021, 2023; Regeringskansliet, 2023). Samtidigt som den digitala plånboken kan skapa en större kontroll över informationsflödet för individen möjliggör den centralisering av en stor mängd känslig information vilket påtrycker behovet av säkerhet och att endast den behöriga har tillgång till den digitala plånboken.

Biometriska identifierare har stött på motstånd hos enskilda individer i exempelvis Storbritannien (Goodstadt et al., 2015) och utifrån våra intervjuer ansåg respondenterna att biometri i kontext med eID inte är en nödvändighet. Samtidigt diskuterades under intervjuerna att användning av biometri kan bedriva oönskade databaser med stora mängder av känslig information vilket kan ha långvariga konsekvenser om informationen skulle nå obehöriga (Lai et al., 2011). Däremot finns det enligt Digg ett behov för biometriska identifierare under grundidentifiering och för de som inte har en styrkt identitet i Sverige vilket gör biometri en viktig förutsättning för digital inkludering i vissa fall. Vidare kan den digitala plånboken innehålla dokument som innehåller biometrisk information. Detta skapar utmaningar på en organisatorisk nivå att bedriva säkerhet kring biometrisk information och undvika obehörig tillgång till dessa men också hantera problematiken om obehöriga får tillgång till informationen.

5.3.3 Digitaliserad interaktion

Lagen om valfrihetssystem och auktorisationssystem kan diskuteras främja individens agens i en digital miljö och vid användning av e-tjänster eftersom val av eID möjliggörs; individen bestämmer själv vilken eID som anses lämplig och därmed bedriver en form av individuell kontroll och egenmakt (Myndigheten för digital förvaltning, 2021; Orlikowski, 1992; Regeringskansliet, 2023; Tsap et al., 2019). Valfrihetssystem och auktorisationssystem kan diskutera påtrycka organisationer att 1) utvecklas utifrån individernas behov och 2) besvara individen om den upplever att en e-tjänst inte uppfyller krav vad gäller tillgänglighet är två faktorer som kan anses sträva efter att främja individens agens och egenmakt då lagförslaget möjliggör att den enskilda individen har möjlighet att påverka organisationens IT

(Regeringskansliet, 2023; Tsap et al., 2019). Valfrihetssystem och auktorisationssystem kan ses som regulativa politiska förutsättningar till en lämplig relation mellan individ och organisation där den enskilda individens behov blir utmaningar för organisationer att hantera.

Däremot kan det diskuteras att medan valfrihetssystemet och auktorisationssystemet bedriver och påtrycker den fortsatta digitalisering av interaktionen mellan en individ och organisation minskar detta individens agens under organisatoriska processer då dessa tar bort möjligheten till att bedriva mer komplexa procedurer under ett fysisk möte. Att processer går från analog till digital påverkar inte nödvändigtvis individens handlingsutrymme; digitalisering i sig innebär egentligen bara att formatet på handlingar och processer förändras. När processer digitaliseras så ökar dock problemen för de som exkluderas på grund av digitalisering och att IT inte adopteras eller används; för dem blir denna digitala interaktion problematisk. På ett sätt främjar e-tjänster individens agens då individen på egen hand kan utföra organisatoriska processer men ställer ytterligare krav på individen att adoptera och använder IT. Därmed blir förutsättningarna när organisationer digitaliseras att integrera individer men också att handskas med utmaningar för både enskilda individer och organisationer när individer inte integreras med teknik vilket återigen upplyser behovet av en fungerande relation mellan individ och IT. Fortsättningsvis blir utmaningen att forma IT på ett sätt som inte minskar individens agens och möjligheten att utföra processer inom e-tjänster.

5.3.4 Konsekvenser av identifierare och organisatoriska konstruktioner

Ett viktigt moment i relationen mellan individ och organisation är förutsättningar för eID. En förutsättning är att en individ innehar identifierare som anses giltiga enligt organisationer där personnummer och i vissa fall samordningsnummer är normen i Sverige. Eftersom Sverige valde en försörjningsmodell som går ut på att privat sektor ska tillhandahålla eID är ett exempel på en konsekvens i form av ett krav där en individ behöver vara en bankkund för att ansöka om BankID (Myndigheten för digital förvaltning, 2021); alltså förutom identifierare kan det finnas andra, relationella krav mellan individ och organisation under ansökan av ett eID. Utmaningen är att organisatoriska strukturer inte ska bedriva onödiga krav på individen och minimera behandling av individens känsliga information för identifiering med eID, statlig eID och i e-tjänster samtidigt som organisationerna säkerställer tillräckligt med information för att möjliggöra för individens sociala deltagning (Cuijpers och Schroers, 2014).

Eftersom personnummer eller samordningsnummer verkar vara en viktig förutsättning för utfärdandet av svensk eID kan det skapa problematik om en individ inte innehar dessa identifierare eller om en internationell individ inte har möjlighet till anskaffning av personnummer. Detta är en möjlig konsekvens av att svenska myndigheternas IT-system är strukturerade främst med personnummer i åtanke. Utmaningen i det är möjligen att IT-system är låsta till att endast behandla specifika identifierare och inte innehar förutsättningarna att vara alltäckande.

Personnummer eller samordningsnummer är däremot inte de enda förutsättningar i form av identifierare. Under en grundidentifikation som ska förstärka autentisering av en individ kan flera identifierare vara kritiska. Samtidigt som organisationer behöver bedriva strukturer eller standard kan det krävas av dem att vara adaptiva till diverse individer som både är bosatta i Sverige men också till internationellt bosatta individer (Tsap et al., 2019; Tsap et al., 2020; Twizeyimana & Andersson, 2019). Utmaningar är möjligtvis i form av att bedriva en önskad standard av vad gäller utfärdande, drift och säkerhet av eID (Myndigheten för digital förvaltning, 2021, 2023; Regeringskansliet, 2023) men samtidigt behovet av att vara adaptiv till sociala omständigheter med teknik (Kallinikos et al., 2013; Orlikowski, 1992). En nackdel med standarden kan vara att den bedriver en inlåsning på hur procedurer ska genomföras och därmed bedriver deterministiska konsekvenser på bekostnad av individens agens; den enskilde individen behöver anpassas till organisatoriska mönster och behov vilket kan leda till exkludering.

Digg anser att grundidentifieringsprocessen ska kräva en fysisk och personlig inställelse hos en myndighet som har i uppgift att genomföra processen (Myndigheten för digital förvaltning, 2023). Med tanke på att det fysiska besöket kan bli viktigt och uppkomsten av Statens servicecenter kan det diskuteras att det organisatoriska beroendet av IT och e-förvaltning kräver komplettering i form av fysiska besök. Den fysiska processen av grundidentifiering kan ses som ett exempel där det är inte lämpligt att digitalisera. En utmaning för organisationer kan bli att “på nytt” introducera det fysiska mötet mellan individen och en organisation och att göra Statens servicecenter till en värdefull plats där individer kan utföra mer komplexa procedurer till att möjliggöra socialt deltagande.

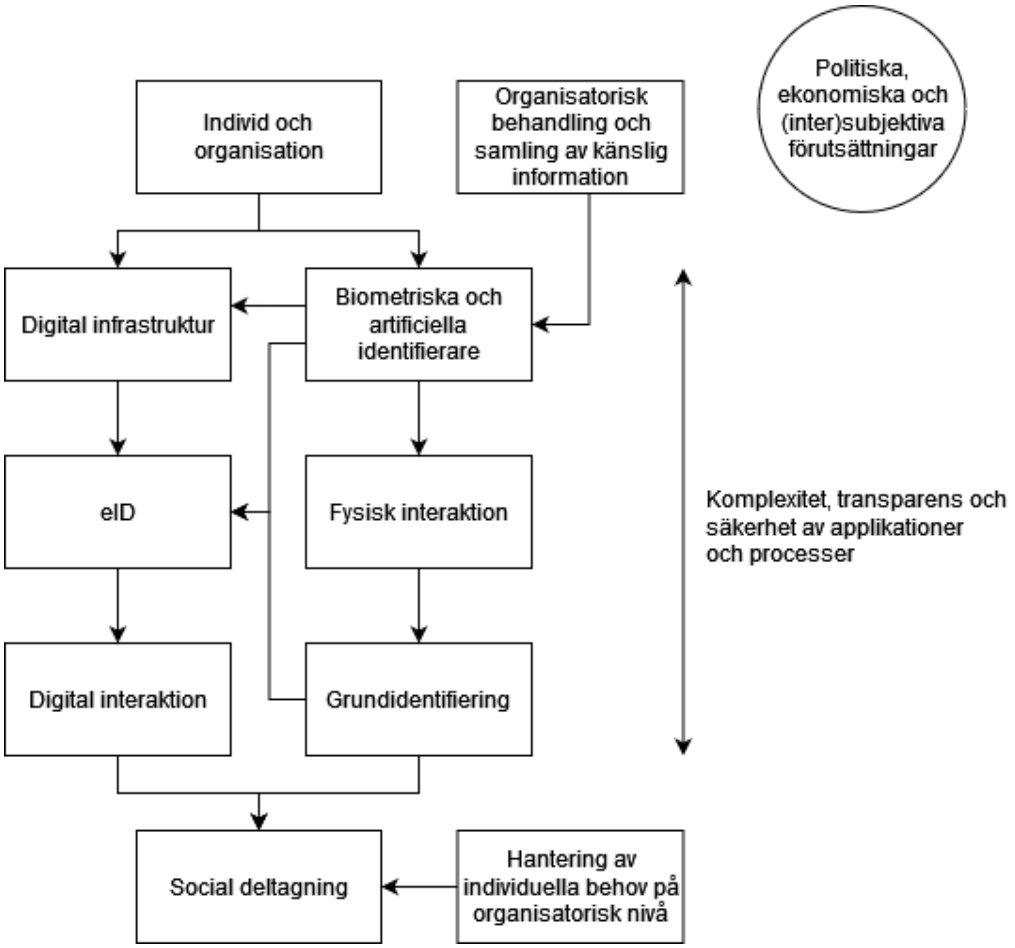
5.3.5 Slutliga utmaningar med ID-kort och digital plånbok

Konceptet av en svensk statlig eID innebär bland annat att introducera ett fysiskt ID-kort och en digital plånbok. Utmaningar med dessa kan vara att både det fysiska eID-kortet och en

digital plånbok kan komma att göra processer av autentisering och informationsutbyte mellan enskilda individer och organisationer mer komplexa (Harbach et al., 2013; Tsap et al., 2019). Konceptet om en svensk statlig eID riskerar att introducera fler steg under processer för autentisering och informationsutbyte vilket organisationer som utvecklar dessa behöver handskas med och ha diverse enskilda individers förutsättningar i åtanke för att bedriva adoption av statlig eID och externt värde (Tsap et al., 2019; Twizeyimana & Andersson, 2019).

Figur 4

Processen och dess utmaningar i relationen mellan individen och organisation



Övergripligt handlar relationen mellan individ och organisation om att en individ behöver interagera med IT och en mängd olika organisationer, inneha giltiga identifierare och uppfylla olika krav i kontext med eID. Samtidigt behöver det finnas förutsättningar i form av digital infrastruktur som organiseras och möjliggör interaktion mellan individ och organisation. Sammanfattningsvis leder relationen till ett socialt deltagande där organisationer aktivt arbetar med hur en individ ska integreras i teknik och hur sociala värden bedrivs där eID är

en förutsättning för helheten (Beynon-Davies, 2006; Myndigheten för digital förvaltning, 2021; Twizeyimana & Andersson, 2019). Detta kräver först giltiga identifierare för att uppnå olika krav inför grundidentifiering och utfärdandet av eID från individens sida samt användning av IT (eller en fungerande relation mellan individ och IT). Därmed är relevanta utmaningar inför inkludering först kring användning av IT på en individuell nivå, vilka identifierare ska anses vara giltiga och individens innehavande av dessa samt hur processen av grundidentifiering ska struktureras i kontext med en statlig eID.

5.4 Interorganisatoriska relationer

De interorganisatoriska relationerna tar form av nationella interorganisatoriska relationer där exempelvis Digg bedriver diverse granskningsprocesser av utfärdare av eID eller där Sweden Connect erbjuder metadataregister för autentiseringar. Interorganisatoriska relationer är även internationella eftersom diverse regulationer av EU så som eIDAS och GDPR påverkar de svenska myndigheterna.

5.4.1 Internationella påtryck och krockar

Den generella utmaningen för statlig eID i Sverige är internationella påtryck från EU som är i form av GDPR och eIDAS. GDPR kan diskuteras gälla alla organisationer som behandlar känslig information i e-tjänster och utmaningar är att realisera regulationer såväl tekniskt som praktiskt (Poritsky et al., 2019). Förutsättningar för en statlig eID är de olika krav som eIDAS ställer. Dessa krav är bland annat att en svensk statlig eID ska fungera internationellt men innebär också att offentlig sektor i Sverige ska kunna hantera internationella eID och autentiseringar. Detta kan ställa utmaningar då svenska IT-system är baserade på personnummer och samordningsnummer medan internationella eID är uppbyggda kring andra identifierare och skiljer sig mellan olika länder. Fortsättningsvis är utmaningen med internationella eID att IT-system som stödjer autentiseringar (men troligtvis också e-tjänster som organisationer erbjuder) behöver bedriva hög grad av interoperabilitet men också att det kan uppstå krockar under autentisering och behörighet till information och organisatoriska processer på grund av heterogen politik, lagar och regulationer mellan länder. De praktiska utmaningarna blir att enskilda organisationer kommer kräva säkerställande av resurser i form av kompetens som kan realisera EU:s påtryck inom sina e-tjänster, organisatoriska strukturer men också innehar ekonomiska förutsättningar (Poritsky et al., 2019). Fortsättningsvis krävs det förutsättningar för lyckade interorganisatoriska samarbeten vilket kan kräva goda mänskliga relationer, språk och kommunikation (Kompella, 2017; Pardo & Tayi, 2007).

På en övergripande nivå är utmaningarna för den svenska eID organiseringen att hantera internationella eID, utveckla en statlig eID som kan användas i internationella IT-system och bedriva interorganisatorisk kommunikation (som kan vara transspråklig och kräva god tolkning).

5.4.2 Organisatorisk agens och e-tjänsternas konvergens

Valfrihetssystem och auktorisationssystem kan ses både som lagar och handlingar och skapar förutsättningar till att användare erbjuds diverse eID; detta kan driva den marknadsdrivna försörjningsmodell som Sverige valde i början av 2000-talet men skapar också möjlighet till att nya utfärdare introducerar nya eID. Detta kan fortsätta att bedriva den tekniska utvecklingen där den privata sektorn historiskt sett har varit i framkant utifrån våra intervjuer. Valfrihetssystemet och auktorisationssystemet kan diskuteras skapa organisatorisk agens där organisationer har möjlighet att innovera kring eID och vidare konkurrera på marknaden. En utmaning med valfrihetssystemet och auktorisationssystemet är att de kan bedriva påtryck på organisationer och att de behöver integrera en diversitet av eID i sina e-tjänster; om det inte sker kan det i sig bedriva en organisatorisk digital klyfta (Shakina et al., 2021). Det kan argumenteras att organisationer behöver bedriva konvergens i interna e-tjänster genom att integrera dessa med bland annat eID och bedriva något som upplevs bekvämt för användaren (Tsap et al., 2019; Yoo et al., 2010a).

Trots att valfrihetssystemet och auktorisationssystemet kan främja en diversitet av eID lösningar i organisationer anser vi inte att det alltid realiseras i praktiken. Organisationer som inte integrerar diverse eID kan skapa utmaningar för enskilda individer som inte innehar någon av de specifikt erbjudna lösningarna (Pardo & Tayi, 2007), något som hade kunnat lösas genom att gå vidare med Diggs förslag om att samtliga enligt Digg godkända e-legitimationer med tillräckligt hög tillitsnivå enligt lag ska inkluderas i offentlig verksamhet då detta skapar förutsättningar till integration (Myndigheten för digital förvaltning, 2023).

5.4.3 Interorganisatoriska relationer i kontext med centralisering- och decentraliseringfenomenen

En annan aspekt av interorganisatoriska relationer är att Digg har blivit ansvarig för att samordna, stödja och främja bruket av eID (Myndigheten för digital förvaltning, 2021). Detta manifesteras exempelvis genom delning av infrastruktur för metadataregister som erbjuds av

Sweden Connect för övriga relevanta organisationer. Detta kan vidare ses som en delning av resurser som stödjer interorganisatorisk relation, interoperabilitet av data och teknologisk konvergens när e-tjänster integrerar diverse eID (Kompella, 2017; Yoo et al., 2010b). Sweden Connect och deras metadataregister kan ses som en centralisering av tekniska resurser och data (Pardo & Tayi, 2007; Yoo et al., 2010a) och utgör en kritisk förutsättning för utfärdare av eID för att realisera utveckling och kontinuerligt bedriva användning av eID. Denna centralisering kan på ett sätt diskutera minska externa organisationers agens framöver då de inte självständigt kan driva processer som krävs för eID och påpekar behovet av organisatoriskt samarbete, beroende och teknisk självreferering (Pardo & Tayi, 2007; Yoo et al., 2010a). Samtidigt då autentiseringar är iakttagna som något som kräver hög säkerhet för att minska bedrägerier (Myndigheten för digital förvaltning, 2021, 2023; Regeringskansliet, 2023) kan vissa anse det fördelaktigt med att statligt centralisera förutsättningarna till eID processer om den offentliga sektorn på ett lämpligt och säkert sätt kan bedriva metadataregistret och individernas känsliga information (Beynon-Davies, 2006; Taddei & Contena, 2013). Samtidigt finns de som argumenterar att decentraliserade resurser och register är säkrare (Castro, 2011), förslag som den digitala plånboken som centraliserar dokument och därmed känslig information på ett och samma ställe har väckt en diskussion mellan lagstiftare och diverse integritetsaktivister huruvida det inte innebär ökade risker för identitetsstöld (Illing, 2022). Oberoende om centralisering eller decentralisering bedrivs så är utmaningen att organisationer som ansvarar för teknik som möjliggör eID och autentiseringar ses av den enskilda individen såväl som övriga organisationer som en pålitlig aktör till att hantera känslig information (Taddei & Contena, 2013; Pardo & Tayi, 2007) vilket vidare kan kräva transparens (Tsap et al., 2020; Twizeyimana & Andersson, 2019).

Vidare delgav Respondent D att en eID med låg tillitsnivå kan förminska möjligheterna en individ kan ha i en e-tjänst, om en tjänst innefattar känslig data krävs en eID av hög tillitsnivå. Detta skapar ännu en utmaning, samtidigt som organisationer strävar efter både interna och externa värden så får det inte bli på bekostnad av säkerheten med eID (Björkdahl, 2020; Myndigheten för digital förvaltning, 2023; Parviainen et al., 2017). Säkerheten i kontext med centralisering- kontra decentraliseringsfenomen kan vara en av utmaningarna inom interorganisatoriska relationer och strukturer (Anthes, 2015; Kerttula, 2015). Statliga och centraliserade autentiseringar ansågs säkrast av några, medan andra menar att det krävs decentraliserade tekniker och integration inom e-tjänster för säkerheten. Det kan ses som ett kontextuellt dilemma där olika nationer har olika förutsättningar. Då den sociala dimensionen

är dynamisk kan det tyckas att även teknik ska vara dynamisk; decentraliserad teknik kan då argumenteras vara lämplig då ett flertal organisationer bedriver samarbete och teknisk konvergens när e-tjänster integrerar med andra e-tjänster och undviker därmed en centraliserad organisation eller maktstruktur som innehåller alla resurser.

5.4.4 Transparens, kommunikation och relationer för organisatorisk granskning

Enligt GDPR är officiella utredningar av organisationer som behandlar känslig information ett viktigt moment (Poritsky et al., 2019). I Sverige är utfärdare av eID under granskning av Digg vilket enligt oss bedriver och påtrycker underhållningen av en standard och riskbedömningar, både av teknik men också av praktik; överlag uppvisar utredningar och granskningar ett behov på transparens av teknik, procedurer och handlingar vilket kan leda till interorganisatoriska konflikter (Kompella, 2017; Pardo & Tayi, 2007; Parviainen et al., 2017; Myndigheten för digital förvaltning, 2021). Då konflikter kan ses som något som främst utspelar sig mellan individer blir utmaningen att bedriva god kommunikation och relationer mellan organisationer (Lips et al., 2020).

Eftersom eID har blivit en samhällskritisk infrastruktur och att digital autentisering kan användas i många olika e-tjänster, blir en av utmaningar att just bedriva en kontinuerlig hög standard kring integration och procedurer av eID i en mängd organisationer och digitala miljöer. Den offentliga sektorns påtryck kan ses nödvändig då teknik har tendens att förändras över tid, möjligtvis bedriva disruptiva förändringar och att organisationer kan bedriva varierande praktik (Adler et al, 2022; Kallinikos et al, 2013; Kompella, 2017). Dessa förändringar har inte enbart med teknisk förändring att göra utan också tillämpning av nya lagar och regulationer; auktorisationssystem, valfrihetssystem och GDPR är exempel som utfärdare av eID i Sverige behöver hantera (Poritsky et al., 2019). De organisationer som är under granskning av Digg står inför utmaningen att vara transparenta vad gäller teknik, procedurer, handlingar och hur de kommuniceras på ett meningsfullt sätt.

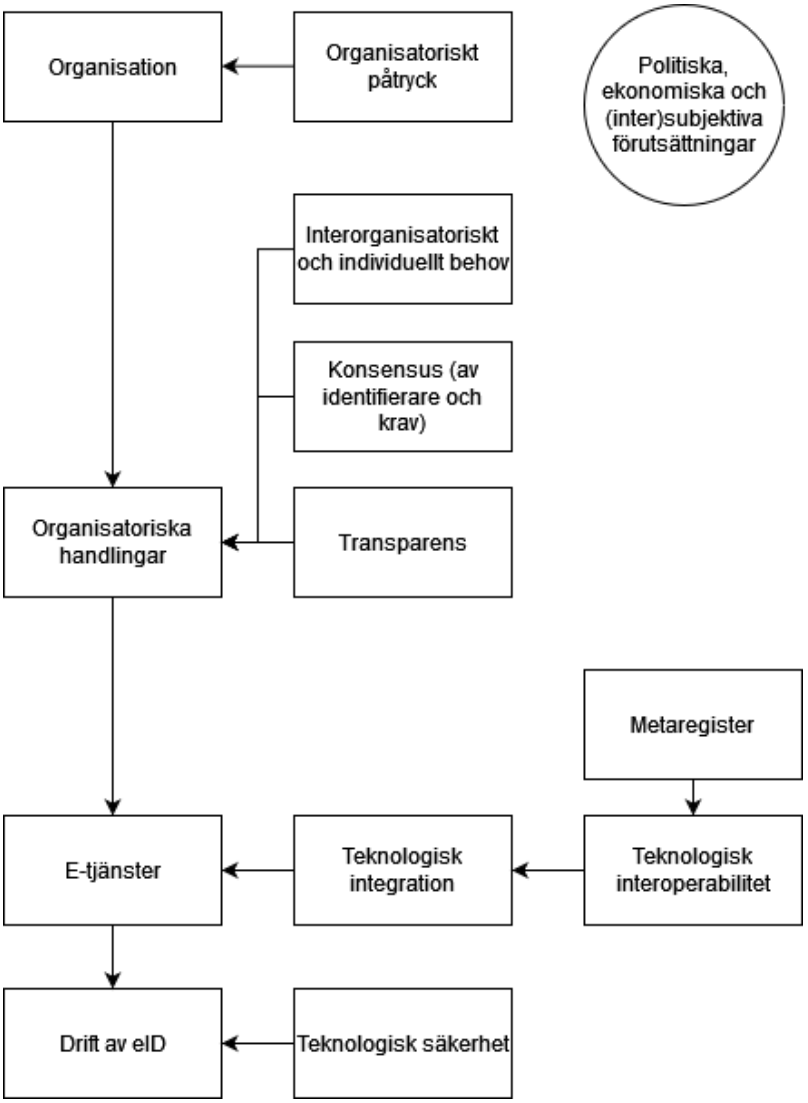
5.4.5 Interorganisatorisk konsensus av identifierare

Ännu en viktig utmaning i den interorganisatoriska relationen är att bedriva en konsensus över vilka identifierare och krav anses giltiga under både grundidentifiering, utfärdandet av eID och under internationella autentiseringar. I dagsläget kräver exempelvis BankID, utöver giltiga identifierare som personnummer, att en individ också är en bankkund. Detta utpekar

enligt oss att institutioner kan bedriva variationer och idiosynkratiska krav som ställs upp av organisatoriska interna skäl vilket har möjlighet att bedriva exkludering; i slutändan kan det komma att uppstå situationer där en individ behöver en specifik eID som den inte är behörig till eller har åtkomst till. Utmaningen blir att svenska organisationer behöver inneha tekniska förutsättningar som interoperabilitet och inte vara fastbunden till IT-system där personnummer eller samordningnummer är standard för bearbetning av enskilda individer.

Figur 5

Interorganisatoriska förutsättningar och utmaningar med eID



Även de nuvarande svenska myndigheternas IT-system som är baserade på personnummer eller samordningsnummer kan tyda på en teknisk och strukturell inlåsning och vara problematiska i längden om svenska myndigheter ska kunna bearbeta internationella eID alternativt ändrar hur vi bearbetar identifiering.

Vi anser att interorganisatoriska relationer som stöds av lag, politik och praktik är viktiga förutsättningar för vidare drift av eID och utveckling av en statlig eID. De främsta utmaningarna inom den interorganisatoriska relationen är utmaningen att främja utveckling av ett statligt eID i en social och teknisk miljö som redan använder och har integrerat en diversitet av olika eID i sina e-tjänster. Granskningar som Digg utför kan också bedriva utmaningar då proceduren kräver transparens av praktik och IT mellan Digg och utfärdare som granskas. Vidare kräver dessa granskningsprocesser att vara adaptiva till förändring då IT förändras snabbt. Konsensus över giltiga identifierare och krav inför grundidentifiering och utfärdande av eID är ännu ett moment som kräver vidare diskussion och formning mellan institutioner. I slutändan är kanske den största utmaningen att skapa ett behov av en statlig eID med tanke på att processer för autentiseringar redan existerar.

6. Slutsatser

Olika utmaningar med eID i Sverige har diskuterats. Dessa utmaningar har diskuterats utifrån tre perspektiv och relationer: individ och IT, individ och organisation, och interorganisatoriska relationer.

Förutsättning inom relationen mellan individ och IT är att individen behöver adoptera IT och befinna sig i en digital infrastruktur för att bli autentiserad inom organisatoriska processer och utöva social deltagning. Utöver tekniska förutsättningar krävs meningsfull användning av IT på individuell nivå som kräver teknologisk kunskap och kompetens, något som inte alltid finns. De främsta utmaningarna mellan individ och IT är att på en individuell nivå säkerställa tekniska förutsättningar och teknologisk kompetens. Ytterligare anledningar kan vara funktionsnedsättningar av olika slag som omöjliggör, alternativt försvårar, social deltagandet.

Utmaningar mellan individ och organisation är att främja individens agens samtidigt som det bedrivs strukturella och teknologiska standarder. Samtidigt som organisatoriska tjänster digitaliseras och bedriver teknologiska konsekvenser i form av teknisk självrefererande och digital klyfta, är utmaningen att integrera enskilda individer i digitaliseringen. I kontrast med digitalisering finns det förslag till fysiska möten mellan individen och organisationen; där är utmaningen att skapa förutsättningar till mer komplexa ärenden. Både i digital såväl som fysisk interaktion är utmaningen att inkludera en individ för socialt deltagande. En annan utmaning är att organisationer ska kunna hantera en diversitet med identifieringar som individer kan inneha och inte bli inlåsta på redan befintliga organisatoriska strukturer. Samtidigt blir utmaningen att minimalisera informationsutbytet mellan individ och organisation att endast innefatta nödvändig information, något som kan hjälpa till att främja integritet. Då anser vi att förslagen om ID-kort och digital plånbok kan innebära mer komplexa tekniska procedurer så blir ytterligare en utmaning att utveckla en lösning som upplevs enkelt i användning och att diverse individuella förutsättningar tas i åtanke. Organisatorisk och e-tjänsternas utveckling som är interaktiv, inkluderande, och som hanterar dynamiska förändringar på både organisatorisk och individuell nivå kan ses som den största utmaningen i relationen mellan individen och organisationen.

Utmaningar inom interorganisatoriska relationer är att bedriva samarbete, koncept och IT mellan heterogena organisatoriska, nationella och internationella strukturer. I Sverige är utmaningen för en statlig eID att handskas med konsekvenser av den marknadsdrivna

försörjningsmodellen för eID. Eftersom Digg har stor inverkan på externa organisationer är utmaningen att bedriva lämpliga granskningsprocesser av eID, bedriva interorganisatorisk transparens av handling och IT i syfte att identifiera problem men också bedriva politik som hanterar inkluderings- och integritetsfrågor. Resursdelning av metadataregister till lämpliga organisationer är vidare en förutsättning och något som kan skapa organisatoriska digitala klyftor om resursdelning inte realiseras.

Eftersom svensk statlig eID är under påtryck från EU kan det bedriva utmaningar då svenska organisationer behöver handskas med diverse krav från EU och eIDAS. Utmaningar där är bland annat hur förordningen tolkas där koncept av eIDAS är mångtolkade. Fortsättningsvis skapar det utmaningar med att IT-system behöver bedriva internationell interoperabilitet. Det kan finnas utmaningar i att bedriva en interorganisatorisk och nationell konsensus över vilka identifierare och krav som en individ behöver inneha och uppfylla för att möjliggöra processer inom e-tjänster. Kontextuella nationella lagar är ännu en utmaning som kan påverka internationella autentiseringar och processer inom e-tjänster.

Den generella utmaningen med utvecklingen och introduktionen av en statlig eID är att hitta behovet inom olika kontexter, exempelvis bland diverse målgrupper och organisationer. Eftersom BankID redan är en etablerad applikation bland befolkningen kan det finnas brist på behov av ytterligare eID. Det finns en risk att svensk statlig eID formas på grund av interorganisatoriska behov, något som kan innebära en risk då fokus försvinner från individer som är digitalt exkluderade i Sverige. En svensk statlig eID behöver utvecklas med allt detta i åtanke.

7. Reflektion/metodkritik

7.1 Reflektion kring undersökningsprocessen

Myndigheter som verkade vara insatta i eID frågor och som har adopterat diverse eID i sina interna organisatoriska strukturer var mer benägna att ställa upp till intervju. Detta kan ha bedrivit en konsekvens där den induktiva aspekten av studien har en bias av organisationer som lyckas med att integrera diverse eID i sina e-tjänster. Överlag skulle studien kräva fler iterationer av empiriinsamling där diverse åsikter från intervjuer kontrasteras med andra åsikter för att fördjupa möjlig problematik som kan uppstå med eID och statlig eID.

Undersökningsprocessen har endast kommit i kontakt med några förvaltningsmyndigheter som lyder under staten, den svenska staten består av många fler organisationer som även de hade kunnat ge goda insikter och vara till grund för en bredare empirisk datainsamling för studien. Empiri som fångar statliga aspekter kunde ha uppvisat ytterligare utmaningar av stor vikt. Fortsättningsvis exkluderade undersökningsprocessen privata organisationer vilket vidare kunde ge insyn med problematik kring eID och ge insyn i hur de ser på en statlig eID.

Vår undersökning kan diskuteras vara för generell eftersom den inte endast diskuterar en enda relation som exempelvis mellan individ och organisation. Istället för att bearbeta många identifierade problem och analysera både på en mikro- eller makronivå kunde ett mer reduktivt tillvägagångssätt vara lämpligt genom att koncentrera på endast en relation eller ett specifikt fenomen i kontext med eID. En konsekvens är att analysen bearbetar fenomen mycket generellt, diskuterar normativt och kan ses som något icke fördjupad eller nyanserat.

Därmed tycker vi att eID i sig är otillräckligt att diskutera och kräver kontextualisering; eID i sig har inget värde utan endast då eID används i en kontext med en annan organisatorisk process (exempelvis digitala transaktioner) skapar det mening. Fortsättningsvis anser vi att utveckling av statlig eID kräver strategi som handskas med en mycket bred utblick och att se med hjälp av diverse relationer som exempelvis mellan individ och IT, individ och organisation samt interorganisatoriska relationer blir kritiskt. En annan nackdel med resultatet är att de interorganisatoriska perspektivet inte inkluderades vilket i sig behöver mer kontextuella studier då en specifik organisation kan ses som något unik.

7.2 Reflektion kring resultatet

Då undersökningsprocessen och analysen bearbetade en variation av förutsättningar och utmaningar kopplade till eID och statlig eID kan resultatet av vår studie ses som ett generellt koncept som kan vara av vikt i den strategiska nivån för organisationer. Förutsättningar är bland annat de generella fenomen såsom individuella och organisatoriska behov och handling i kontext med IT. Dessa förutsättningar har vidare diverse utmaningar som hur adoption och användning ska realiseras på en individuell nivå, hur den enskilda individen ska bearbetas i organisatoriska processer och hur organisationer ska relateras och påverka varandra.

7.3 Reflektion utifrån kvalitetskriterier

7.3.1 Hermeneutiska cirkeln

Den hermeneutiska cirkeln i vår studie bestod av att empiri i form av intervjuer, dokument men också litteraturgranskning av akademisk litteratur gav insyn i fenomenet och organisatoriska praktiken av eID, statlig eID och dess mening. Det var en iterativ process där intervjuer och dokument granskades och analyserades mot den akademiska litteraturen.

7.3.2 Kontextualisering

I syfte att beskriva studiens kontext och hur den vuxit fram har vi dels avgränsat oss i kapitel 1.4, men även diskuterat den historiska bakgrunden till hur och varför vi idag har en marknadsdriven försörjningsmodell, generellt kring vår digitaliseringspolitik och varför elektronisk identifiering är viktig i ett digitalt samhälle.

7.3.3 Interaktion mellan forskaren och det som studeras

Om vi ser på den generella processen för utbyte av information med utgångspunkt i subjektiva tankar från informationsägaren så kodar denna ett meddelande i något form av medium, detta behöver sedan avkodas, eller tolkas, av mottagaren. Här sker ett brus, det vill säga skillnader mellan tolkning och budskap. I syfte att minska detta brus och skapa en intersubjektiv tolkning har vi i våra intervjuer arbetat med att återupprepa vad som sagts, försökt förklara hur vi tolkat det, och ställt följdfrågor till respondenterna. En fullkomligt intersubjektiv förståelse mellan parterna anser vi nog är svår, om inte omöjlig att uppnå vilket innebär viss risk för feltolkning.

7.3.4 Dialogiskt resonemang

Vi som forskare innehöll begränsad kunskap kring elektronisk identifiering som fenomen innan studiens start, något som inneburit att vi varit öppna för information. Vi studerade elektronisk identifiering som fenomen till viss grad innan vi genomförde våra intervjuer, viss kunskap ansågs nödvändigt för att kunna ta fram en aktuell intervjuguide och föra diskussion med våra respondenter; det huvudsakliga litterära arbetet har dock gjorts i efterhand. Vi anser att vår studie är abduktiv då det varit en iterativt, växelverkande process men på skalan mellan induktion och deduktion ligger vi närmre induktion. Det har inneburit att empirin med största sannolikhet har kommit att påverka hur vi tolkat litteraturen, likt hur en deduktiv studie med formade hypoteser med största sannolikhet hade kommit att påverka empirin. Även om digitalisering kan innebära nackdelar, är vi som forskare generellt positiva till samhällets digitala utveckling; något som riskerar att ha speglat sig i vår forskning.

7.3.5 Mångtolkning

Då interpretivistiska studier kan stöta på mångtolkning av ett och samma koncept försäkrade vi oss att vår egen tolkning av intervjuer är likartad med respondenterna både under och efter intervjuerna genom att fråga och undersöka deras tolkning. Samtidigt kontrasteras akademisk litteratur med diverse skribenter och artiklar av samma kontext.

7.3.6 Bias

Inför intervjuerna misstänkte vi att respondenterna skulle försöka porträttera sig själva i ett positivt ljus där de förringar svagheter och lyfter upp sina styrkor. De visade sig istället att de öppet diskuterade sina utmaningar och problem i verksamheterna i relation till de frågor som ställdes under intervjuerna.

Å andra sidan kan det diskuteras att både organisationer och dokument som studerats har ett visst bias och ett optimistiskt ställningstagande till digitalisering vilket kan bedriva praktik som inte handskar med den digitala klyftan och social ojämlikhet på ett lämpligt sätt.

7.4 Fortsatta studier

Fortsatta studier kring digital klyfta på både individuell och organisatorisk nivå kan vara fortsatt värdefulla studier. Dessa studier kan då handskas med tekniska- eller kunskapsklyftor som kan uppstå. Undersökningar av diverse fenomen som digitala enheter, applikationer, individuella förutsättningar och deras kontext som en del av empiri kan vara nyttiga moment

för mer rigorösa analyser kring digital klyfta. Syftet med dessa studier är att minska exkludering inom e-tjänster. I kontext med eID, fortsatta studier som undersöker exkludering av individer på grund av identifierare och organisatoriska krav kan vara av stort värde. Det kan även vara av värde att studera det fysiska mötet mellan individen och organisationen, och klargöra förutsättningar för detta för att sedan handskas med den digitala klyftan.

I Sverige kan det vara kritiskt att undersöka de olika statliga organisationer, strukturer, processer och aktörer som initierar utvecklingen av en statlig eID. Denna undersökning kan vara i syfte att vidare analysera nuläget, problematisera den och diskutera anledningar till varför utvecklingen av en statlig eID inte har realiserats.

En annan relevant organisation att undersöka kan vara Sweden Connect; denna aktör kan ge insyn till den tekniska infrastrukturen som eID i Sverige är beroende av. Undersökningar av Sweden Connect har möjlighet att studera teknisk och interorganisatorisk interoperabilitet möjligtvis på både nationell och internationell nivå.

Ett stort problem med eID är en diversitet av kontextuella och nationella lagar och därför kan fortsatta studier fokusera på internationella relationer och hur heterogena lagar kan handskas.

Fortsättningsvis kan det vara nyttigt för fortsatta studier att undersöka organisationer som inte adopterar diverse eID i sina e-tjänster och undersöka varför diverse eID inte integreras i organisatoriska e-tjänster.

Nya lagförslaget om auktorisationssystem kan ännu vara ett fördjupningsområde för vidare studier. Dessa studier kan då undersöka konsekvenser på teknik, e-tjänster samt konsekvenser på organisatorisk och individuell nivå.

Eftersom en statlig eID länge har varit ett koncept som inte realiserats kan mer pragmatiska studier som fokuserar på organisatoriska handlingsförslag bli av stort värde. Dessa studier skulle bland annat kräva hur organisatorisk praktik kan bedriva den tekniska utvecklingen av statlig eID och hur en statlig eID kan adopteras av enskilda individer.

I slutändan kan vidare studier fördjupa sig i konceptet av utmaningar inom olika kontexter och relationer; hur utmaningar uppstår, bedriver förändring och hur de hanteras.

Referenser

Adler, P. S., Adly, A., Armanios, D. E., Battilana, J., Bodrožić, Z., Clegg, S., Davis, G. F., Gartenberg, C., Glynn, M. A., Gümüsay, A. A., Haveman, H. A., Leonardi, P., Lounsbury, M., McGahan, A. M., Meyer, R., Phillips, N., & Sheppard-Jones, K. (2022). Authoritarianism, Populism, and the Global Retreat of Democracy: A Curated Discussion. *Journal of Management Inquiry*, *32*(1), 3–20. https://doi.org/10.1177/10564926221119395

Aichholzer, G., & Strauß, S. (2010). The austrian case: multi–card concept and the relationship between citizen ID and social security cards. *Identity in the Information Society*, *3*(1), 65–85. https://doi.org/10.1007/s12394-010-0048-9

Andermatt, K., & Göldi, R. (2018). Introducing an Electronic Identity: The Co-design Approach in the Canton of Schaffhausen. *Yearbook of Swiss Administrative Sciences*, *9*(1), 41–50. https://doi.org/10.5334/ssas.122

Anthes, G. (2015). Estonia: A Model for e-Government. *Communications of the ACM*, *58*(6), 18–20. https://doi.org/10.1145/2754951

Bannister, F., & Connolly, R. (2012). Defining e-Governance. *E-Service Journal*, *8*(2), 3–25. https://doi.org/10.2979/eservicej.8.2.3

Baskerville, R. L., Myers, M. D., & Yoo, Y. (2019). Digital First: The Ontological Reversal and New Challenges for IS Research. *MIS Quarterly*, *44*(2), 509–523. https://doi.org/10.25300/MISQ/2020/14418

Becker, J., & Niehaves, B. (2007). Epistemological perspectives on IS research: a framework for analysing and systematizing epistemological assumptions. *Information Systems Journal*, *17*(2), 197–214. https://doi.org/10.1111/j.1365-2575.2007.00234.x

Becker, H., & Geer, B. (1957). Participant observation and interviewing: A comparison. *Human Organization*, *16*(3), 28–32. https://doi.org/10.17730/humo.16.3.k687822132323013

Beynon-Davies, P. (2006). Personal identity management in the information polity: The case of the UK national identity card. *Information Polity*. https://doi.org/10.3233/ip-2006-0085

Björkdahl, J. (2020). Strategies for Digitalization in Manufacturing Firms. *California Management Review*, *62*(4), 17–36. https://doi.org/10.1177/0008125620920349

Bowen, G. A. (2009). Document Analysis as a Qualitative Research Method. *Qualitative Research Journal*, *9*(2), 27–40. https://doi.org/10.3316/qrj0902027

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Clark, T., Foster, L., Sloan, L., & Bryman, A. (2021). *Bryman's Social Research Methods* (6 uppl.). UK: Oxford University Press.

De Cock, D., Wolf, C., & Preneel, B. (2006). The Belgian Electronic Identity Card (Overview). I J. Dittmann (Red.), *Sicherheit 2005: Sicherheit - Schutz und Zuverlässigkeit*, *Beiträge der 3rd Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.v. (GI)* (Vol. P-77, 298–301). Gesellschaft für Information.

Cuijpers, C., & Schroers, J. (2014). eIDAS as guideline for the development of a pan European eID framework in FutureID. *Hühnlein, D. (Ed.), GI-Edition Lecture Notes in Informatics*, *2014*, 23–38.

Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *Management Information Systems Quarterly*, *13*(3), 319–340. https://doi.org/10.2307/249008

Dawes, S. S. (2008). The Evolution and Continuing Challenges of E-Governance. *Public Administration Review*, *68*, 86–102. https://doi.org/10.1111/j.1540-6210.2008.00981.x

Dobel, J. P. (2007). Public Management as Ethics. In *Social Science Research Network* (s. 156–181). Social Science Electronic Publishing. https://doi.org/10.1093/oxfordhb/9780199226443.003.0008

Ebrahim, Z., & Irani, Z. (2005). E‐government adoption: architecture and barriers. *Business Process Management Journal*, *11*(5), 589–611. https://doi.org/10.1108/14637150510619902

Feenberg, A. (2010). Ten Paradoxes of Technology. *Techné*, *14*(1), 3–15. https://doi.org/10.5840/techne20101412

Flyvbjerg, B. (2011). Case Study. I N. Denzin & Y. Lincoln (Red.), *The Sage Handbook of Qualitative Research* (4 uppl., s. 301–316). Sage.

Friemel, T. N. (2016). The digital divide has grown old: Determinants of a digital divide among seniors. *New Media & Society*, *18*(2), 313–331. https://doi.org/10.1177/1461444814538648

George, A. L., & Bennett, A. (2005). *Case Studies and Theory Development in the Social Sciences*. MIT Press (MA).

Gerber, N., Gerber, P., & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security*, *77*, 226–261. https://doi.org/10.1016/j.cose.2018.04.002

Gobble, M. M. (2018). Digitalization, Digitization, and Innovation. *Research-Technology Management*, *61*(4), 56–59. https://doi.org/10.1080/08956308.2018.1471280

Goldkuhl, G. (1996). Informatik - Ett ämne i, om och för förändring. Föreläsning Internationella Handelshögskolan, Högskolan i Jönköping [Föreläsning vid professorsinstallation]. 12 oktober 1996.

Goldkuhl, G. (2012). Pragmatism vs interpretivism in qualitative information systems research. *European Journal of Information Systems*, *21*(2), 135–146. https://doi.org/10.1057/ejis.2011.54

Goldkuhl, G. (2019). The Generation of Qualitative Data in Information Systems Research: The Diversity of Empirical Research Methods. *Communications of the Association for Information Systems*, *44*(28), 572–599. https://doi.org/10.17705/1CAIS.04428

Goldkuhl, G. (2022). Linguistic and Ontological Concept Formation: The LION Method. *The Qualitative Report*, *27*(12), 2715-2743. https://doi.org/10.46743/2160-3715/2022.5633

Goldkuhl, G. (2023). Theory as discourse for action - Conceptualization and theoretical statements [Opublicerat manuskript. Information systems and digitalization - Department of Management and Engineering]. Linköpings universitet.

Goodstadt, L. F., Connolly, R., & Bannister, F. (2015). The Hong Kong e-Identity Card: Examining the Reasons for Its Success When Other Cards Continue to Struggle. *Information Systems Management*, *32*(1), 72–80. https://doi.org/10.1080/10580530.2015.983025

Grönlund, Å. (2010). Electronic identity management in Sweden: governance of a market approach. *Identity in the Information Society*, *3*, 195-211. https://doi.org/10.1007/s12394-010-0043-1

Guzzini, S. (2005). The Concept of Power: a Constructivist Analysis. *Millennium: Journal of International Studies*, *33*(3), 495–521. https://doi.org/10.1177/03058298050330031301

Harbach, M., Fahl, S., Rieger, M., & Smith, M. R. (2013). On the Acceptance of Privacy-Preserving Authentication Technology: The Curious Case of National Identity Cards. *Lecture Notes in Computer Science*, 245–264. https://doi.org/10.1007/978-3-642-39077-7_13

Harvey-Jordan, S., & Long, S. (2001). The process and the pitfalls of semi-structured interviews, *Community practitioner*, *74*(6), 219–221.

Henfridsson, O., & Bygstad, B. (2013). The Generative Mechanisms of Digital Infrastructure Evolution. *Management Information Systems Quarterly*, *37*(3), 907–931. https://doi.org/10.25300/misq/2013/37.3.11

Hirst, P., & Norton, M. (1998). *Electronic Government*. https://researchbriefings.files.parliament.uk/documents/POST-PN-110/POST-PN-110.pdf

Hodder, I. (1994). The interpretation of documents and material culture. I N. Denzin & Y. Lincoln (Red.), *Handbook of qualitative research* (s. 393–402). Sage Publications.

Hoffman, D. D., Singh, M., & Prakash, C. (2015). The Interface Theory of Perception. *Psychonomic Bulletin & Review*, *22*(6), 1480–1506. https://doi.org/10.3758/s13423-015-0890-8

Igolkin, S., Zhilnikov, A., Gubertov, E., & Provotorov, I. (2020). Digitalization of Innovative Process: Evolution and Problems. *Conference Digital Economy*. https://doi.org/10.2991/aebmr.k.200730.046

Introna, L. D. & Ilharco, F. M. (2004). Phenomenology, Screens, and the World: A Journey with Husserl and Heidegger into Phenomenology. I R. Boland & R. Hirschheim (Red.), *Social Theory and Philosophy for Information Systems* (s. 56-102). Wiley.

Johansson, S., Gulliksen, J., & Gustavsson, C. (2020). Disability digital divide: the use of the internet, smartphones, computers and tablets among people with disabilities in Sweden. *Universal Access in the Information Society*, *20*(1), 105–120. https://doi.org/10.1007/s10209-020-00714-x

Jahnke, M. (2012). Revisiting Design as a Hermeneutic Practice: An Investigation of Paul Ricoeur's Critical Hermeneutics. *Design Issues*, *28*(2), 30–40. https://doi.org/10.1162/desi_a_00141

Jansson, T. (2015). *Agila Projektledningsmetoder och motivation - Varför man blir produktiv av att flytta lappar på en whiteboard.* [Doktorsavhandling, Karlstads universitet].

James, W. (1907). Pragmatism's Conception of Truth. *The Journal of Philosophy, Psychology and Scientific Methods*, *4*(6), 141–155. https://doi.org/10.2307/2012189

Kallinikos, J., Aaltonen, A., & Marton, A. (2013). The Ambivalent Ontology of Digital Artifacts. *Management Information Systems Quarterly*, *37*(2), 357–370. https://doi.org/10.25300/misq/2013/37.2.02

Kaminski, J. (2011). Diffusion of Innovation Theory. *Canadian Journal of Nursing Informatics*, *6*(2), 1–7. https://cjni.net/journal/?p=1444

Kesmodel, U. S. (2018). Cross-sectional studies - what are they good for? *Acta Obstetricia Et Gynecologica Scandinavica*, *97*(4), 388–393. https://doi.org/10.1111/aogs.13331

Kiger, M. E., & Varpio, L. (2020). Thematic analysis of qualitative data: AMEE Guide No. 131. *Medical Teacher*, *42*(8), 846–854. https://doi.org/10.1080/0142159X.2020.1755030

Klein, H. K., & Myers, M. D. (1999). A Set of Principles for Conducting and Evaluating Interpretive Field Studies in Information Systems. *Management Information Systems Quarterly*, *23*(1), 67–93. https://doi.org/10.2307/249410

Kompella, L. (2017). E-Governance systems as socio-technical transitions using multi-level perspective with case studies. *Technological Forecasting and Social Change*, *123*, 80–94. https://doi.org/10.1016/j.techfore.2017.06.024

Kvale, S., & Brinkmann, S. (2009). *InterViews: Learning the Craft of Qualitative Research Interviewing* (2 uppl.). Sage Publications.

Lai, L., Ho, S., & Poor, H. V. (2011). Privacy–Security Trade-Offs in Biometric Security Systems—Part I: Single Use Case. *IEEE Transactions on Information Forensics and Security*, *6*(1), 122–139. https://doi.org/10.1109/tifs.2010.2098872

Lee, A. S. (2004). Thinking about Social Theory and Philosophy for Information Systems. I R. Boland, & R. Hirschheim (Red.), *Social Theory and Philosophy for Information Systems* (s. 1-26). Wiley.

Lee, A. S., & Baskerville, R. L. (2003). Generalizing Generalizability in Information Systems Research. *Information Systems Research*, *14*(3), 221–243. https://doi.org/10.1287/isre.14.3.221.16560

Leitold, H. (2010). Challenges of eID Interoperability: The STORK Project. I *IFIP Advances in Information and Communication Technology* (s. 144–150). Springer Science+Business Media. https://doi.org/10.1007/978-3-642-20769-3_12

Lenk, K. (2002). Electronic service delivery—a driver of public sector modernization. *Information Polity*, *7*(2,3), 87-96. http://doi.org/10.3233/IP-2002-0009

Lips, S., Bharosa, N., & Draheim, D. (2020). eIDAS Implementation Challenges: The Case of Estonia and the Netherlands. I *Communications in computer and information science* (s. 75–89). Springer Science+Business Media. https://doi.org/10.1007/978-3-030-67238-6_6

Lockton, V. (2009). e-Government and identity management in British Columbia: implementation of the BCeID. [Doktorsavhandling, Simon Fraser University].

Loux, M. (2006). *Metaphysics: A Contemporary Introduction*. Routledge.

Lythreatis, S., El-Kassar, A., & Singh, S. (2021). The digital divide: A review and future research agenda. *Technological Forecasting and Social Change*, *175*, 1–11. https://doi.org/10.1016/j.techfore.2021.121359

Martens, B. (2018). *The impact of data access regimes on artificial intelligence and machine learning*. Digital Economy Working Paper. JRC Technical Reports.

Mathiassen, L. (2017). Designing Engaged Scholarship: From Real-World Problems to Research Publications. *Engaged Management ReView*, *1*(1). https://doi.org/10.28953/2375-8643.1000

Myers, M. D. (1997). Qualitative Research in Information Systems. *MIS Quarterly*, *21*(2), *Systems*, 241–242. https://doi.org/10.2307/249422

Mir, R., & Watson, A. T. (2000). Strategic management and the philosophy of science: the case for a constructivist methodology. *Strategic Management Journal*, *21*(9), 941–953. https://doi.org/10.1002/1097-0266(200009)21:9

Myers, M. D. (2004). Hermeneutics in Information Systems research. I R. Boland, & R. Hirschheim (Red.), *Social Theory and Philosophy for Information Systems* (s. 103-26). Wiley.

Naumann, I., & Hogben, G. (2008). Privacy features of European eID card specifications. *Network Security*, *2008*(8), 9–13. https://doi.org/10.1016/s1353-4858(08)70097-7

Tiits, M., Kalvet, T., & Mikko, K. (2014). Social acceptance of epassports. In *International Conference on Biometrics* (pp. 1–6). https://subs.emis.de/LNI/Proceedings/Proceedings230/15.pdf

Oakley, K. (2002). *What is e-governance?* (IP1(2002)9e). Council of Europe. https://www.coe.int/t/dgap/democracy/Activities/GGIS/E-governance/Work_of_egovernance_Committee/Kate_Oakley_eGovernance_en.asp

Ohm, P. (2015). Sensitive information. *Southern California Law Review*, *88*(5), 1125–1196.

Orlikowski, W. J. (1992). The Duality of Technology: Rethinking the Concept of Technology in Organizations. *Organization Science*, *3*(3), 398–427. https://doi.org/10.1287/orsc.3.3.398

Orlikowski, W. J., & Baroudi, J. J. (1991). Studying Information Technology in Organizations: Research Approaches and Assumptions. *Information Systems Research*, *2*(1), 1–28. https://doi.org/10.1287/isre.2.1.1

Orlikowski, W. J., & Iacono, C. S. (2001). Research Commentary: Desperately Seeking the "IT" in IT Research—A Call to Theorizing the IT Artifact. *Information Systems Research*, *12*(2), 121–134. https://doi.org/10.1287/isre.12.2.121.9700

Pardo, T. A., & Tayi, G. K. (2007). Interorganizational information integration: A key enabler for digital government. *Government Information Quarterly*, *24*(4), 691–715. https://doi.org/10.1016/j.giq.2007.08.004

Parida, V. (2018). Digitalization. I J. Frishammar & Å. Ericson (Red.), *Addressing Societal Challenges* (s. 23–38). Luleå University of Technology.

Parida, V., Sjödin, D., & Reim, W. (2019). Reviewing Literature on Digitalization, Business Model Innovation, and Sustainable Industry: Past Achievements and Future Promises. *Sustainability*, *11*(2), 391–408. https://doi.org/10.3390/su11020391

Parviainen, P., Tihinen, M., Kääriäinen, J., & Teppola, S. (2017). Tackling the digitalization challenge: how to benefit from digitalization in practice. *International Journal of Information Systems and Project Management*, *5*(1), 63–77. https://doi.org/10.12821/ijispm050104

Powell, A., Bryne, A., & Dailey, D. (2010). The Essential Internet: Digital Exclusion in Low-Income American Communities. *Policy & Internet*, *2*(2), 159–190. https://doi.org/10.2202/1944-2866.1058

Rennie, D. L. (2012). Qualitative research as methodical hermeneutics. *Psychological Methods*, *17*(3), 385–398. https://doi.org/10.1037/a0029250

Ribeiro, C. F., Leitold, H., Esposito, S., & Mitzam, D. (2018). STORK: a real, heterogeneous, large-scale eID management system. *International Journal of Information Security*, *17*(5), 569–585. https://doi.org/10.1007/s10207-017-0385-x

Robinson, C. (2017). Disclosure of personal data in ecommerce: A cross-national comparison of Estonia and the United States. *Telematics and Informatics*, *34*(2), 569–582. https://doi.org/10.1016/j.tele.2016.09.006

Saxena, K. (2005). Towards excellence in e‐governance. *International Journal of Public Sector Management*, *18*(6), 498–513. https://doi.org/10.1108/09513550510616733

Shakina, E., Parshakov, P., & Alsufiev, A. (2021). Rethinking the corporate digital divide: The complementarity of technologies and the demand for digital skills. *Technological Forecasting and Social Change*, *162*, 1–16. https://doi.org/10.1016/j.techfore.2020.120405

Sparks, C. (2013). What is the "Digital Divide" and why is it Important? *Javnost-the Public*, *20*(2), 27–46. https://doi.org/10.1080/13183222.2013.11009113

Söderström, F. (2017). *Introducing public sector eIDs: The power of actor's translations and institutional barriers*. [Licentiat-uppsats, Linköpings universitet]. DiVA. http://liu.diva-portal.org/smash/record.jsf?pid=diva2%3A1048744&dswid=-967

Smith, B. (2003). Ontology. Floridi, L (Red.), *The Blackwell Guide to the Philosophy of Computing and Information* (s. 155-166). Wiley-Blackwell.

Thompson, E. D., & Kaarst-Brown, M. L. (2005). Sensitive information: A review and research agenda. *Journal of the Association for Information Science and Technology*, *56*(3), 245–257. https://doi.org/10.1002/asi.20121

Tihinen, M., & Kääriäinen, J. (2016). *The Industrial Internet in Finland: on route to success?* VTT.

Tsap, V., Pappel, I., & Draheim, D. (2019). Factors Affecting e-ID Public Acceptance: A Literature Review. *Lecture Notes in Computer Science*, 176–188. https://doi.org/10.1007/978-3-030-27523-5_13

Tsap, V., Lips, S., & Draheim, D. (2020). eID Public Acceptance in Estonia: towards Understanding the Citizen. *International Conference on Digital Government Research*. https://doi.org/10.1145/3396956.3397009

Twizeyimana, J. D., & Andersson, A. (2019). The public value of E-Government – A literature review. *Government Information Quarterly*, *36*(2), 167–178. https://doi.org/10.1016/j.giq.2019.01.001

Qu, S. Q., & Dumay, J. (2011). The qualitative research interview. *Qualitative Research in Accounting & Management*, *8*(3), 238–264. https://doi.org/10.1108/11766091111162070

Saxena, K. (2005). Towards excellence in e‐governance. *International Journal of Public Sector Management*, *18*(6), 498–513. https://doi.org/10.1108/09513550510616733

Söderström, F. (2016). *Introducing public sector eIDs: The power of actors' translations and institutional barriers*. [Doktorsavhandling, Linköpings Universitet]. DiVA. https://doi.org/10.3384/diss.diva-132737

Taddei, S., & Contena, B. (2013). Privacy, trust and control: Which relationships with online self-disclosure? *Computers in Human Behavior*, *29*(3), 821–826. https://doi.org/10.1016/j.chb.2012.11.022

Yoo, Y., Henfridsson, O., & Lyytinen, K. (2010a). The New Organizing Logic of Digital Innovation: An Agenda for Information Systems Research. *Information Systems Research*, *21*(4), 724–735. https://doi.org/10.1287/isre.1100.0322

Yoo, Y., Lyytinen, K., Boland, R. J., & Berente, N., Gaskin, J., Schutz, Doug & Srinivasan, N. (2010b). The Next Wave of Digital Innovation: Opportunities and Challenges: A Report on the Research Workshop "Digital Challenges in Innovation Research." *Social Science Research Network*. https://doi.org/10.2139/ssrn.1622170

ANDRA KÄLLOR

ACM (2018). ACM *Code of Ethics and Professional Conduct*. https://acm.org/code-of-ethics

Castro, D. (15 september 2011). *Explaining International Leadership: Electronic Identification Systems*. The Information Technology & Innovation Foundation. https://itif.org/publications/2011/09/15/explaining-international-it-application-leadership-electronic-identification/

Consid. (6 mars 2018). *BankID vs Freja eID*. https://consid.se/blogg/bankid-vs-freja-eid/

Dir 2022:142. *Säker och tillgänglig digital identitet*. https://www.regeringen.se/rattsliga-dokument/kommittedirektiv/2022/12/saker-och-tillganglig-digital-identitet/

E-delegationen. (2009). *Strategi för myndigheternas arbete med e-förvaltning*. *Betänkande* (SOU 2009:84). Fritzes. https://www.regeringen.se/rattsliga-dokument/statens-offentliga-utredningar/2009/10/sou-200986-/

Finansiell ID-Teknik BID AB (2023a). *Om BankID*. https://www.bankid.com/privat/om-bankid

Finansiell ID-Teknik BID AB (2023b). *Vår historia*. https://www.bankid.com/om-oss/historia

Finansiell ID-Teknik BID AB (2023c) *Statistik.* https://www.bankid.com/om-oss/statistik

Illing, D. (21 april 2022). *Electronic Identity (eID): Government versus Privatization - A European / United States comparison*. Ultimaco. https://utimaco.com/current-topics/blog/electronic-identity-government-vs-privatization

Merriam-Webster. (4 mars 2023). *Case study*. https://www.merriam-webster.com/dictionary/case%20study

Myndigheten för digital förvaltning (2023). *En säker och tillgänglig statlig e-legitimation - Slutredovisning av regeringsuppdrag att föreslå hur en statlig e-legitimation kan utformas (I2022/01335)*. Myndigheten för digital förvaltning. https://www.digg.se/download/18.5b30ce7218475cd9ed3ee0e/1675088054155/en-saker-och-tillganglig-statlig-e-legitimation.pdf

Utredningen om bildande av en e-legitimationsnämnd. (2010). *E-legitimationsnämnden och Svensk e-legitimation*. *Slutbetänkande* (SOU 2010:104). Fritzes. https://www.regeringen.se/rattsliga-dokument/statens-offentliga-utredningar/2010/12/sou-2010104/

Polisen. (29 juni 2020). *Giltiga id-handlingar när du ansöker om pass eller nationellt id-kort*. https://polisen.se/tjanster-tillstand/pass-och-nationellt-id-kort/giltiga-id-handlingar/

Regeringskansliet (2023). *Auktorisationssystem för elektronisk identifiering och för digital post*. https://www.regeringen.se/rattsliga-dokument/lagradsremiss/2023/02/auktorisationssystem-for-elektronisk-identifiering-och-for-digital-post/

Bilagor

Bilaga 1 – Intervjuguide

Datum: [datum]
Tid: [tid]
Plats: Digitalt, Teams
Respondent: [namn, roll]
Intervjuare: [namn]
Sekreterare: [namn]

Intro
Vi studerar på masterprogrammet IT & Management vid Linköpings universitet. Inom ramen för vår masteruppsats studerar vi elektronisk identifikation och dess bruk inom en offentlig myndighetskontext i samband med diverse e-förvaltningstjänster. Studien innehåller intervjuer med respondenter från flera olika myndigheter. Kontakt via Linus Blomgren (linbl625@student.liu.se) och Hubert Czekierda (hubcz868@student.liu.se). Medgivande till inspelning/ljudupptagning (konfidentialitet, validering, avidentifiering, och frivillighet att delta och möjlighet att avbryta intervjun).

Inledande frågor
- Tid i verksamheten, tidigare arbetsuppgifter och bakgrund?
- Beskriv din roll och arbetsuppgifter

Utforska nuläget
- Vad är elektronisk identifikation för dig? – Varför är det viktigt? – De främsta motiven
- Brukar du personligen applikationer som identifierar dig online?
    - Används dessa applikationer på jobbet?
- När introducerades eID och hur påverkade det organisationen?
- Vilken roll har elektronisk identifiering i er organisation nu?
- I vilken utsträckning brukar ni elektronisk identifikation? Vilken spridning har det fått?
    - Vilka alternativ kring elektronisk identifiering har ni? Krävs fler och/eller bättre alternativ?
- Finns det brister i hur medborgare identifieras online?
- Hur sker samverkan med parter som möjliggör eID?
    - Vilken relation har statlig eID till BankID?
- Regulationer och lag för eID i organisationen
- Hur ser ni generellt på sekretess av eID?
    - Vad tycker ni om nuvarande sekretess av exempelvis BankID?

Politisk nivå, ledning
- Nuvarande strategier/mål/visioner kring eID
    - Finns det projekt/program/portföljer för att genomdriva dessa?
- Hur sker organisering, samverkan, styrning och uppföljning av eID implementering och dess drift?

- Finns det någon som har helhetsperspektiv/ansvar för elektronisk identifikation, kommunikation och nytta?
- Finns det en sammanhållande funktion som arbetar bland annat med elektronisk identifikation: styrning, stöd, medel, uppföljning?
- Fångas åsikter och tankar internt från organisationen och externt av medborgare kring olika digitaliseringslösningar?
    - Verksamhetens delaktighet i digitaliseringsbeslut: hur fångas behoven?
    - Spelar de roll?

Förändringsarbete, framtid

- Vilka prioriteringar och förväntningar finns för en statlig eID och dess framtid?
- Hur kommer en statlig eID att stå i relation till BankID i framtiden?
    - Blir det ytterligare ett alternativ i mängden?
    - Finns det planer att uteslutligen bruka en sådan lösning om den får fattning?
- Kan en statlig eID lösning erbjuda något som inte BankID gör?
- Hur sker interorganisatorisk utveckling för statlig eID framöver?
- Hur integreras medborgare/användare med eID?
- Vilken kompetens (och IT) behövs för eID?
- Hur informeras verksamheten om processer och tekniken/digitala möjligheter?
- Hur möjliggörs nationellt övergripande digitaliseringsinsatser (IT/digitalisering)?
- Andra utmaningar vid digitalisering (kravställning, kompetens, upphandling etc)?
- Andra drivkrafter/förväntningar på nationell nivå (automation, goda exempel etc)?

Avslutning

- Något att tillägga kring det vi talat om – är det något relevant vi missat?
- Någon annan du tycker vi ska prata med? Ok att återkomma? Tack och hej!

Figur- och tabellförteckning

1. Figurer

2. Tabeller