Myndigheten för samhällsskydd och beredskap

Framtidens säkra elektroniska identifiering

Framväxt och användning av e-legitimationer

FORSKNING

MSB:s kontaktpersoner:
Svante Ödman

Publikationsnummer MSB 663
ISBN 978-91-7383-425-4

Förord

Vi som arbetat i projektet kommer från olika vetenskapliga discipliner (informatik och statsvetenskap) och har haft med oss olika perspektiv, tidigare erfarenheter och kunskaper in i samarbetet. Gemensamt är att vi delar ett genuint intresse för hur elektronisk identifiering och tekniska lösningar för att kunna legitimera sig på nätet påverkar oss som individer, yrkesverksamma och som medborgare i ett samhälle, långt utanför de rent informationstekniska frågorna. Detta har inneburit att vi anlagt ett flervetenskapligt angreppssätt i projektet och när vi närmar oss utmaningarna och möjligheterna med elektronisk identifiering.

De teman som vi diskuterar är sådana som vi hoppas kan vara värdefulla för Dig som kommer i kontakt med utveckling och användning av elektronisk identifiering i praktiken. Målgrupper vi tror kan ha intresse av denna rapport är ansvariga beslutsfattare och tjänstemän inom offentlig sektor, men även utvecklare av tekniska lösningar för elektronisk identifiering och e-tjänster. Vår förhoppning är även att intresserade användare av e-ID – i olika roller – skall finna boken läs- och tänkvärd. Arbetet inom ramen för detta forskningsprojekt går mot sitt slut, men utmaningarna och möjligheterna kring elektronisk identifiering kommer att fortsätta vara många.

Innehållsförteckning

Sammanfattning

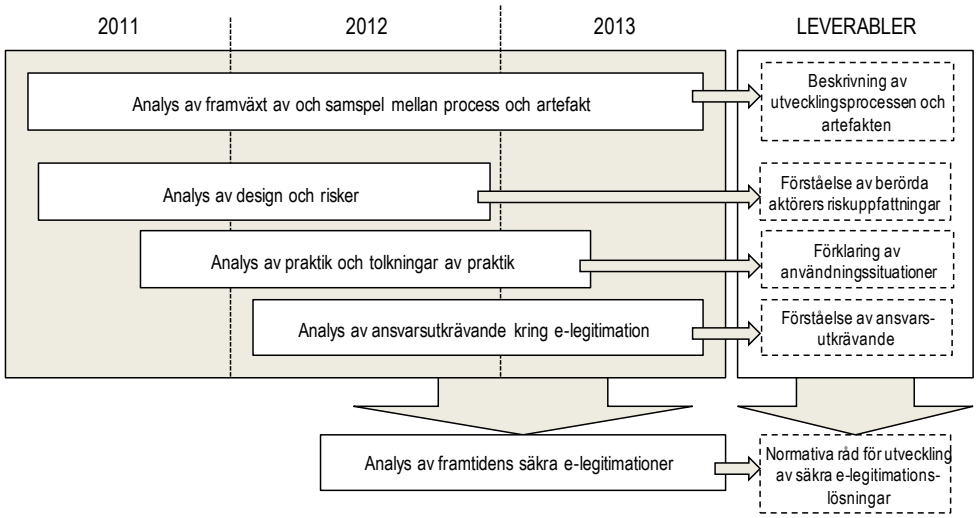
I denna rapport beskriver vi forskningsprojektet ”Framtidens säkra elektroniska identifiering – framväxt och användning av e-legitimationer” (FUSe-projektet) där sju forskare från informatik och statsvetenskap vid Linköpings universitet (LiU) har samverkat. Projektet är finansierat av Myndigheten för samhällsskydd och beredskap (MSB) och har bedrivits under åren 2011 till 2014. I projektet har vi ur ett socialt, organisatoriskt och tekniskt perspektiv följt och kritiskt studerat utvecklingsprocesser, implementering och användning av säker elektronisk identifiering i olika sammanhang. Vi beskriver här de fallstudier vi genomfört inom projektet. Därefter diskuterar vi iakttagelser från projektet i form av ett antal teman som är relaterade till elektronisk identifiering. Rapporten avslutas med lästips för den intresserade.

1. Inledning

I forskningsprojektet ”Framtidens säkra elektroniska identifiering – framväxt och användning av e-legitimationer” (FUSe-projektet) är vi sju forskare från informatik och statsvetenskap vid Linköpings universitet (LiU) som har samverkat. Projektet är finansierat av Myndigheten för samhällsskydd och beredskap (MSB) och har bedrivits under åren 2011 till 2014. I projektet har vi ur ett socialt, organisatoriskt och tekniskt perspektiv följt och kritiskt studerat utvecklingsprocesser, implementering och användning av säker elektronisk identifiering i olika sammanhang. I våra studier har vi valt att fokusera fem analysperspektiv:

1. Analys av framväxt av och samspel mellan process och artefakt – Beskriver övergripande, gemensam karaktärisering av hur elektronisk identifiering som process och artefakt har vuxit fram över tiden i Sverige samt vilka utvecklingsmöjligheter och hinder som har diskuterats och prövats.
2. Analys av design och risker – Fångar olika aktörers riskuppfattning före och vid användning av elektronisk identifiering med fokus på såväl tekniska som sociala risker, värderingar av risker samt designens betydelse för riskuppfattningar.
3. Analys av praktik och tolkningar av praktiker – Fokuserar hur faktisk och uppfattad säkerhet vid elektronisk identifiering framträder för olika aktörer och i olika situationer. Faktisk och uppfattad säkerhet får konsekvenser för elektronisk identifiering. eID används inte separat utan ingår i ett nätverk av artefakter när en e-tjänst ska användas. Uppfattningar kring eIDs säkerhet kan påverka uppfattningar kring e-tjänstens säkerhet och vice versa.
4. Analys av ansvarsutkrävande kring elektronisk identifiering – Identifierar vilka aktörer, organisationer och institutionella arrangemang som tar ansvar för utveckling och användning av elektronisk identifiering samt vilka som uppfattas som ansvariga och kan avkrävas ansvar då problem uppstår.
5. Analys av framtidens säkra elektroniska identifiering – Formulerar på basis av ovanstående analysresultat normativa, vägledande implikationer för kravställande och utveckling av morgondagens elektroniska identifiering.

I figuren nedan sammanfattar vi de fem analysperspektiven samt de kunskapsbidrag som analysperspektiven har gett.



FUSe-projektets analysperspektiv och leverabler

2. Genomförda fallstudier

För att studera de teman och analysperspektiv som vi beskriver ovan har vi genomfört fallstudier. Vi har studerat elektronisk identifiering i olika sammanhang (skola, vård, privatliv och riksdag för att nämna några) och med olika metoder. Vi har ett uttalat praktikintresse i vår forskning och har därför samlat in och analyserat empiriska data genom intervjuer, fokusgrupper, observationer och studier av systemanvändning. Vi har även studerat dokument, IT-systems utformning, gemensamma initiativ och sammankomster kring utveckling av eID och diskussioner i media. Vi har varit flera forskare i varje delstudie och samverkat vid såväl datainsamling som analys av resultaten. Fallen har varit olika omfattande och har involverat olika forskare i samverkan. Sammantaget täcker fallen in de fem analysteman som projektet har fokuserat.

2.1 Kartläggning av dåtid och nutid inom e-legitimationsområdet

Under projektets initiala skede skrev Fredrik Söderström sin masteruppsats (”I backspegeln, i fordonet och genom vindrutan – Den svenska e-legitimationens framväxt och nuläge”) som visar en sammanhållen bild av den elektroniska legitimationens (e-legitimationens) framväxt i Sverige. En sådan kartläggning är en viktig förutsättning för utvecklingen av säkra offentliga elektroniska tjänster inom den elektroniska förvaltningen. Eftersom statsförvaltningens styrning historiskt uppfattats som relativt otydlig har området med tiden kommit att präglas av olika enskilda aktörers egna insatser, intressen och föreställningar. Denna delstudies bidrag är att beskriva och analysera framväxten av den svenska e-legitimationen med hjälp av de tre analysperspektiven deltagande, föreställningar samt legitimitet. Delstudien fokuserar vad som skett historiskt och hur detta kan kopplas till det som sker i nutid kring e-legitimationer.

Särskild vikt har lagts vid aspekter av icke-teknisk natur, varvid studien kan ses som en motvikt till den tydligt teknikfokuserade utredning kring den framtida e-legitimationen som genomfördes under hösten 2010. Resultatet av arbetet visar bland annat på att praktisk erfarenhet är en nyckelaspekt för deltagandet och formandet av föreställningar kring e-legitimationen. Statens bristande intresse för området har även tydligt påverkat utrymmet för eget meningsskapande samt e-legitimationens erhållna legitimitet. När staten under 2010-11 fick ökat intresse för området och identifierade ett tydligt samordningsbehov stod det därmed klart att dessa ansatser inte kommer att vara av helt oproblematisk natur.

Arbetet i sig beskriver tolkningen av e-legitimationens framväxt i Sverige från dess start fram till nuläget. Framväxten som sådan får betecknas som god och Sverige tycks i detta avseende vara något av ett framgångsexempel. Det är dock tydligt att de motiv som drivit på denna utveckling kan återkopplas till stora myndigheters effektivitetssträvanden i kombination med utveckling av säkra

e-tjänster inom e-förvaltningen. När aktörer med annan bakgrund, till exempel inom kommun- eller landstingssektorn, kommer in i debatten blir detta faktum än tydligare. Skälet är att dessa sektorer inte har haft samma utvecklingstakt vad gäller e-tjänster och därmed har andra erfarenheter av e-legitimationsbegreppet i sig. Vidare har aktörer som kan kopplas till framväxten beskrivits i denna delstudie och hur dessa aktörer både påverkat och påverkats av framväxten. De aktörer som beskrivits som framgångsrika och drivande inom området har huvudsakligen representerats av myndighetssidan, men dessa har kontrasterats av en aktör inom den privata sektorn samt en aktör som är företrädare för kommuner och landsting. Arbetet i sig kan ses som fokuserat på myndigheters arbete kring e-legitimationer. Myndighetssidan har de facto kommit längre i utvecklingen och således har den bild som beskrivs i denna delstudie blivit färgat av detta. Vidare har arbetet i delstudien även innefattat framtagandet av en analysmodell för att undersöka aktörernas ömsesidiga påverkan på framväxten på en fördjupad nivå. Tillämpningen av denna modell visar tydligt på att förutsättningar finns för att nå en bättre förståelse kring hur struktur och handlingar har kommit att påverka aktörernas deltagande, föreställningar samt uppfattade legitimitet kring e-legitimationen. I ett försök till en generaliserande slutsats av detta arbete betonas att statsförvaltningens roll och intresse kring e-legitimationsområdet tydligt kan sättas i samband med de olika åsikter och föreställningar som bildats över tiden. Tydligare styrning, större intresse samt tydligare ansvarsfördelning kring e-legitimationen hade resulterat i ett gynnsammare utgångsläge att samordna området.

2.2 E-tjänstekort i användning vid Landstinget i Östergötland (LiÖ)

I denna delstudie har vi studerat e-legitimationer i olika användningssammanhang. Vårt fokus är olika typer av användningssituationer där e-tjänstekortet i vården har en roll eller funktion att fylla och hur detta är länkat till utvecklings- och införandeprocesser. Vi har här intresserat oss för organisationens erfarenheter kring arbete med införande av e-tjänstekort (såväl strategiskt som operativt) och de hinder eller möjligheter samt risker som kan sammankopplas med detta arbete.

LiÖ har använt e-tjänstekort i verksamheten en tid (med funktioner såsom passerkort, SIS-legitimation, privat e-legitimationer etc.), men har först under 2012 börjat implementera användning av detsamma i sin IT-miljö på bred front. Centrala system i detta sammanhang är det digitala patientjournalsystemet Cosmic, där användare vid olika enheter har börjat använda sitt e-tjänstekort (SITHS-kort) för att säkert kunna logga in i systemet och komma åt patient- och vårddata. Studien har därmed haft god timing för att kunna lära av införande, tidig användning och sedan också följa upp användning i ett längre perspektiv. Att vården dessutom är en kritisk miljö med avseende på tid, integritet och dess allmänt krävande insatser för att hantera människors hälsa har gjort delstudien än mera intressant och relevant.

Under fallstudiens gång har det stått klart för oss att den verksamhetskontext där eID introduceras har stor betydelse för hur denna artefakt mottas,

uppfattas och integreras i daglig användning. Till exempel är brister i flexibilitet och tekniska begränsningar något som vi sett har påverkat hörsamheten gentemot gällande regler att e-tjänstekortet ständigt skall följa den anställde under arbetsdagen. Vidare har vi även funnit en tydlig diskrepans kring hur e-tjänstekortet värderas och uppfattas, där den centrala IT-funktionens strikt tekniska värdeskapande nyttoperspektiv inte nödvändigtvis delas av den övriga verksamheten. Vi har funnit att hur e-tjänstekortet har mottagits varierar mycket mellan olika typer av verksamhet, vilket i sig får konsekvenser för dess användande.

Resultat från studien visar bl.a. komplexiteten i att införa eID i en stor och heterogen organisation, att införandet ses som oproblematiskt ur ett juridiskt perspektiv men samtidigt problematiskt ur ett tekniskt, användarmässigt och informationssäkerhetsmässigt perspektiv. Det är också tydligt hur olika användargruppers förväntningar på, och förhållande till, eID särskiljer. Exempelvis försöker man från ledningens sida maximera användningen av eID genom att bygga på många olika funktioner på kortet och på så sätt tvinga användarna att använda eID. En del av dessa funktioner är kopplade till användaren som privatperson snarare än som anställd, vilket gör att gränsen mellan privat- och arbetsliv sammankopplas. Just kopplingen mellan eID som ett privat/personligt kort och dess användning i en tjänsteroll är komplex och problematiskt. Ur implementeringssynpunkt finns också utmaningar kring att införa en lösning i vårdverksamhet samtidigt som den utvecklas. Även tidigare erfarenheter har stark påverkan på hur man uppfattar och förhåller sig till införande av ny teknik som eID. Exempelvis har det tidigare införandet av journalhanteringssystemet Cosmic stark påverkan på hur olika grupper tar till sig eID-lösningen. Vidare har vi funnit att det som särskiljer detta införande från andra traditionella införanden av olika typer av IT-stöd är att vi här har att göra med en teknisk artefakt (e-tjänstekortet) som är tydligt kopplad till individens tjänsteutövning med hänsyn till roller och identitet men även till personens privata sfär och identitet. I tjänstesammanhang har e-tjänstekortet en mycket viktig funktion att fylla i och med att patientsäkerheten i den sammanhållna journalföringen säkerställs enligt lag, men frågan är vilka konsekvenser ett e-tjänstekort kan få i privat bruk. Vi ser att det är e-tjänstekortets tekniska arkitektur som skapar flera frågeställningar, till exempel kring förhållandet mellan tjänsteutövarens och den privata individens integritet och autonomitet. Denna delstudie kan relateras till analysperspektiv 2, 3 och 4 ovan.

2.3 Användning av e-legitimationer vid kommunikation mellan skolan och hemmet inom grundskolor i Linköpings kommun

Användningen av IT inom skolan har på senare år ökat kraftigt. Därtill har skolsektorn utvecklats genom friskolereformen och den mångfald av skolhuvudmän som vuxit fram. På så sätt är skolsektorn i Sverige idag en heterogen verksamhet med omfattande informationsutbyte. Sedan 2011 krävs enligt den nya Skollagen (SFS 2010:800) kontinuerlig uppföljning av elevens

arbete, skriftliga omdömen och digital hantering av individuella utvecklingsplaner (IUP). Kraven på kommunernas och skolornas digitala dokumenthantering har ökat och skapar efterfrågan på säker dokumenthantering mellan olika aktörer som lärare, elever, föräldrar och skolledning. I flera kommuner används därför olika s.k. lärplattformar som fungerar som pedagogiska arbetsmiljöer, verktyg för utbildningsadministration samt kommunikation mellan hem och skola. Det finns tydliga behov av att beakta informationssäkerhet då dessa system systematiskt och specifikt hanterar stora volymer elevdata som också skall lagras i många år. Säker inloggning och användningen av eID är kritiskt för tilltron till och användningen av dessa system. Därför har vi valt att studera utbildningsadministration och särskilt kommunikationen mellan hem och skola i dessa system. Syftet med denna delstudie har varit att studera implementering av säker inloggning till IKT-plattformar och e-tjänster i skolan samt hur slutanvändare tolkar säkerhet i relation till dessa.

Denna delstudie har haft två mål. För det första att utifrån den kommunala organisationen analysera utvecklingsprocesser, implementering och användning av säker elektronisk identifiering. För det andra att analysera hur faktisk och uppfattad informationssäkerhet i privata och offentliga e-tjänster formas och visa på utvecklingsmöjligheter för ökad tillit till systemen. Delstudien baseras på en kvalitativ studie i Linköpings kommun, där tre olika lärplattformars design, implementering och användning har analyserats. De tre studerade systemen är FRONTER, SKOLA 24 och SKOLSOFT, vilka har många olika funktioner. Vi har främst uppmärksammat de som har med individdokumentation att göra samt kontakter mellan hem och skola. Säker inloggning till dessa system för föräldrar började implementeras 2011 och skolorna har kommit mycket olika långt, vilket i sig är ett tydligt uttryck för hur olika de ser på informationssäkerhet och hur decentraliserade dessa beslut är.

Det är tydligt att skolorna och även enskilda lärare förhåller sig mycket olika till dessa frågor och har kommit olika långt i sin användning av lärplattformarna. Inloggningen sker huvudsakligen med användarnamn och lösenord (för elever och lärare). eID är avsedd som inloggningsalternativ för föräldrar, men få föräldrar har än så länge utnyttjat den möjligheten. Flera av föräldrarna har haft tekniska problem med eID, vilket gör att de istället väljer att logga in med elevernas användarnamn och lösenord. Detta var även en vanlig strategi bland de föräldrar som inte sedan tidigare använt eID. Att nå säker information om sina barns skolgång var således inte ett tillräckligt motiv för att börja använda eID, bland de intervjuade (ett litet urval). Genomgående var dock föräldrarna positiva till att kraven på plattformarnas säkerhet höjs och att eID kan användas. En del föräldrar är positiva till att använda eID i framtiden, men det förutsätter att eID fungerar tekniskt och är enkelt att hantera och använda. De som använder eID på andra områden är nöjda med hur det fungerar och ser inget problem i att använda eID i kommunala e-tjänster.

Alla de andra intervjuade grupperna var eniga om att informationssäkerhet är viktig i skolkontexten i och med att mer och mer information om elever digitaliseras. Många av lärarna ställde sig tvekande eller negativa till möjligheten att använda eID som inloggning för att höja

informationssäkerheten. Detta eftersom de förväntades använda sin privata eID och inte erbjöds någon slags tjänste-ID, som inom landstinget. Lärarna upplevde därför kravet på inloggning i hög grad som en ökad kontroll från arbetsgivaren och myndigheter eller en onödig komplikation som försvårar arbetet. Lärarna föredrog dagens sätt att logga in med användarnamn och lösenord.

Både lärare och rektorer uttryckte en tveksamhet till om informationssäkerheten var tillräckligt hög för att börja lagra och arbeta med känsligare information som förekommer i pedagogiska dokument, så som skriftliga omdömen och de lagstadgade individuella utvecklingsplanerna. Pedagogiska utredningar som klassas som känsligast lagrades eller delades inte på någon av de studerade skolorna via lärplattformarna. Det finns missnöje inom alla grupperna angående själva designen av plattformarna, som alla utvecklats av fristående företag. Systemen beskrevs som föråldrade, krångliga och att gränssnittet inte var användarvänligt. De efterfrågar uttryckligen en flexibel plattform som kan anpassas till skolans arbetsformer och metoder och inte tvärtom. Det finns fortfarande en okunskap bland rektorer både om lärplattformarnas praktiska användning och informationssäkerheten, vilket i sin tur gör lärarna osäkra om hur de ska förhålla sig till plattformen.

Sammantaget var det tydligt att lärplattformarna inte uppfattas av användarna som tillräckligt säkra för att kunna hantera känsligare uppgifter. Användningen av eID verkar vara beroende av hur plattformarna fungerar tekniskt. eID som inloggning till en dåligt fungerande plattform uppfattas inte som en bra lösning. eID som inloggning till en komplicerad plattform där användarna har lite kunskap verkar helt enkelt inte vara en bra lösning. Det finns dock möjligheter till förbättringar och de allra flesta informanterna har intresse att öka användningen om systemen vore enklare att använda. De efterfrågar här en integrerad, flexibel och säker lösning som samtidigt är enkel och intuitiv att hantera. Därtill finns det en stor utmaning i behovet av kompetensutveckling och ökad medvetenhet om informationssäkerhet, särskilt efterfrågas det av lärarna. Denna delstudie kan relateras till analysperspektiv 2, 3 och 4 ovan.

2.4 Medborgarattityder kring användning av e-legitimation

Under 2011 genomförde Karl Eriksson och Tommy Thalén, studerande på masterprogrammet IT och management vid Linköpings universitet, inom ramen för sitt magisteruppsatsarbete (”E-legitimationen och studenter – En studie om eId nu och i framtiden”) en fokusgruppsstudie bland studenter från olika utbildningar vid Linköpings universitet. Syftet med fokusgrupperna var att undersöka hur e-legitimationer används av unga idag, hur unga ser på e-legitimationer i relation till användbarhet, säkerhet och förtroende, samt hur deras syn på framtida e-legitimationer eventuellt skiljer sig från statens vision. I tre fokusgrupper deltog totalt sexton personer som fick i uppgift att använda en av CSN:s e-tjänster som kräver e-legitimation samt lösa problemet som uppstår om man glömt sitt e-legitimationslösenord. Utifrån dessa uppgifter diskuterade sedan deltagarna hur de ser på nuvarande och framtida e-legitimationslösningar. Studien visar att e-delegationens förslag är relativt

övergripande och odetaljerat i förhållande till denna användargrupps krav och förväntningar. Slutsatserna kompletterar och kontrasterar förslaget genom att ge bilder av hur unga ser på framtiden när det gäller e-legitimationer samt vilka tjänster de skulle vilja se.

Huvudbudskapet i detta arbete är att den studerade användarkategorin (unga universitetsstuderande) betonar användbarhet och säkerhet som två viktiga aspekter vid e-legitimationsanvändning, då dessa påverkar tilliten för såväl e-legitimationslösningen som för e-tjänsten i sig. I denna studie framhålls användbarhet som en något viktigare fråga än säkerhet, vilket i sig är intressant då säkerhet till stor del är det övergripande målet med e-legitimationsutvecklingen. Studien visar även att användargruppers attityder till e-legitimationer kan studeras genom fokusgrupper samt att dessa attityder är viktiga att fånga. Olika användargrupper kan se helt olika på t.ex. användbarhet och säkerhet och det innebär därför en potentiell risk att inte beakta medborgares attityder, på strategisk såväl som artefaktnivå, vid utveckling av ny e-legitimationslösning. Att inte fånga in medborgares attityder under utvecklingsprocessen kan i förlängningen leda till minskad användning av offentliga e-tjänster och minskad tillit till elektronisk förvaltning.

I denna delstudie visar vi att medborgares attityder kan vara viktig input vid utveckling av e-legitimationslösningar. Hittills i den studerade utvecklingsprocessen har inte medborgarattityder varit i fokus, vilket i sig inte är konstigt då processen inrymmer en mängd olika intressenter och såväl tekniska som organisatoriska utmaningar. E-legitimationer är heller inte en separerbar artefakt för användaren, som t.ex. aldrig använder e-legitimation utan ett syfte att nå en e-tjänst, signera ett dokument, e.dyl. Trots dessa karaktäristika visar vi i denna delstudie att användarattityder är viktiga att ta hänsyn till i utvecklingsprocessen, för att på sikt nå lösningar som är att betrakta som framgångsrika och användbara för många. Denna delstudie kan relateras till analysperspektiv 3 ovan.

2.5 eID:s betydelse för kommunikation och organisering på en statlig myndighet

Vi arbetar för närvarande med en studie vid Försäkringskassan, där vi undersöker eID från olika perspektiv och på olika nivåer i organisationen. Med olika perspektiv menas att vi är intresserade av användningen av eID både internt, i de anställdas tjänsteutövning, och externt, i kontakten med medborgare. Med olika nivåer avses att vi studerar olika delar av organisationen. Dels studerar vi den centrala ledningsnivån på myndigheten och hur man där arbetar med (1) strategier och policyer kring eID såväl som (2) teknisk och organisatorisk utveckling kopplat till e-tjänster och eID. Dels studerar vi det vardagliga samt utvecklingsarbetet på de Kundcenter som handhar den stora delen av de direkta medborgarkontakterna, då vi är intresserade av hur kommunikation mellan myndighet och medborgare potentiellt förändras med den ökade digitaliseringen. Studien på Försäkringskassan genomförs framförallt genom dokumentstudier samt intervjuer med nyckelaktörer inom organisationen. Denna delstudie kan relateras till analysperspektiv 2, 3 och 4 ovan.

2.6 Den politiska konstruktionen av eID

En ytterligare aspekt av den process där eID utvecklats och kommit till användning är hur den tolkas av olika politiska aktörer. För att belysa detta har vi analyserat hur utvecklingen av elektronisk identifikation diskuterats i riksdagen. Här är det tydligt att i hög grad kopplas samman med praktiska situationer där det krävs lösningar för den enskilda medborgaren eller en viss myndighet. I likhet med andra komplexa tekniska frågor är det ofta lösningar och användning som står i fokus. Men det finns få exempel i debatten där mer underliggande politiska utmaningar om exempelvis integritet och kontroll lyfts fram. Inte heller tydliggörs frågor om samverkan och ansvarsfördelning mellan privata och offentliga aktörer i riksdagsdebatten. Detta trots att det i praktiken framträder som ett särskilt viktigt och kritiskt område i våra andra fallstudier. Slutsatsen av denna diskursanalys av eID i riksdebatten är att avgränsade frågor om praktiska tillämpningar döljer den större underliggande frågan om vad som skulle kunna vara början på konstruktionen av informationssamhällets medborgarskap.

3. Iakttagelser från projektet

När vi analyserat resultaten från ovanstående delstudier ser vi ett antal återkommande intressanta teman, vilka diskuteras nedan.

3.1 Faktisk och upplevd informationssäkerhet

Informationssäkerhet kan delas upp i teknisk, formell och informell säkerhet. Den tekniska säkerheten syftar till att skapa en säkrarare informationshantering med hjälp av IT i form datasäkerhet och kommunikationssäkerhet samt med hjälp av fysiska skydd som exempelvis lås eller larm. Datasäkerhet handlar om att skydda data och system mot obehörig åtkomst eller obehörig eller oavsiktlig förändring eller störning. Kommunikationssäkerhet innebär skydd av nätverk och annan utrustning som används för att kommunicera mellan datorer. Genom den formella säkerheten vill en organisation styra användarens beteenden genom att införa policyer, rutiner, riskbedömningar, etc. Den informella säkerheten handlar om det som är svårare att uppfatta, och därmed styra, såsom värden, attityder och uppfattningar om hur man som användare ska handla i informationssäkerhetsfrågor. Alla dessa delar är viktiga för att skapa en säker och trygg informationsanvändning. Mycket forskning har hittills fokuserat den tekniska säkerheten, men användares beteenden och det organisatoriska sammanhanget är minst lika viktigt för säker hantering av information. Informationssäkerhet handlar därför om det tekniska och användarens beteende i ett organisatoriskt sammanhang. Alla dessa delar ska helst hänga samman och bidra till varandra för att på ett så effektivt sätt som möjligt skydda verksamhetens informationstillgångar. Detta är vad vi menar med att betrakta säkerhet i ett sammanhang.

En organisations säkerhetskultur kan beskrivas som det sätt som man gör saker och ting inom en verksamhet för att skydda informationen. Säkerhetskulturen är med den beskrivningen handlingsorienterad och kopplad till organisationskulturen. Som organisationskultur har den element av det som tas för givet och ”sitter i huvudet på folk”, men den har också element av det som är mera institutionaliserat, dvs. ”det som sitter i väggarna” eller det som finns nedtecknat. Informationssäkerhet finns därmed inte isolerat, utan ingår i ett verksamhetsmässigt sammanhang och ska i bästa fall också bidra till verksamhetens organisatoriska mål. Styrning och ledning av informationssäkerhet kan inte ses som en egen isolerad aktivitet, utan måste naturligt ingå i det övergripande ledningsarbete. Att arbeta med informationssäkerhet är mycket mer än att införa lösenordsskydd eller kryptering, det handlar också om att ta hänsyn till och att utveckla verksamheten. Det måste finnas säkerhetsrutiner som fungerar – dvs. verksamhetskopplade och användbara rutiner som på ett naturligt sätt är en del av den anställdes arbete. Informationssäkerhet är en del av den anställdes dagliga arbete. Ledningens arbete med informationssäkerhet måste också utgå från ett synsätt där informationssäkerhet integreras som en naturlig del i den

anställdes arbete. Informationssäkerhet skapas och omskapas hela tiden vid hantering av information. Tekniska kontroller, formella rutiner och normer bör utgå från, och sammanlänkas med, den anställdes arbetsuppgifter och organisationens mål.

Hur man inom en organisation uppfattar informationssäkerhet och säkerhetsrisker och vad som faktiskt händer kan skilja sig åt. De uppfattade säkerhetsriskerna är inte bara beroende av de implementerade kontrollerna i form av IT-säkerhet och av användarnas beteenden, normer och värderingar. De är också beroende av vad man tycker är viktigt och vad man anser att man ska skydda. Det skiljer sig med andra ord mellan olika aktörer inom och mellan organisationer vad man anser vara en säkerhetsrisk. Och därmed också hur man uppfattar säkerheten. Den upplevda och faktiska säkerheten kan alltså variera.

3.2 Tillit och risk

Att vilja och därmed sträva efter att känna tillit är en grundläggande mänsklig känsla. Det är en förutsättning för att vi ska känna oss trygga och lita på att det andra utger sig för att vara, och det de uttrycker, faktiskt stämmer. I möten med andra människor bygger vi vår tillit på det vi ser, hur andra människor bemöter oss, att vi kan anpassa oss till varandra för samförstånd och nyttja våra erfarenheter av tidigare möten. Att bygga upp tillit tar ofta lång tid, men tillit kan gå mycket snabbt att rasera. I våra möten med samhällsaktörer såsom myndighetspersoner, lärare eller vårdpersonal färgas vår tillit i den enskilda situationen av vilken grundläggande tillit vi känner till samhällsapparaten. Eftersom myndighetspersonen är representant för samhället, så påverkar också våra möten med myndighetspersoner den tillit vi känner till samhället i stort. Ett bra möte gör att vi känner oss tryggare som medborgare.

När vi går från möten med andra människor till möten med teknik och att använda e-tjänster för att utföra uppgifter i samhället, byter vi till viss del fokus för vad vi känner tillit för. Även tekniken, IT-systemets gränssnitt eller säkerhetslösningen vid överföring av data påverkar vår tillit; inte bara en persons bemötande och kompetens. Detta påverkar också vår tillit till samhället och de uppgifter vi ska utföra. Hur det påverkar vår tillit varierar dock mellan människor. En del har låg tilltro till tekniken i sig och/eller sin förmåga att använda tekniken på ett ändamålsenligt sätt. Andra litar blint på att det blir rätt när det är en dator som till synes automatiskt utför uppgifterna. Vi kanske till och med lämnar över ansvaret för våra handlingar till den som utvecklar eller levererar den tekniska lösningen. Eller så sjunker vårt förtroende för en tjänst just för att den sker via en teknikmedierad kanal, oavsett om kvaliteten i tjänstens innehåller eller leverans i sig förändrats eller inte.

När vi talar om elektronisk identifiering tillkommer ytterligare en aspekt som vi kan känna mer eller mindre tillit till. Identifieringstekniken är ämnad att ge den säkerhetsnivå som krävs för det aktuella användningsområdet. Dess funktion och användbarhet kan påverka vår tillit till själva identifieringen, men den kan också ”spilla över” på graden av tillit till e-tjänsten eller IT-systemet som vi ska använda samt även till de samhällsaktörer som erbjuder tjänsten.

Därigenom finns komplexa och mångfacetterade samband mellan tillit till teknik och människor, som är viktiga att förstå och kunna relatera till då man utvecklar och använder e-tjänster och elektronisk identifiering. Denna mångfacettering kan sällan hanteras av en enskild profession som utvecklar eller inför e-tjänster eller elektronisk identifiering, utan kräver att personer med olika kompetenser samverkar för att öka sannolikheten för framgång.

Nära kopplat till tillit är hur man uppfattar risker med att använda teknik för identifiering. Finns det risk att känslig information kommer i orätta händer? Vilken information är känslig? Är det verkligen rätt (uppdaterad, fullständig etc.) information som jag har när jag exempelvis ska behandla en patient? Och hur är det med den information som finns registrerad om mig själv? Har jag kontroll på den informationens användning och spridning? Hur man uppfattar risker beror på vem man är, hur man använder tekniken, och för vad. En person med stora tekniska kunskaper kan exempelvis identifiera risker kopplat till tekniken i sig, som problem med att integrera olika IT-system. Andra, med mer verksamhetskunskap, kanske snarare ser risker med att använda eID som passerkort som i exemplet från sjukvården ovan. Ytterligare andra, som jobbar med eID på en nationell nivå, kopplar riskerna till utmaningar med nationell samordning och exempelvis standarder inom området. Många uppfattningar existerar parallellt.

3.3 Kan eID bidra till att stärka den offentliga sektorns legitimitet?

Den offentliga förvaltningen (i vid mening) har en viktig roll att spela när det handlar om att skapa och upprätthålla legitimitet för det politiska systemet. Att rösta och att kommunicera med folkvalda är för det stora flertalet individer händelser som sker relativt sällan. Kontakten med den offentliga förvaltningen och med välfärdstjänster förekommer däremot ofta. Framförallt gäller detta i anslutning till vissa händelser och perioder i livet, exempelvis när du studerar, får barn eller blir pensionär.

Med andra ord är det genom den offentliga förvaltningen som medborgarna kommer i kontakt med effekterna av politiska beslut. Genom välfärdsstatens aktiviteter och tjänster som exempelvis förskola, studielån, föräldraförsäkring, bostadsbidrag och pensionsutbetalningar kommer medborgarna i kontakt med det offentliga. Forskning visar att interaktionen mellan medborgarna och den offentliga sektorn är viktig för att bygga förtroende och stöd för det politiska systemet som helhet. Det är betydelsefullt att medborgarna upplever den offentliga förvaltningen och välfärdstjänsterna som effektiva och att alla medborgare behandlas lika och rättvist.

Digitaliseringen av den offentliga sektorn (och därmed sammanhängande ökad användning av eID som förutsättning för att kunna nyttja offentliga e-tjänster) kan ses som positiv då den kan bidra till likabehandling och rättssäkerhet i förvaltningen. Detta kan ske på två sätt. Dels genom att medborgarens identitet i flera aspekter döljs för handläggaren, vilket skulle kunna hindra handläggare från att fatta beslut som färgas av medvetna eller omedvetna förutfattade meningar. Dels genom att myndighetsbeslut kan fattas automatiserat av IT-

system istället för av människor, vilket kan uppfattas som en slags objektivitetens ytterlighet – maskinen behandlar alla lika såvida de generella utgångspunkterna vid designen av tekniken är kvalitetssäkrad. Digitaliseringen skulle alltså kunna bidra till att förvaltningens beslut uppfattas som rättvisa av medborgarna, och genom detta bidra till att stärka det offentligas legitimitet.

Många offentliga aktörer menar också att det finns ett tryck och en förväntan från allmänheten att offentliga organisationer ska skapa tillgänglighet till information och tjänster via nätet, och att digitaliseringen i sig är ett sätt att skapa legitimitet. Medborgarna förväntar sig ofta att det offentliga ska kunna tillhandahålla e-tjänster i minst samma omfattning och med samma kvalitet som företag och att tjänsterna ska vara tillgängliga via olika kanaler, stationärt och mobilt. Den kommun som exempelvis inte låter medborgarna ansöka om förskoleplats på nätet riskerar att anses som gammalmodig. Det finns alltså en föreställning om att en myndighet med en hög grad av digitalisering, tvärtemot den ”mossiga” kommunen, uppfattas som modern, framåtskridande och effektiv. I relation till detta så är det viktigt att de tekniska lösningar (exempelvis eID och länkade e-tjänster) som används i interaktionen är stabila, funktionella och inger förtroende – annars kan digitaliseringen ha motsatt effekt när det gäller legitimitet. Vi ska också komma ihåg att mera komplexa och krävande ärenden fortfarande inte sällan kräver större inslag manuell handläggning och innehåller interaktion som inte sker elektroniskt. Viktigt är också att väga dessa kanaler ur ett medborgarperspektiv.

När medborgarnas uppfattningar betonas bör vi också beakta de grupper av medborgare som av olika anledningar (exempelvis teknisk okunskap, språkbarriärer eller funktionshinder) är skeptiska till eller missnöjda med det offentligas ökade användning av e-tjänster. Det kommer sannolikt alltid att finnas individer som hellre talar med eller av olika skäl föredrar att träffa en handläggare personligen än hanterar sina myndighetsärenden på nätet. För den här gruppen är det irrelevant huruvida de tekniska lösningarna fungerar till synes perfekt, om de bidrar till en kvalitetshöjning i verksamheten eller om utfallet av myndighetskontakten är den önskade – dessa medborgare kommer ändå att vara missnöjda. Det är i anslutning till detta värt att påminna om att myndigheter är skyldiga att möta medborgare på olika sätt, vilket är en viktig skillnad jämfört med till exempel företag som kan välja att styra och avgränsa sin kommunikation med kunder på ett mera valfritt sätt.

Sammanfattningsvis kan användning av e-tjänster och eID i interaktionen mellan medborgare och offentliga organisationer öppna upp för såväl stärkt som försvagad legitimitet för den offentliga sektorn. Stärkt då en myndighet kan uppfattas som trovärdig om den har en hög grad av digitalisering och då en utbyggd e-förvaltning kan ge goda förutsättningar för likabehandling. Försvagad då brister i de tekniska och organisatoriska lösningarna kan ge upphov till irritation och misstro, och då det finns grupper av medborgare som har en skeptisk grundinställning till digitalisering.

3.4 Ansvarsutkrävande

Våra analyser visar att det inte finns en aktör eller organisation som ensam är ansvarig för att eID utvecklas och används. Utvecklingen och framväxten av

eID karaktäriseras snarare av omfattande och ingående samverkan mellan många olika aktörer. Även när det kommer till praktisk användning av eID är det tydligt att det är många inblandade som påverkar hur, när och med vilka tekniska lösningar som den enskilde kan använda eID. När enskilda användare i våra studier upplevde problem var det sällan självklart vem de skulle vända sig till och på vilket sätt den ansvarige tog ansvar för att lösa det som upplevdes som problematiskt.

Trots otydligheterna så har den svenska staten ett övergripande ansvar och intresse av att eID utvecklas i Sverige. Detta blir tydligt genom e-legitimationsnämndens uppdrag och koordinerande funktioner. Staten har dock i uppdraget byggt in ett tydligt beroende av externa aktörer, som banker och andra aktörer. Rollerna för olika aktörer har varit otydligt formulerade, vilket lett till otydligheter i uppdraget och kanske även försinkat utvecklingen. På så sätt blir även ansvarsfördelningen mellan dessa otydlig. För användarna kan detta å ena sidan upplevas som otydligt och krångligt, men å andra sidan så kan det ses som att det finns möjligheter att byta lösning om man är missnöjd.

Den här formen av samverkan för att genomföra offentligt beslutade policymål – att införa eID – kallas nätverksstyrning och blir allt vanligare inom många områden. Staten tar då på sig en mer förhandlande än bestämmande och styrande roll. Därför kan inte heller staten i denna styrningsmodell vara ansvarig för allt. När ansvaret delas på många blir det dock än viktigare att man kan förutse problem, både vad gäller innehållet i tjänsten och rollfördelningen kring den, för att redan på förhand fördela ansvaret mellan de inblandade.

I organisationer där den dagliga användningen av eID äger rum, som verksamheterna i våra delstudier, blir behovet av att klargöra ansvarsfördelningen på förhand än viktigare. Där finns ofta aktörer med olika kompetenser och intressen. Exempelvis kan det finnas personal med juridiska respektive tekniska kompetenser. De har då olika perspektiv på eID och upplever olika problem och utmaningar med eID. Men det kan också leda till att de på olika sätt tar ansvar för utvecklingen. Särskilt tydligt blev detta när jurister och tekniker möts för att designa lokala utformningar av eID i en organisation. Det som ansetts vara en lämplig teknisk lösning kan vara förenat med många juridiska problem och tvärtom. Ingen av dessa professioner har möjlighet att helt förstå och beakta båda dessa sidor av problemen. Den här mångtydligheten visade sig i våra studier leda till att det blev svårt att ställa någon i organisationen till fullo till svars för vad som sker.

4. Mer att läsa

Inom ramen för projektet har vi skrivit olika typer av publikationer. I dessa kan du läsa vidare om du vill fördjupa dig i de frågor vi diskuterat i denna rapport.

Andréasson, E., Axelsson, K., Gustafsson, M.S., Hedström, K., Melin, U., Söderström, F., Wihlborg, E. (2014). Vem är vem på nätet? En studie av elektronisk identifiering, Linköpings universitet, LiU-Tryck

Andréasson, E. (2011), Utvecklingen av e-legitimationer i Sverige - en studie av det privata och det offentligas roller, presenterat vid Statsvetenskapliga förbundets årsmöte, 28 oktober 2011, Umeå

Andréasson, E. (2013). Identity and Identification - Perspectives on Citizen-Government Relationships in the Digital Era, The 8th International IFIP Summer School on Privacy and Identity Management for Emerging Services and Technologies, June 2013, Berg en Dal, the Netherlands.

Axelsson, K., Melin, U. (2012). Citizens' Attitudes towards Electronic Identification in a Public E-service Context – An Essential Perspective in the eID Development Process, in Scholl, H. J., Janssen, M., Wimmer, M. A., Moe, C. E., Flak, L. S. (Eds.): EGOV 2012, LNCS 7443, Springer-Verlag Berlin Heidelberg, pp. 260–272, 2012.

Eriksson, K., Thalén, T. (2011). E-legitimationen och studenter – En studie om eId nu och i framtiden. Magisteruppsats i informatik, Linköpings universitet, ISRN LiU-IEI-FIL-A—11/01066—SE.

Gustafsson, M. (2014). Constructing Security - reflections on the margins of a case study of use of electronic identification in ICT platforms in schools. Proceedings of The 8th International IFIP Summer School on Privacy and Identity Management for Emerging Services and Technologies, Berg en Dal, the Netherlands.

Gustafsson, M., & Wihlborg, E. (2013). Safe on-line e-services building legitimacy for e- government: A case study of public e-services in education in Sweden. eJournal of eDemocracy & Open Government, Vol. 5(2), pp. 155-173. (ISSN 2075-9517)

Hedström, K., Wihlborg, E., Söderström, F. & Gustafson, M. (2014), The construction of identity – the use of eID in public organizations. 11th Scandinavian Workshop on Electronic Government (SWEG), Linköping University, Feb 4-5, 2014, Linköping, Sweden.

Melin U, Axelsson K, Söderström F (2014), Developing e-ID in a Public e-service Context – Challenges and Success Factors from a Life-cycle Perspective, submitted to TGPPP SI

Melin, U., Axelsson, K., Söderström, F. (2013). Managing the development of secure identification – Investigating a national e-ID initiative within a public e-

service context, in Proceedings of the 21st European Conference on Information Systems (ECIS 2013), 6-8 June 2013, Utrecht, The Netherlands.

Söderström, F. (2011). I backspegeln, i fordonet och genom vindrutan – Den svenska e-legitimationens framväxt och nuläge. Masteruppsats i informatik, Linköpings universitet, ISRN LiU-IEI-FIL-A—11/00987—SE.

Söderström, F. (2012a). Weak Governance Leading to Success – Aspects of the National Electronic Identification in Sweden's Public Sector, 9th Scandinavian Workshop on E-Government, February 9-10, 2012, Copenhagen.

Söderström, F. (2012b). The National eID in Sweden: an Actor-Network Perspective, PhD Colloquium, The 11th IFIP E-Government Conference, September 2, Kristiansand, Norway.

Söderström, F., Melin, U. (2012). The Emergence of a National eID Solution – an Actor-Network Perspective, The 35th Information Systems Research Seminar in Scandinavia, August 17-20, 2012, Sigtuna, Sweden.

Wihlborg, E. (2012). eID (electronic identification) as an Innovation in the Interface of Politics and Technology. Paper presterat vid Uddevalla symposiet, University of Algarve, Faro, 14-16 juni 2012.

Wihlborg, E., Gustafsson, M. S. (2013). Electronic identification in practice – a case study of use and organization of eID in public e-services in schools, paper presented at Scandinavian Workshop on E-Government (SWEG'13), 5-6 February 2013, Oslo, Norge.

Wihlborg, E. (2013). Secure eID (electronic identification) in the intersection of politics and technology, International Journal of Electronic Governance (IJEG), 6(2), 143-151.

Myndigheten för samhällsskydd och beredskap
651 81 Karlstad Tel 0771-240 240 www.msb.se
Publ.nr MSB 663 ISBN 978-91-7383-425-4