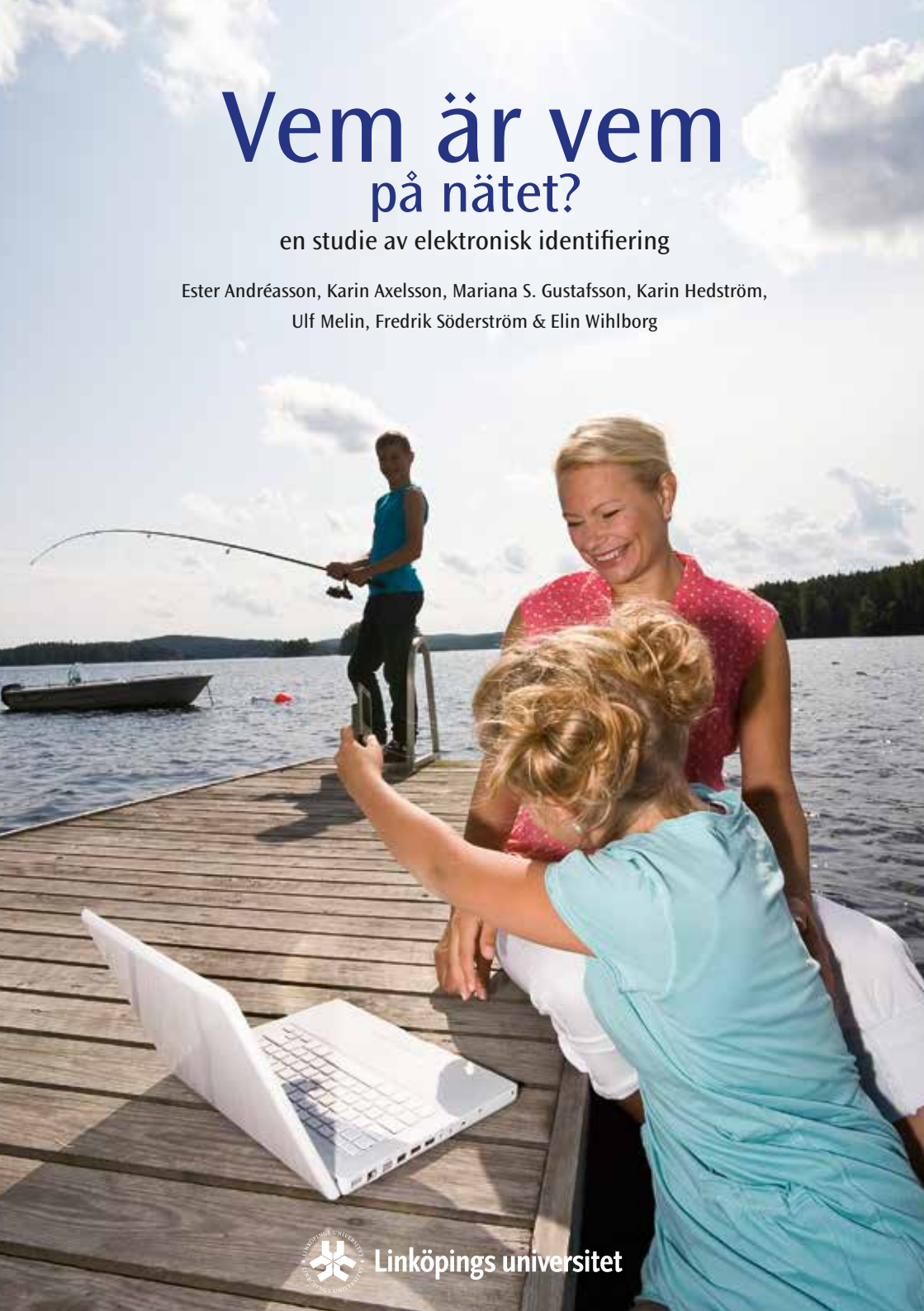
Vem är vem
på nätet?

en studie av elektronisk identifiering

Ester Andréasson, Karin Axelsson, Mariana S. Gustafsson, Karin Hedström,
Ulf Melin, Fredrik Söderström & Elin Wihlborg



Linköpings universitet

Vem är vem
på nätet?
en studie av elektronisk identifiering

En diskussionsbok baserad på forskningsprojektet
”Framtidens säkra elektroniska identifiering
– framväxt och användning av e-legitimationer”

vid Linköpings universitet 2011-2014

Utgiven av Linköpings universitet

ISBN 978-91-7519-326-7

Finansiering: Myndigheten för samhällsskydd och beredskap, MSB

Grafisk formgivning och språkgranskning: Mediahavet AB, S-610 42 Gryt
www.mediahavet.se | redaktionen@mediahavet.se | tel +46 123 40110

Distribueras av: Linköpings universitet
Institutionen för ekonomisk och industriell utveckling
581 83 Linköping | Tel: 013-281000
Tillgänglig elektroniskt via: www.ep.liu.se

LiU-Tryck, april 2014

Innehåll


REKNINGAR

Samhällets och företagens **legitimitet** påverkas av hur medborgarna **uppfattar** IT-lösningar.

Inledning

Att identifiera sig är något vi gör i många olika vardagssituationer; exempelvis när vi ska styrka vår ålder i krogkön, uträtta bankärenden eller bli insläppta av vakten på en bevakad arbetsplats. För att identifiera oss i dessa situationer använder vi oftast någon form av fysisk identitetshandling; ett körkort, pass eller ID-kort. Samtidigt har vi idag ett samhälle där allt fler ärenden går att utföra via nätet, där såväl offentliga som kommersiella aktörer erbjuder elektroniska tjänster (e-tjänster) i ökande omfattning. Vi blir därmed alltmer beroende av informationsteknik (IT) i samhället för att samverka och kommunicera effektivt och enkelt. Vår riskexponering och sårbarhet ökar i takt med att vi utför allt fler ärenden via e-tjänster. Känslig information kan utnyttjas av obehöriga eller missbrukas på olika sätt.

Elektronisk identifiering blir i dessa sammanhang en viktig komponent och förutsättning för att kunna erbjuda och använda effektiva och säkra e-tjänster. När man identifierar sig på nätet och i IT-system kan man göra det på många olika sätt; man kan logga in med användarnamn och lösenord, använda elektroniska ID-lösningar (eID) med dosor och koder, scanna fingeravtryck, använda e-tjänstekort och kortläsare eller RFID-teknik. Man skulle kunna betrakta dessa identifieringslösningar som rent tekniska landvinningar, som bara syftar till att man ska kunna nå den e-tjänst man vill använda. Likt en nyckel som används för att låsa upp dörren så att man kommer in i sitt hus. Vi menar dock att det är en alldeles för snäv syn på elektronisk identifiering – den behöver vara vidare än så för att vara fruktbar och kunna sättas i meningsfulla sammanhang av exempelvis design, utvärdering och vidareutveckling.

Även om det är en teknisk lösning (en artefakt) med en begränsad uppgift vi avser, så kan dess utformning och sättet den införs och används på få stora konsekvenser för hela användningssituationen. Med artefakt menas här konstruerade föremål i form av olika tekniska lösningar och människors meningar kopplade till dessa. Identifieringslösningen påverkar både säkerheten i sig och den bild vi får av den e-tjänst eller det IT-system där vi identifierar oss. Dessutom påverkar den också bilden vi har av det sammanhang där vi använder identifieringslösningen. Om vi använder en e-tjänst som erbjuds av exempelvis den kommun där vi bor, påverkas också vår tilltro till kommunen och samhället av hur vi uppfattar identifieringslösningen och e-tjänsten. Samma resonemang gäller om vi köper en vara av ett privat företag på nätet. Med andra ord påverkas samhällets såväl som företagens legitimitet av hur vi som medborgare eller kunder uppfattar olika IT-lösningar.

Den här boken handlar därför om de möjligheter och utmaningar som elektronisk identifiering kan innebära för individer, organisationer och samhället. Vi talar inte om isolerade tekniska problem i första hand, utan anlägger ett vidare perspektiv på de möjligheter och problem som kommer med e-tjänster och elektronisk identifiering.

Slutsatser och erfarenheter

Den här boken rymmer slutsatser och erfarenheter som vi samlat under ett tre år långt forskningsprojekt om framtidens säkra elektroniska identifiering. Vi som skrivit boken och 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 när vi närmar oss utmaningarna och möjligheterna med elektronisk identifiering.

Bilderna vi målar upp i boken och 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 boken 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 eID – i olika roller – ska finna boken läs- och tänkvärd.

Syftet med denna bok

Vi har skrivit den här boken för att dela med oss av en del av de tankar och insikter som vi fått under projektet. Syftet med boken är att sätta ljuset på ett antal teman som framstår som centrala för utveckling och användning av elektronisk identifiering. Vi beskriver tre exempel som hämtar inspiration från våra studier inom projektet. Utifrån dessa exempel lyfter vi fram ett antal teman och diskuterar dessa samt sammanfattar utmaningar som vi sett i våra studier. Vår förhoppning är att Du som läser vår bok kan använda våra resonemang för att diskutera frågorna vidare i det praktiska sammanhang som Du befinner Dig i. Oavsett om Du finns på ett kommunkontor, i ett landsting, i en myndighet eller i en privat livssituation. Vi har inte haft ambitionen att skriva en vetenskaplig, teorirelaterad text, men Du som vill läsa forskningsbaserade publikationer från projektet hittar lästips i slutet av boken.

Forskningsprojektet

I forskningsprojektet ”Framtidens säkra elektroniska identifiering – framväxt och användning av e-legitimationer” är vi sju forskare från informatik och statsvetenskap vid Linköpings universitet (LiU) som har samverkat. Projektet finansierades av Myndigheten för samhällsskydd och beredskap (MSB) och har bedrivits under åren 2011 till 2014. Delfinansiering för forskares medverkan har också kommit från andra källor; främst Linköpings universitet och Vinnova.

I projektet har vi ur sociala, organisatoriska och tekniska perspektiv följt och kritiskt studerat utvecklingsprocesser, implementering och användning av säker elek-

tronisk identifiering i olika sammanhang. För att vi skulle förstå nuläget och kunna värdera goda framtida lösningar behövde vi till att börja med kartlägga bakgrunden till den situation vi har i Sverige idag vad gäller elektronisk identifiering. I den här boken redogör vi för den bild av utvecklingsprocessen som vår kartläggning resulterade i. Därefter har vi studerat och analyserat policyskapande och beslutsfattande kring elektronisk identifiering samt utveckling, implementering och användning i praktiken. De sammanhang vi studerat rör bland annat skolans webbaserade kommunikation med föräldrar och elever, kortlösningar för inloggning i IT-system inom sjukvården, privatpersoners uppfattningar kring säkerhet och användbarhet vid användning av eID samt hur elektronisk identifiering lyfts fram i riksdagsdebatten. I våra studier har vi valt att fokusera fem analysperspektiv.

Våra 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 i praktiken. 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 på nästa sida sammanfattar vi de fem analysperspektiven samt de kunskapsbidrag (resultat) som analysperspektiven har gett. I denna bok lyfter vi upp några av de teman som projektet rymmer.

Fältstudier av elektronisk identifiering

För att studera de teman och analysperspektiv som vi beskriver ovan har vi genomfört fältstudier. Vi har studerat elektronisk identifiering i olika sammanhang (skola, vård, privatliv och hur det diskuteras i riksdagen för att nämna några) och med olika perspektiv och metoder. Några av studierna har varit mer omfattande och har genomförts under längre tid, medan andra studier har varit kortare. 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 (exempelvis konferenser, workshops och hearings) kring utveckling av eID samt diskussioner i media. Vi har varit flera forskare i varje delstudie och samverkat vid såväl datainsamling som analys av resultaten.

Vi har fokuserat olika situationer och organisationer. Vi har pratat med människor i olika roller och studerat dokument och skeenden. För att förstå och kunna förklara det vi sett har vi tillämpat olika teorier och begrepp för att strukturera våra iakttagelser. Den här boken är inte summan av allt vi har sett och gjort under projektets tre år. Vi försöker istället att lyfta fram ett antal teman som framstår som särskilt viktiga i detta sammanhang. Det är vår förhoppning att dessa teman kan vara till nytta för Dig som läser vår bok.

Analys 1

av samspelet mellan process och olika tekniska lösningar och människors uppfattningar om dessa lösningar (artefakt)

Analys 2

av hur aktörerna påverkas av design och risker

Analys 3

av praktisk användning och tolkningar i dessa olika sammanhang

Analys 4

av vem och hur har ansvar för och kring e-legitimation

Analys 5

av framtidens säkre e-legitimationer

2011

Resultat

1. Beskrivning av utvecklingsprocessen och artefakten
2. Förståelse av berörda aktörers riskuppfattningar
3. Förklaring av användarsituationer
4. Förståelse av ansvarsutkrävande

5. Normativa råd för utveckling av säkra e-legitimationslösningar

2014

Figur 1: Undersökningens fem analysperspektiv samt de kunskapsbidrag (resultat) som analysperspektiven har gett.

Elektronisk identifiering – en virtuell konstruktion eller möjlighet att hantera det viktiga i mänskliga möten?

Utvecklingsprocessen

Framväxten av den svenska nationella elektroniska identifieringen, populärt kallat e-legitimation (eID), lägger grunden för den fortsatta utvecklingen och användningen i praktiken. Denna framväxt är även något som till dags dato inte sällan beskrivits som något av en framgångssaga.

Några förutsättningar

Utvecklingen bygger på en unik företeelse och historia här i Sverige som i sin tur är en viktig förutsättning för etablerandet av eID; det svenska personnumret. Personnumret är ett unikt nummer som delas ut av Skatteverket till samtliga folkbokförda personer i landet. Det syftar till att fungera som identifiering hos olika aktörer inom både offentlig och privat verksamhet. Det system vi har idag infördes 1947 och Sve-

rige var på den tiden unikt i världen med att på detta sätt identifiera sin befolkning. Tilldelningen av personnummer regleras i Folkbokföringslagen 18 § där det också beskrivs hur så kallade samordningsnummer tilldelas till personer som inte är eller har varit folkbokförda i landet. Den speciella förutsättningen i detta sammanhang är därmed att samtliga personer i landet har ett unikt nummer som identifierare. Andra länder kan ha andra typer av lösningar där till exempel varje relation mellan individen och en viss organisation får en egen identitet, vilket i sig skapar en större komplexitet vid identifiering.

I sammanhanget är det även intressant att många av oss ser den personnummerbaserade identifieringen som en naturlig del av vår interaktion med organisationer både inom offentlig och privat sektor. Att relativt oskyddat ange sitt personnummer ses ofta inte som något problematiskt i sig, men användandet av personnumret i samband med eID har kritiserats bland annat ur ett integritetsperspektiv. Den svenska lösningen bygger på att man som individ tillåter att ens personnummer används – att det till exempel sprids och delas i god tro mellan olika aktörer. Personnumret är i grunden vår identifiering, men vi har ringa kontroll över hur det används. Det är nog knappast någon av oss som skulle kunna svara på frågan om exakt i vilka sammanhang och i vilket syfte vårt personnummer figurerar. Det finns liksom inbyggt i själva systemet att vi godkänner den användning som förekommer så länge den inte vållar skada eller problem. Vidare är även Personuppgiftslagen (PuL) viktig i sammanhang där det rör sig om behandling av personuppgifter och syftet med denna lag är att skydda människor mot att deras personliga integritet kränks.

Hur det hela började

Behovet av elektronisk identifiering uppkom när persondatorerna blev alltmer vanliga på arbetsplatserna. Från att tidigare ha varit stora kolosser som sköttes av särskilda operatörer och matades med hålkort, blev med tiden datorn allt vanligare på våra arbetens skrivbord för att även senare göra sitt intåg i våra hem och privatliv. Den gavs även ett namn som betonade dess personliga bruk (persondatorn). När fler och fler användare på detta sätt gavs tillgång till systemen, föddes även behovet av att säkerställa behörigheten och hindra obehörig åtkomst på individnivå och behovet av att identifiera sig elektroniskt såg därmed dagens ljus. Denna utveckling skedde under 1980- och 1990-talet och vid denna tid genomfördes även ett projekt inom den offentliga sektorn, där syftet var att ta fram en identifieringslösning med hjälp

av så kallade smarta kort. I kölvattnet av detta projekt följde även diskussioner kring behovet av elektroniska identiteter och andra aktörer, som till exempel telefonoperatörer och banker, visade tidigt intresse för denna typ av lösningar.

Inom den offentliga sektorn var Skatteverket tidigt ute med att identifiera nyttan med eID och omsätta detta i praktiska tillämpningar. Då var det tydliga effektiviseringsmål som var drivande och man såg stora potentiella vinster att med hjälp av eID automatisera och underlätta samordningen av sina olika ärenden. Med hjälp av elektronisk kommunikation och identifiering utvecklades därmed i början av 1990-talet ett system för företagsdeklarationer som har beskrivits som en framgång; effektiviseringsvinsterna med denna typ av lösning var tydliga. Skatteverket försökte redan då påtala för regeringen nyttan med en ökad samordning inom myndighetssektorn kring denna typ av utveckling, men man fick dock inget gehör för sina argument.

Det dröjde ända till 1999-2000 innan de första stegen mot en sammanhållen lösning för eID inom offentlig sektor togs. Regeringen hade vid denna tidpunkt insett vikten av offentlig sektors samordning kring eID och ett projekt tillsattes för att undersöka hur en sådan lösning skulle kunna realiseras. I detta projekt deltog flera myndigheter som tidigt insett vilken nytta och vilka effektiviseringsvinster denna typ av lösning kunde medföra. Dock stod det ganska snart klart att det skulle bli mycket kostsamt att helt från grunden utveckla en egen statlig lösning för eID. Man började därför snegla på andra områden för att se om någon annan aktör kanske hade gjort något som man skulle kunna utnyttja även inom offentlig sektor. Vid denna tid hade banksektorn på ett framgångsrikt sätt redan lanserat sina elektroniska banktjänster där eID ingick och hade då en ansenlig kundbas och frekvent användning.

Bankernas lösning ansågs vara säker och tillförlitlig och därmed även lämplig att utnyttja i offentlighetens tjänst och det var på detta sätt som de första avtalen mellan banksektorn och offentliga sektorn gällande eID slöts. Den offentliga sektorn kunde därmed snabbt få tillgång till en beprövad teknisk säkerhetslösning för eID och även direkt få tillgång till dess, vid denna tid, högst ansenliga kundbas om cirka 1 miljon identifierade kunder. Arbetet resulterade i att två stora myndigheter slöt avtal med var sin bank för att få tillgång till lösningen. Detta första projekt kring utnyttjandet av en marknadslösning för offentlig sektors försörjning av eID kom även att bli vägledande för det första ramavtalet som tecknades mellan bankerna och myndigheterna och ett flertal upphandlingar har därefter genomförts för att säkra den fortsatta försörjningen av dessa tjänster.

E-tjänsterna tar fart

Eftersom användningen av eID i sig inte innebär en särskilt stor nytta för vare sig institutionella eller privata användare (jämför med om vi exempelvis skulle ha en bilnyckel utan bil - den fyller ingen större funktion i sig men är en förutsättning för att nyttja något annat) så måste denna del ingå i ett större sammanhang av tjänster och åtkomst till olika resurser. Inom offentlig sektor brukar man tala om nyttan av eID som en del i säkra elektroniska tjänster (e-tjänster), där det i kommunikationen exempelvis mellan medborgaren och myndigheten finns ett tydligt behov av att identifiera användaren på ett tillförlitligt och säkert sätt. Ett välkänt exempel på en sådan e-tjänst är Skatteverkets elektroniska deklaration (E-deklarationen) som först lanserades på webben 2002. Detta första år kunde medborgarna dock enbart se och verifiera sina uppgifter och därefter skriva under deklarationen. Följande år (2003) utökades funktionaliteten och ändringar kunde därmed göras och utvecklingen fortsatte därefter i stadig takt där funktionaliteten utökades för varje år som gick. 2006 deklarerade ca 2,7 miljoner svenskar elektroniskt. Skatteverkets E-deklaration belönades samma år med Guldlänken, priset för innovativ e-förvaltning i offentlig sektor, och myndigheten utsågs därmed till årets innovatör inom offentlig verksamhet. Skatteverkets E-deklarationsprojekt har även väckt stort intresse internationellt och Sverige sågs vid denna tid som världsledande inom området.

Därefter har den fortsatta utvecklingen och lanseringen av säkra offentliga e-tjänster med hjälp av eID varit fortsatt positiv och framgångsrik. För många av oss har detta sätt blivit helt naturligt när det kommer till att sköta kontakten med olika parter inom offentlig sektor. Även om flera stora myndigheter som till exempel Försäkringskassan, Skatteverket och CSN idag erbjuder ett stort antal e-tjänster som möjliggörs med eID, så finns det även inom kommuner och landsting många olika exempel på eID-baserade e-tjänster för medborgare och brukare. Det är även viktigt att klargöra att exemplen ovan är tagna från situationer där användare är externa i förhållande till de som tillhandahåller tjänsterna, men det finns även ett identifieringsbehov för användare som är interna; till exempel anställda vid myndigheterna ovan eller andra organisationer. Även i sådana sammanhang används sedan lång tid tillbaka elektronisk identifiering i form av exempelvis smarta kort (e-tjänstekort, e-tjänstelegitimationer etc.).

Ökat behov av gemensam samordning av e-identifiering

Utan eID fungerar inga e-tjänster där det krävs att vi är identifierade på ett säkert och tillförlitligt sätt. I takt med att vi i allt större utsträckning utför tjänster mot offentlig såväl som privat sektor via Internet ökar därmed samtidigt kraven på en säker och hållbar lösning för eID. Både medborgare och företagare samt aktörer inom såväl offentlig som privat sektor är idag beroende av att det finns en lösning som fungerar, är säker och som man känner förtroende och tillit till. Vid första anblicken kan eID tyckas vara en ganska avgränsad teknisk lösning, men den har faktiskt en desto större betydelse för bibehållandet och vidareutvecklingen av vår moderna elektroniska förvaltning; den har därmed en mycket viktig funktion att fylla i ett medborgerligt såväl som institutionellt sammanhang.

Under åren har flera olika myndigheter varit inblandade i processen kring den nationella lösningen för eID och detta har i sin tur medfört att den centrala styrningen och koordineringen av detta område uppfattats som otydlig. Utvecklingen inom området har även tydligt drivits av stora och framgångsrika myndigheter i samarbete med aktörer inom banksektorn. Därmed har de parter som redan insett och realiserat nyttan av eID i sin verksamhet kunnat fortsätta denna positiva utveckling medan andra offentliga aktörer, som inte nått denna utveckling, riskerat att hamna på efterkälken. Den svenska modellen i sammanhanget, det vill säga den marknadsbaserade lösningen, har även utsatts för en hel del kritik av aktörer som menat att staten själv skulle stå för infrastruktur och utgivning. Under tiden har det dock växt fram en tydlig medvetenhet kring behovet av att öka samordningen av arbetet på nationell nivå över myndighetsgränserna. Även om det förekommit olika typer av samordningsinitiativ har i huvudsak stora aktörer (myndigheter) agerat i egen sak; man har utvecklat och realiserat nyttan av eID främst sett ur sitt eget verksamhetsperspektiv.

Förslag kring hur den framtida mera centralt samordnade eID-lösningen skulle kunna se ut för offentlig sektor presenterades först av Verva i deras slutrapport innan myndigheten avvecklades samt därefter i två utredningar som genomfördes av E-delegationen. Dessa utredningar hade en sak gemensamt: De såg ett klart och tydligt behov av att samordna området över myndighets- och organisationsgränserna inom offentlig sektor, enligt svensk myndighetsmodell, för att främja den fortsatta utvecklingen och positiva spridningen inom området. Under sommaren 2010 tillsattes ytterligare en utredning för att undersöka hur en mer samordnad lösning för eID i Sverige skulle kunna se ut. Utredningen, som utfördes under hösten, presenterade

sitt förslag i december samma år. Motivet för denna utredning var främst att den dåvarande upphandlingsmodellen för eID var på väg att fasas ut och i akut behov av att förnyas. Syftet angavs även som att beskriva uppdraget för en utsedd myndighet som skulle leda arbetet med att utveckla och samordna nästa generations lösning för eID. Utredningen skapade dock i sig en hel del turbulens inom e-legitimationsområdet när den presenterades. Den beskrev som förväntat uppdraget för den myndighet som skulle tilldelas uppdraget att samordna området, men innehöll även en konceptuell och emellanåt mycket detaljerad ritning av den tekniska lösningen. Denna aspekt uppfattades som ytterst oväntad av flera av de berörda parterna inom området och utredningens slutrapport mottogs med stort intresse och även en hel del negativ kritik. Den främsta kritiken som framkom var att arbetet hade bedrivits på ett forcerat sätt och att berörda parter inte hade hörts i tillräcklig utsträckning. Ungefär samtidigt som utredningen skapade denna turbulens inom området bildades E-legitimationsnämnden den 1 januari 2011, med sin myndighetshemvist hos Skatteverket, med uppdraget att samordna, stödja och utveckla området.

E-legitimationsnämndens uppdrag och arbete

E-legitimationsnämnden (nämnden), en egen myndighet underordnad Näringsdepartementet, leds av en grupp på sju ledamöter utsedda av regeringen för bestämd tid. Skatteverket står som värdmyndighet och kan därmed bidra med personal, lokaler samt administrativa tjänster. Nämndens uppdrag är att samordna och stödja offentlig sektors behov av säkra lösningar för elektronisk identifiering och signering (underskrift) inom myndigheters, kommuners och landstingens e-förvaltning. Det ingår även i nämndens uppdrag att delta i olika typer av internationella initiativ kring till exempel standardisering, samarbete samt informationsutbyte inom e-legitimationsområdet. Sedan starten har nämnden arbetat mycket aktivt med att utveckla nästa generations sammanhållna eID-lösning. Fokus på detta arbete har varit att ta fram en lösning för hela den offentliga sektorn, men lösningen i sig ska även möjliggöra användning av detta eID i privat verksamhet.

Under sitt första verksamma år satte nämnden upp flera långsiktiga mål, bland annat att:

- verka för ökad användning av e-tjänster i samhället genom en svensk e-legitimation (eID)

- verka för kostnadseffektiva och transparenta villkor för såväl leverantörer av e-tjänster som för utfärdare av eID
- skapa förutsättningar för fler utfärdare av eID samt att slutligen tillgodose att övergången mellan den nuvarande och kommande lösningen för eID kan ske på ett smidigt sätt

Till en början angavs att målet för den kommande lösningen var att denna skulle finnas tillgänglig 2013, men denna tidsplan kom senare att revideras. Under sitt första år genomförde nämnden ett flertal aktiviteter som kan kopplas till dess etablering. Med hänsyn till den kommande lösningen skapades även en teknisk testmiljö.

Under 2012 fokuserade nämnden på att skapa ett regelverk med tillhörande tillitsramverk för Svensk e-legitimation. Detta ramverk ska fungera som grund för samverkan. Den ska också utgöra förutsättningen för den tillit man önskar skapa mellan de olika ingående aktörerna i den kommande lösningen. Under detta år fortsatte nämnden att arbeta med målet att den kommande lösningen ska finnas tillgänglig under 2013, men lade samtidigt till att en lagändring måste ske som förutsättning. Detta gäller ett lagförslag om ett Valfrihetssystem med hänsyn till tjänster för eID som då skulle utgöra ett alternativ till Lagen om offentlig upphandling (LOU) i dessa sammahang. I korthet går detta ut på att en aktör inom offentlig sektor kan besluta om att inrätta valfrihetssystem för tillgång till tjänster för elektronisk identifiering och därefter välja eID från valfri godkänd leverantör som finns med i systemet. För att som leverantör ingå i systemet krävs att nämndens uppställda krav uppfylls. På detta sätt går man ifrån tidigare komplexa upphandlingsförfarande till en mer flexibel lösning för e-tjänsteleverantörerna.

Vid E-legitimationsdagen 2012, ett årligt evenemang instiftat av nämnden, talade IT- och energiministern Anna-Karin Hatt om att e-legitimationer är en mycket viktig och helt avgörande fråga. Hon uttryckte det som att ”Utan säker e-legitimation lyfter inga e-tjänster” och framhöll därmed vikten av en tillförlitlig, hållbar och säker lösning för identifiering och underskrift som en förutsättning för offentliga sektorns tillhandahållande av säkra e-tjänster. Vidare framhöll hon även en annan viktig aspekt i detta sammanhang; att e-legitimationer är en mycket viktig del i den offentliga sektorns interna effektiviseringsarbete. Sverige beskrivs som ett framgångsland med hänsyn till vår höga digitaliseringsgrad och det bedrivs en offensiv politik kring det som brukar kallas ”den digitala agendan”. Det är därmed viktigt att inse att

en fungerande svensk eID-lösning ingår som en mycket viktig del i denna agenda.

2013 arbetar nämnden med ett antal olika områden som viktiga förutsättningar för den kommande eID-lösningen. I början av året presenteras en ny version av regelverket för Svensk e-legitimation. Under första halvåret var arbetet intensivt med att införa lagändringen med hänsyn till valfrihetssystemet i fråga om tjänster för elektronisk identifiering. Under våren gjorde nämnden en upphandling kring de centrala tjänsterna i den kommande lösningen. Dessa avser tjänster som nämnden kommer att tillhandahålla via sin roll som central sammanhållande part i den kommande lösningen. Den 1 juli 2013 träder så lagen kring Valfrihetssystemet i kraft och samma månad ingicks även avtal mellan nämnden och en leverantör kring de centrala tjänsterna. I juli månad publiceras även en ny version av regelverket. Nämndens arbete intensifieras under hösten 2013 med bland annat presentationen av en beslutad ersättningsmodell, det vill säga den modell som beskriver den ekonomiska ersättningen som ska utgå till utfärdarna av eID. Dock stod det under året klart att det skulle dröja till minst 2014 innan alla förutsättningar för den kommande lösningen var klargjorda och en ny lösning för Svensk e-legitimation skulle kunna lanseras på bred front.

Sammanfattningsvis kan sägas att nämnden har haft ett mycket omfattande uppdrag. I nämndens mandat har ingått att både samverka kring, stödja samt utveckla nästa version av nationell lösning för eID. Denna process har nämnden bara delvis haft möjlighet att styra, då det skett i samverkan och förhandling mellan staten, privata företag och andra organisationer. Hela processen präglas av en svår uppgift med komplexa förutsättningar, frågor och kravställningar inom områden som teknik, juridik, säkerhet samt ekonomi. Nämnden har inte haft inflytande i hela processen och saknat det koordineringsansvar som andra ibland väntat sig att de haft. Den senaste tiden har nämnden även arbetat med användargränssnitt och dessas användbarhet. I skrivande stund (februari 2014) väntar vi på ett entydigt startdatum för denna nya lösning. Samverkan är processer som tar tid, men som samtidigt ger möjligheter att förankra och koordinera beslut och verksamheter innan de tas i bruk.

eID används i olika roller och ses på olika sätt.

eID i flera skikt

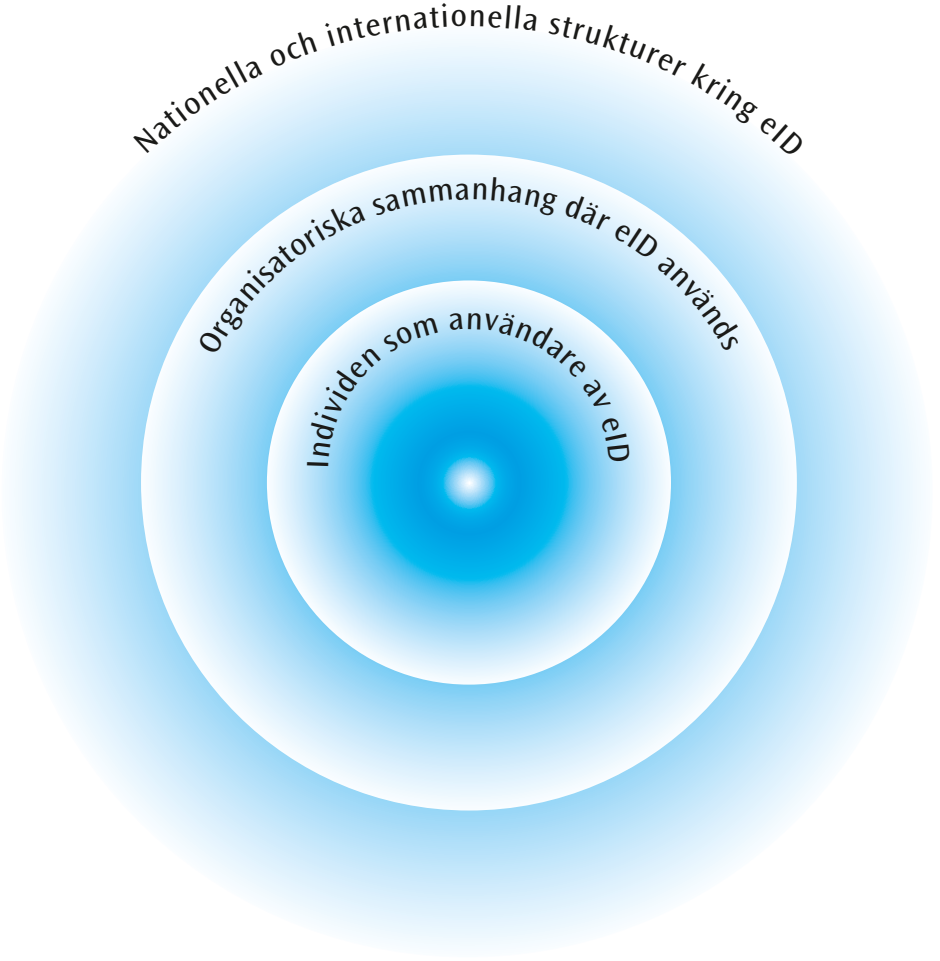
I förra avsnittet såg vi hur lösningar för elektronisk identifiering har vuxit fram i samspel mellan tekniska, politiska och organisatoriska sammanhang. Det är således många aktörer och organisationer som har intressen av utvecklingen av eID. Betydelsen av eID varierar därför också beroende på när, hur och av vem den används. Innan vi går in på våra illustrationer av hur eID kan användas vill vi visa en modell av hur eID kan förstås i relation till politiska och organisatoriska förutsättningar. Med denna modell vill vi även visa att våra vetenskapliga tolkningar grundas på flera perspektiv som vi beskrev i inledningen.

eID bäddas in i många olika sammanhang och ses på olika sätt beroende på vilket perspektiv som är utgångspunkt. Våra resultat i detta forskningsprojekt har visat att

eID ofta ses som en angelägenhet för individen, och det ligger på individen att själv skaffa och använda den typ av eID som passar i sammanhanget. Men individens användning av eID sker i olika roller i relation till de organisationer där hen är verksam och även de nationella och internationella strukturer som formar eID.

Det individen gör i rollen som användare ser vi som en kärna i förståelsen av eID. Kring denna kärna finns närmast de sammanhang och organisationer som hen möter i sin vardag. Det kan vara på arbetsplatsen, som medborgare och skattebetalare, vid ansökan om exempelvis körkortstillstånd eller i roller som anhörig och förälder till barn i skolan. I sådana organisationer som statliga myndigheter, kommuner, skolor och arbetsplatser utvecklas olika förväntningar, kulturer och praxis kring eID. Vi ser det här som ett första skikt närmast individen och användaren. I dessa organisationer finns också individer som använder eID i sina professionella roller. Kring dessa organisationer finns ett nästa skikt av samhälleliga och politiska strukturer där lagstiftning, regler och internationella överenskommelser reglerar hur eID tillåts och kan utvecklas och användas. Detta ser vi som ett yttre skikt av de socialt formade betingelserna kring eID. I bilden intill visar vi hur vi ser att eID kan betraktas och tolkas utifrån olika skikt.

När vi tolkar hur eID utvecklas har vi utgått från en modell av att eID formas i samspel mellan olika skikt. Det innebär att vi för att förstå en helhet inte kan se något av skikten eller sammanhangen avskilt. Vi kan dock av analytiska skäl välja att sätta fokus på ett skikt i taget, men med utgångspunkten och målet att förstå en helhet. Betydelser och användning av eID formas av att det finns kringliggande skikt och strukturer, där olika tolkningar utvecklas. I alla dessa skikt ser vi eID som en socialt och tekniskt formad företeelse och artefakt. Med detta vill vi framhålla att de tekniska och sociala betydelserna av det som kan ses som artefakten – eID – formas i ett ömsesidigt samspel. Det innebär att vi har ett så kallat socio-tekniskt perspektiv på tolkningarna av eID. Vi ser både till de sociala och materiella dimensionerna av tekniken och gör därmed anspråk på att se teknik i sammanhang och betonar olika delar av dess livscykel, där bland annat användning enligt ovan är centralt i samband med utveckling och införande.



Figur 2: Modellen visar hur eID formas i samspel mellan olika skikt.

eID i ett globalt sammanhang

Om vi börjar i det yttre skiktet av modellen så finns det idag ett flertal diskussioner om hur vi hanterar identitet, identifiering och informationssäkerhet i en global internetbaserad värld. Staters och globala företags övervakning och analys av enskildas aktiviteter på nätet, är tekniskt möjlig, men i flera fall etiskt oacceptabel, politiskt svårmotiverad och i flera avseenden även juridiskt ohållbar, såvida det inte handlar om grov brottslighet eller liknande som tydligt sanktionerats.

I takt med den snabba tekniska utvecklingen och lavinartade ökningen av information som görs tillgänglig, så halkar ofta juridiken, politiken och etiken efter. I många länder görs därför försök att utveckla normer och regler för hur vi kan identifieras och följas generellt och inte minst i elektroniska miljöer. Utvecklingen av den svenska elektroniska identifieringen kan ses i ljuset av dessa internationella sammanhang. Staternas engagemang i dessa frågor drivs av möjligheterna att upprätthålla sin demokratiskt grundade makt över medborgare, aktiviteter och verksamheter inom statens territorium. Det innebär att staten ses som legitim av sina medborgare och andra. Statens legitimitet grundas på att vi har tillit till den och att statens agerande sker inom ramen för de lagar som finns på området. Därför gäller det för stater att också hänga med i den tekniska utvecklingen och internationella debatten för att ses som legitim. I detta sammanhang bidrar även samarbeten inom EU till att sträva efter en likartad utveckling av elektronisk identifiering i medlemsländerna.

Som medborgare i en stat får vi en mängd rättigheter och skyldigheter. Det innebär att vi som individer har relationer till staten och dess myndigheter där vi behöver kunna identifiera oss. Som medborgare kan vi genom att identifiera oss få del av de rättigheter som staten ger oss. I forskningen om medborgarskap ses det ofta som en politisk konstruktion. Det innebär att vi politiskt skapar innehåll och betydelser av medborgarskapet. På så sätt skapas även politiska betydelser av elektronisk identifiering.

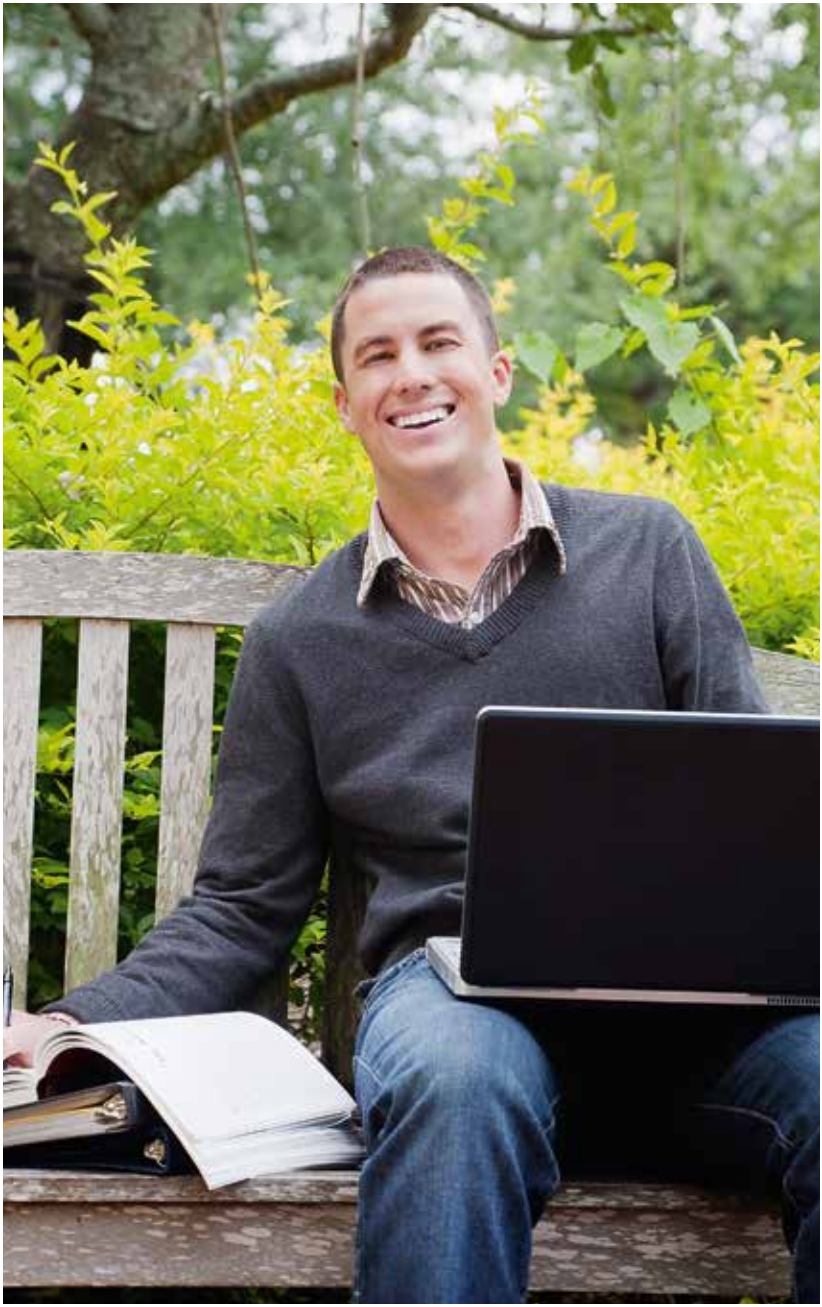
Den svenska statens agerande, som vi sett i avsnittet ovan, visar att utvecklingen av eID i hög grad skett genom förhandling och samverkan mellan staten, privata företag som bankerna och genom att ta utgångspunkt i teknisk utveckling och EU:s policyer på området. Förhandlingar och nätverksbyggande ses ofta som det vanligaste sättet att utveckla nya policyer idag. Utvecklingen av eID på nationell nivå ligger i linje med forskningen om politik och styrning som utvecklat begrepp och teorier om nätverksstyrning och det som kallas förhandlingsstaten. Alltså visar det sig att de politiska nationella tolkningarna av eID utvecklas i samspel med andra stater

och internationella aktörer i ett yttre skikt, men också inåt mot privata såväl som offentliga organisationer nationellt.

eID i ett organisatoriskt sammanhang

I det organisatoriska skiktet formas tolkningar och betydelser av eID-lösningar av organisationens uppdrag och syfte. Offentliga organisationer ska agera rättssäkert, effektivt och demokratiskt. Privata organisationer kan däremot ha vinstdrivande intressen och behöver inte vara demokratiskt öppna. Det får även implikationer för hur de organiserar och tolkar behov och användning av eID. Behovet av att identifiera oss med olika former av eID finns såväl i rollen som medborgare (gentemot offentliga organisationer), i rollen som kund (gentemot privata företag; till exempel banker) eller i rollen som medarbetare i ett företag eller i en offentlig organisation (för att komma åt information som till exempel är känslig). Det eID-kort som man som individ använder i sitt arbete (till exempel ett e-tjänstekort i vården) är kopplat till beslut och rutiner inom den organisation man som medarbetare tillhör. Det ger medarbetaren möjlighet att bekräfta vem hen är och vilken information hen har rätt att ta del av. I organisationer där känslig information om enskilda hanteras, som exempelvis i vården, är det viktigt att bara de som har behörighet kan ta del av informationen. Sådana behörigheter kan även de grundas på att man har en viss position, legitimitet eller en viss kompetens, till exempel att man är anställd som läkare. När man inför eID i en organisation kopplar man därmed också samman individen och organisationen med olika nationella och internationella strukturer och normer. I vården innebär det exempelvis att läkaren har viss behörighet genom att vara godkänd som läkare och därmed får rättigheter att logga in och ordinera läkemedel elektroniskt. På liknande sätt utvecklas och anpassas både eID och organisationer i förhållande till sina specifika uppdrag och uppgifter.

Det samspel mellan skikten ovan som exemplet visar är en illustration av när tekniken och dess sociala sammanhang har framträtt på flera olika sätt i våra studier. Andra exempel är när personer som arbetar i en organisation med frågor kring eID knyter samman den valda organisatoriska lösningen med krav som förs fram på nationell nivå. Detta sätt att arbeta växelvis med nationella och organisatoriska lösningar visar på ett tydligt sätt att eID inte kan ses isolerat, utan måste betraktas som en del av en större helhet. Här kan det dock behövas ytterligare möjligheter för att underlätta lärande mellan såväl de olika nivåerna som mellan organisationer.



Den privata rollen vävs samman med yrkesrollen.

Växla mellan privata och offentliga roller

I organisationer kan vi ha olika fokus och agera olika både som offentliga och privata personer. Vi har roller som medborgare i relation till offentliga sammanhang, men vi är även privatpersoner som kan agera med vår eID för att ha relationer till våra arbetsgivare, och exempelvis banker och andra privata organisationer. För den enskilde individen är det inte alltid klart hur dessa olika roller samordnas; rollerna kan till och med krocka. Elektroniska identifieringssystem som utfärdas av arbetsgivare påverkar individen både i rollen som medborgare och i yrkesrollen. Det finns inte alltid tydliga gränser mellan det privata och det yrkesmässiga att luta sig mot när det gäller eID. Ett e-tjänstekort som är kopplat till arbetet och den yrkesmässiga rollen, är också privat eftersom det också är kopplat till den enskilda individen som är ansvarig

för kortet och dess användning. Ett e-tjänstekort kan även ha funktionen av att vara godkänt som fysiskt ID-kort i andra sammanhang, även de strikt privata (som privat Bank-ID eller legitimation). Det kan, som vi noterat i tillämpning, också användas på arbetet för att få tillgång till service som exempelvis att köpa fika eller betala parkeringen på arbetsplatsen. Vi har också i våra studier sett att personer använder sitt privata bank-ID i sitt arbete när de uppfattar att de lösningar som tillhandahålls av arbetsgivaren inte känns tillräckligt säkra vid hantering av känsliga uppgifter. Detta gör att den privata rollen vävs samman med yrkesrollen vid användning av eID.

Denna sammanblandning av det privata och det professionella kan vid en första anblick te sig tämligen lockande, integrativ och till och med oproblematisk. Även om det kan tyckas vara självklart att det vore mer praktiskt med ett enda kort som kan användas i alla sammanhang – oavsett i rollen som medborgare eller i sin yrkesroll – har vi i våra studier sett att det uppstår mycket diskussion om detta, kring till exempel risk och integritet. Enbart några få användare säger sig tycka att det vore praktiskt med ett enda kort som innehåller allt man behöver. De flesta är inte intresserade av att koppla på ”privata” funktioner på ett tjänstekort, och använder tjänstekortet enbart i jobbet. De vill istället ha en tydlig separation mellan det privata och det yrkesmässiga.

Detta analysperspektiv att eID måste ses ur olika sammanhang och skikt, som en både teknisk och/eller materiell och social artefakt, som kan tolkas ur olika perspektiv, har genomsyrat alla våra analyser och ligger till grund för de fortsatta resonemangen här.

eID i skolan

Karl har just betalat räkningarna via sin Internetbank. Han fortsätter att använda bankdosan när han skriver in adressen till lärplattformen för dottern Lottas skola. Han måste logga in i applikationen för att kolla vilken dag det är friluftsdag. När han loggat in ser han den uppgift i samhällskunskap om djurs rättigheter som ledde till heta diskussioner vid köksbordet förra helgen. Han ler för sig själv och minns; svåra och utmanande frågor! Han letar vidare efter datumet för att ta reda på när Lotta ska ta med skridskorna och matsäcken till skolan. Men istället ser han att han måste kvit-

tera till dotterns mentor att han tagit del av uppföljningen av den individuella utvecklingsplanen. Lärarna har tillsammans med dotterns mentor lagt in olika delar och registrerat hela dokumentet. Han klickar OK för att göra en säker bekräftelse att han tagit del av den individuella utvecklingsplanen. Till slut hittar han informationen han söker. Skridskorna och matsäcken ska med redan i övermorgon. Undrar om hon har växt ur skridskorna? Det är mycket nu!

I exemplet ovan använder Karl sitt bank-ID för att logga in på den webbplats som den kommunala skolan använder för sin kommunikation med föräldrarna. Han och dotterns lärare kan här bland annat dela och bekräfta hanteringen av de skriftliga omdömen som lärarna ger och den individuella utvecklingsplanen (IUP). I många skolor, både i kommunal regi och friskolor, finns i dag sådana plattformar med intentionen att underlätta och förbättra kommunikationen mellan hem och skola.

Idag ställer skollagen krav på att alla elever har dokumenterade IUP. Just detta krav har i många kommuner lett fram till att man skapat eller köpt in olika IT-system eller lärplattformar för ändamålet. Detta för att ge bättre skydd åt känslig information, och för att underlätta och förbättra kommunikationen mellan hem och skola. Lagens krav på IUP kan ses som en trigger, eller en kritisk uppgift, som lett till att nya system har införskaffats och införts. I våra analyser har vi sett att det ofta är nyheter eller skyldigheter med krav på högre säkerhet som leder till att nya IT-system utvecklas. När högre säkerhet krävs för en viss typ av information så ökar hela verksamhetens medvetenhet om vikten av god informationssäkerhet.

Det är dock inte alltid enkelt att få sådana här system att fungera på ett säkert sätt i praktiken. De ska även fungera för många olika personer; användare i olika roller med olika förväntningar, vanor och behov. Lärare, elever, föräldrar och bland annat administratörer på skolorna måste kunna komma åt informationen. Att hantera information säkert, och gärna med olika säkerhetsnivåer för olika ändamål, och samtidigt hålla den tillgänglig för de personer som har rätt att komma åt den, är inte helt enkelt. Dessutom ska systemen vara enkla att använda. Utmaningen är att skapa säkra IT-system som samtidigt är enkla och intuitiva att använda i vardagen.

Bland lärare, föräldrar och elever finns det personer med vitt skilda intressen, kompetenser, behov och resurser för att använda dessa IT-system. Utmaningarna är särskilt stora när det gäller den här typen av system som måste kunna inkludera alla.

Säker informationshantering blir på så sätt beroende av tillgång till datorer, till nätet och kompetens att använda tekniken. Även andra kompetenser som språk och insyn i skolans verksamhet är viktiga aspekter av säker informationshantering. Att förstå användares olika förutsättningar och förmågor är viktigt för att kunna skapa system som både är säkra och används på säkra sätt.

Lärarna är en kritisk grupp för att dessa system ska få förväntade positiva effekter och kunna användas väl i vardagen. I de skolor som vi studerat har lärarna kunnat logga in och identifiera sig på olika sätt. Oftast har de bara haft ett användarnamn och lösenord. I några sammanhang användes eID, men det upplevdes som komplicerat. Då plattformarna hade både pedagogiska och administrativa mål, så var det inte alltid enkelt för dem att länka samman de olika behoven. I skolan finns en arbetsorganisation och kultur som är självständig, rörlig och varierande, vilket inte passade ihop med dessa system för inloggning. Lärarna var exempelvis sällan inloggade längre stunder vid samma dator. Rektorerna, som arbetsledare, hade till uppgift att prata positivt om dessa system och ”sälja in” dem till medarbetarna. Men i vardagen föll den uppgiften ofta bort bland de mängder av andra saker som rektorerna måste hinna med. Därför är det tydligt att när det ställs ökade krav på säker hantering av information och identifiering så påverkas även andra delar av organisationen.

Plattformarna används även av eleverna, som ofta loggade in med ett personligt lösenord, men det var inte alltid som eleverna förstod att dessa lösenord var viktiga värdehandlingar. Ibland delade eleverna lösenord med varandra för att lösa någon uppgift i skolan. Det kanske inte vore ett problem om det bara handlade om till exempel anvisningar till en uppgift, men då det även finns känslig information i samma system kan det bli problematiskt. Precis som i exemplet ovan så kan personlig och ibland känslig information blandas med helt allmän information om skoltider och exempelvis friluftsdagar.

Föräldrarna är en kritisk grupp som loggar in på plattformarna med sina privata eID. Meningarna är delade angående tilliten till och användbarheten av plattformens olika funktioner. En del av dem såg inga problem med att använda sitt eID i kommunikation med skolan, medan andra tyckte att det var krångligt och onödigt omständligt, speciellt för att komma åt enkel information i vardagen. Det var inte ovanligt att föräldrarna lånade sina barns inloggningsuppgifter för att få tillgång till informationen. Många i denna grupp ställde sig frågande till blandningen av deras barns information av olika känslighetssgrad och användningen av olika inloggnings-

lösningar som hade en högst varierande säkerhetsgrad.

E-tjänstekort i vården

Måndag morgon. Sen oktober. Höst. Regn. Ruggigt. Vårdcentralen i Mellanstad har just slagit upp sina slitna aluminiumbeklädda dörrar och välkomnar de första patienterna för besök. Egentligen har personalen redan varit i gång 1,5 timme – via telefonbokningen och rådgivningen, så patientkontakterna har redan startat. Det ser ut att bli en hektisk och innehållsrik dag; likt andra måndagar. Det gäller att hålla bokningarna igång och prioritera. För Lisa, läkarsekreterare på vårdcentralen sedan sju år tillbaka, är det än mer hektiskt. Hon har glömt sitt passerkort hemma i sommarjackan. Det fungerar inte med sommarjacka idag; hösten är definitivt här, vinterjacka på! Passerkortet behövs ju numera inte bara för att komma in i personalentrén utan också för att komma åt patientjournalerna på datorn och bokningarna i hennes arbete i receptionen på vårdcentralen.

Hon går in i byggnaden när Sven kommer och säger hej. Att åka tillbaka hem och hämta kortet är inget alternativ; hon tillbringade ju helgen i sommarstugan med familjen fem mil bort för att få ut det mesta av oktober som hittills har varit ovanligt varm. Dags att dra igång rutinen för att få ett reservkort för att få dagens arbete att fungera. Hur var det man gjorde nu igen? tänker Lisa. Hon talar högt med sig själv. Är Ola här idag; han brukar ju ha koll på det här. Jaså, inte här. Hmm… kanske Adele vet, hon är ju IT-samordnare för oss. Jo, Adele vet, hon har reservkort och utfärdar ett sådant för dagen i dialog med IT-personalen centralt. Skönt. Igång med jobbet – men sen! Redan… och dagen som knappt har börjat. Patienterna står i kö och Lisa springer redan mellan receptionen och skrivaren för att få fart på dagens inbokade besök. Det är viktigt att patienterna blir nöjda; ja viktigast av allt.

Det är lite krångligt med e-tjänstekortet för att komma åt patientdata och journalerna tycker Lisa och hennes kolleger. Kortet måste sitta i datorn hela tiden för man ska kunna komma åt informationen. Samtidigt måste Lisa ta med kortet för att kunna skriva ut papper i skrivaren. Där försvinner värdefull tid att dra ur och sätta i kortet igen. Ibland låter hon kortet sitta kvar i datorn i receptionen när hon visar patienter vägen till undersökningsrummen eller till provtagningen, eller till och med diskuterar kommande besök med sina kolleger – det blir mera praktiskt så. Det måste ju gå snabbt med en sådan kö med patienter, och så vill jag fika med kollegorna också, tänker Lisa. Vi har ju personalfesten nästa torsdag att planera. Sen är det ju läkarkandidaten som behöver komma åt information också. Hon har inget kontor än, de är trångbodda på vårdcentralen och hon har heller ingen egen dator så att hon brukar låna Lisas dator för att komma åt patientinformation och kunna läsa på när hon går bredvid. Det känns OK tänker Lisa, vi behöver hjälpa dem att komma igång så att de lär sig jobbet.

Lisa funderar på vad som har förändrats mot förr. Det var inte länge sedan de hade journaler på papper. Då krävdes ingen inloggning. Alla som fick tag i journalerna kunde läsa. Varför blir det annorlunda nu på datorn? Och varför räcker det inte med lösenord som för det gamla journalsystemet som bara de hade här på vårdcentralen? Hon har sitt favoritlösenord som hon minns väl. Det gick ju heller inte att glömma i jackan. Det har blivit krångligt och tar mera tid nu. Var det meningen? Har det verkligen blivit säkrare med tanke på krånglet? Kanske har nya risker tillkommit?

Säker identifiering är ett lagkrav för att skydda känslig information (till exempel patientdata), som man i berättelsen ovan åstadkommer genom att logga in i journalsystemet med hjälp av ett personligt kort (e-tjänstekort) för att säkerställa att endast behöriga kan komma åt informationen i patientjournalsystemet. Kravet på säker identifiering är något som alla vårdgivare behöver följa. Hur ska detta uppnås samtidigt som man måste ta hänsyn till en vårdverksamhets vardag som ofta är rörlig, snabb och med ständigt behov av tillgång till information? Att det behövs en katalog för att hålla ordning på vilka som är behöriga och ska komma åt informationen är en

annan förutsättning. Att det behöver vara en säker men samtidigt användbar teknik är en annan förutsättning, följt av rutiner för att på ett säkert sätt kunna hantera (utfärda, använda och avsluta) den teknik som har valts för identifiering. Att organisera för detta och att välja en fungerande, säker och användbar teknik för att uppnå verksamhetens mål är utmanande i sig. Mötet med en vårdvardag – med höga krav på kvalitet i vården, patientmöten och upplevd stress – gör inte saken mindre komplex.

Våra studier i detta projekt pekar på att arbetet med e-tjänstekortet har underskattats på flera punkter vad gäller dess komplexitet. Det tekniska sammanhang som e-tjänstekortet som artefakt har kommit in i har underskattats. Det har till exempel uppstått problem med prestanda kring e-tjänstekortet givet olika versioner av operativsystem på klientdatorerna. Införande av e-tjänstekort har inte heller fullt ut tagit hänsyn till att en till synes begränsad artefakt påverkar sjukvårdspersonalens vardag och systemanvändning i så stor utsträckning som berättelsen ovan visar. Vi har också noterat att det finns skillnader i hur olika professioner tar till sig teknik i vårdvardagen; vilket utrymme man förväntar sig och tar i utvecklings- och införandeprocesser. Vi har sett att även tidigare erfarenheter av systeminförande spelar stor roll för hur man uppfattar och tar till sig ny teknik. Här spelar också kompetenser in och vilken position man har i organisationen. Det finns med andra ord en betydande verksamhetsdimension som gör skillnad. Detta pekar också på behovet av att kommunicera nyttan kring säker hantering och identifiering inom vården när det handlar om att skydda känslig information. Enkelhet i användningen även av en säker e-identifieringslösning, som e-tjänstekortet är ett exempel på, behöver stå i fokus; annars finner användare i vården olika sätt att utföra sin verksamhet på ett effektivt sätt oavsett säkerhetsnivå. Säkert får inte vara synonymt med krångligt och omständligt – då blir det inte säkert i praktiken!

eID och identitet

Fatima är ensamstående mamma till lille Hadi, två år. Hon arbetar som receptionist på Stadshuset och Hadi går i förskolan, men en dag i veckan är hon föräldraledig för att hon och Hadi ska få mer tid tillsammans. Sent en fredagskväll när Fatima äntligen fått sonen att somna kommer hon på att det är dags att ansöka hos Försäkringskassan om att ta ut fler dagar i föräldraförsäkringen för de

kommande månaderna. Hon har redan lämnat in sin ansökan på jobbet, så då är det bäst att hon ser till att ordna det administrativa med Försäkringskassan också – annars blir inkomstminskningen väl kännbar.

Hon kryper upp i soffan i vardagsrummet med sin bärbara dator och skriver in adressen till Försäkringskassans webbplats i webbläsarens adressfönster. Sedan loggar hon in på "Mina sidor" med hjälp av den e-legitimation som hon ordnat genom Internetbanken. På "Mina sidor" kan hon ansöka om att fortsätta ta ut föräldradagar på fredagarna under resten av våren. När hon har fyllt i vilka dagar det gäller i det elektroniska formuläret blir hon ombedd att signera sin ansökan. Även det gör hon med hjälp av sin e-legitimation.

När Fatima är klar med ansökan känner hon sig lättare om hjärtat – skönt att ha det avklarat. Nu ska hon nog ta en kopp te och läsa en stund innan hon själv går och lägger sig.

Offentliga e-tjänster används i det här fallet för kommunikation mellan myndigheter och medborgare. För många e-tjänster måste medborgarna använda sig av eID för att bekräfta sin identitet. Det faktum att kommunikationen sker via nätet har vissa praktiska implikationer. När Fatima sitter i soffhörnet med sin bärbara dator finns det ingen handläggare närvarande som kan se hennes hudfärg, kläder, tatueringar och piercings. Till skillnad från vid ett telefonsamtal finns det heller ingen tjänsteman som kan höra hennes karaktäristiska skånska dialekt. Och då hon fyller i ett elektroniskt formulär är det heller ingen anställd på Försäkringskassan som kan se hennes synnerligen individualistiska handstil.

Faktum är att ett ökande antal av de ärenden som kommer in till Försäkringskassan behandlas helt och hållet digitaliserat och automatiserat av ett IT-system. När Fatimas identitet bekräftats sker beslutsfattandet automatiskt – det behöver alltså inte sitta en handläggare "på andra sidan" och läsa och bedöma de uppgifter som Fatima lämnat. Det innebär att alla ärenden av samma slag bedöms enligt exakt samma regelverk och mall – inga individuella avvikelser sker. Med den utgångspunkten är det lätt att argumentera för att maskiner är de perfekta byråkraterna, och att likabehandling av medborgarna och därmed rättssäkerheten stärks när det är ett IT-system

som fattar besluten istället för handläggare av kött och blod. Detta kan betraktas som positivt då likabehandling är ett av den svenska offentliga förvaltningens överordnande värden.

Genom att använda Försäkringskassans e-tjänster med säker identifiering är alltså, som diskuterats ovan, Fatimas identitet i flera aspekter dold för Försäkringskassan. Samtidigt bidrar användandet av eID till ett starkt fokus på just identifiering – när inga andra sätt finns att styrka personens identitet och rätt till förmåner i socialförsäkringen blir identifieringen viktig. I exemplet med Fatima är det hennes personnummer i kombination med eID som är nyckeln till att få tillgång till de välfärdstjänster hon efterfrågar. Personnumret ger myndigheten (Försäkringskassan) information om vilka förmåner Fatima har rätt till, och genom e-legitimationen bekräftas kopplingen mellan den fysiska personen Fatima och personnumret som en representation av henne. Konstruktionen av medborgarskapet sker då utan personliga möten och rätten till de ersättningar och stöd som medborgarskapet ger skapas med automatik.

Det kan framstå som en paradox att e-tjänster och användandet av eID å ena sidan bidrar till ett starkt fokus på identifiering (vilket kan uppfattas som ett hot för integriteten), samtidigt som medborgarens identitet i flera aspekter döljs (vilket kan uppfattas som ett större utrymme för lika och rättvis behandling). Medborgarskapet och identiteten uttrycks i det här fallet med hjälp av eID elektroniskt utan personliga möten. Detta kan på sikt leda till att vi ser medborgarskapet som en virtuell konstruktion där kopplingarna till andra människor blir mindre viktiga eller så ger det oss möjligheter att just hantera det viktiga i mänskliga möten. Betydelser av medborgarskap och tillit till statens möjligheter och ansvar för att stödja medborgare formas, eller konstrueras, då på förändrade eller nya sätt och vi vet ännu inte hur och vilka konsekvenser detta kan få på sikt.

Informationssäkerhet är **mer** än lösenord och **kryptering**, som att ta hänsyn till och **utveckla** verksamheten.

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 av 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 både om det tekniska och om 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, det vill säga ”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 ledningsarbetet. 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.

…att diskutera

- Vilka erfarenheter har du av offentliga e-tjänster – i tjänsten såväl som privat?
- Påverkas ditt intryck av en offentlig organisation av dess webbplats och e-tjänster? Hur?
- Hur arbetar ni i er organisation med värden, attityder och uppfattningar om säker hantering av information genom elektroniska plattformar och system?
- Om de flesta användare upplever att den säkra inloggningen blir omständlig och kräver en enklare lösning, ser du då detta som ett tekniskt problem, ett kompetensproblem eller ett större arbetsorganisationsproblem?
- Som illustreras i denna bok kan inte eID ses som ett isolerat fenomen. Vilka problem relaterade till eID finns i er organisation?

Tillit **beror** på sammanhang. Många olika **kompetenser** behöver samverka för en **tillitsfull** utveckling av eID.

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 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. 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 ett IT-system. Det kan ske oavsett om kvaliteten på tjänsten i sig förändrats eller inte, i och med användningen av IT.

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.

…att diskutera

- Vilken roll spelar eID för att bygga upp medborgarnas tillit för myndigheternas e-tjänster?
- Hur kan politiker, tjänstemän och medarbetare (exempelvis lärare, sjuksköterskor, socialsekreterare) bidra till att medborgare känner tillit för offentliga organisationer?
- Vilka hinder upplever ni att ni har just i er organisation i samband med säkra inloggningslösningar till elektroniska plattformar? Hur hanterar ni dessa hinder?
- Har ni upplevt att användarna ställer krav på hur dessa lösningar måste se ut för att vara mer säkra, innehållsrika och/eller användarvänliga?
- Vilka risk- och integritetsaspekter innebär användningen av era inloggningslösningar? Är användarna medvetna om dessa?

Genom **offentlig** förvaltning kommer **medborgarna** i kontakt med effekterna av **politiska** beslut.

Kan eID stärka det offentligas 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.

Som vi diskuterat tidigare i boken kan digitaliseringen av den offentliga sektorn (och därmed sammanhängande ökad användning av eID som förutsättning för att kunna nyttja offentliga e-tjänster) 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 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 mer komplexa och krävande ärenden fortfarande behöver större inslag av manuell handläggning och innehåller interaktion som inte sker elektroniskt. Elektronisk hantering kanske inte ens är önskvärd i dessa fall, även om det vore tekniskt möjligt.

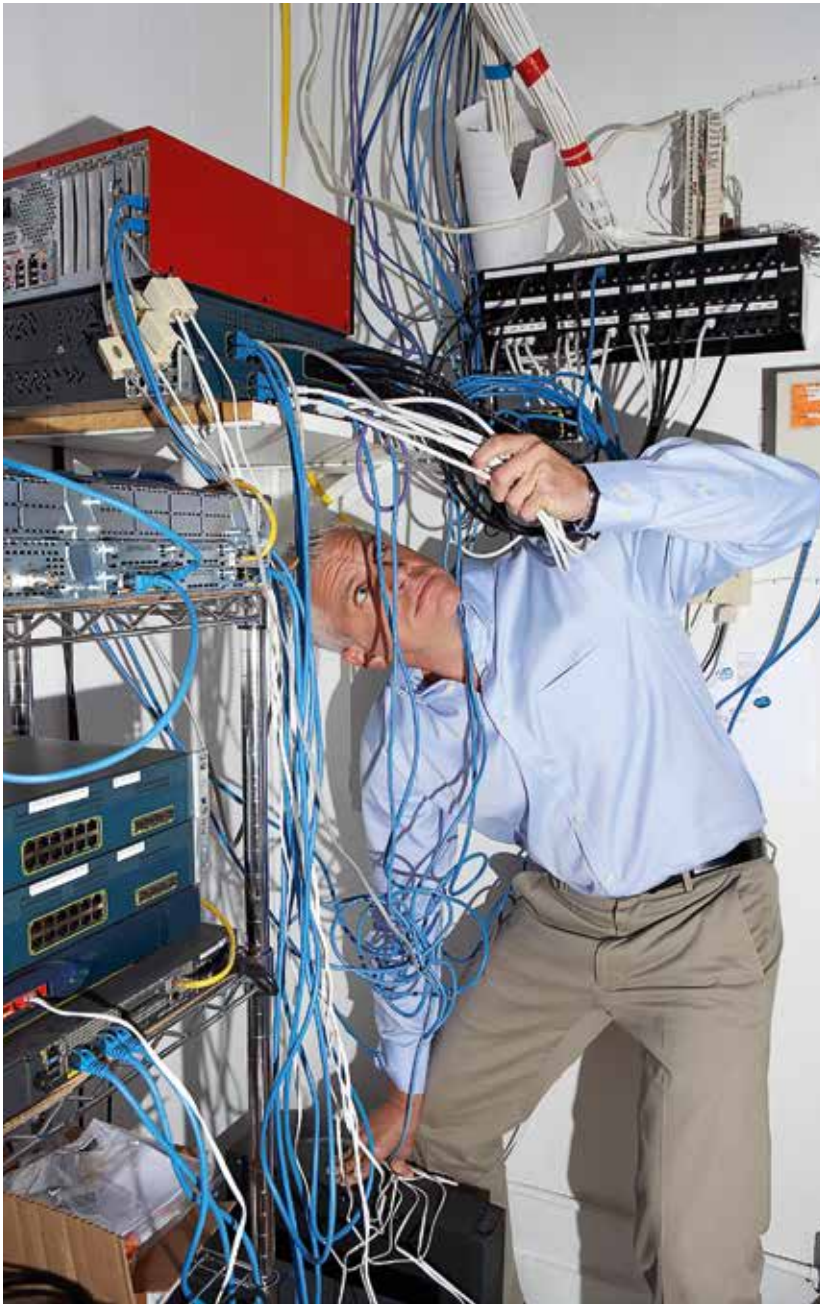
När medborgarnas uppfattningar betonas bör vi också beakta de grupper av medborgare som av olika anledningar (exempelvis teknisk okunskap, språkbarriärer

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 såväl stärka som försvaga legitimiteten för offentliga organisationer. 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.

…att diskutera

- Vad är viktigt för att vi ska uppfatta en offentlig organisation som legitim? Hur kan eID och e-tjänster påverka legitimiteten?
- Vad kan underlätta spridningen av eID, så att fler använder alltmer säkra tjänster?
- Hur skulle tilliten till offentliga elektroniska verksamheter på nätet och i andra gränssnitt kunna förbättras?



Ingen aktör eller organisation är ensam ansvarig för att eID utvecklas och används.

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, så som den inledande beskrivningen visade, 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 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 fallen ovan, 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.

…att diskutera

- Vem har ansvar för att sprida eID som lösning och bidra till att öka dess användning; de som tillhandahåller eID eller de som erbjuder tjänster som kräver eID?

- Vad händer när eID inte fungerar? Vem bör ta ansvar för det, de som tillhandahåller eID eller de som erbjuder tjänster där eID krävs?

- Om staten ska vara den som tar det yttersta ansvaret för att det fungerar, vad krävs då för att staten ska kunna styra alla och få dem att följa regler och normer om eID? Hur samlar man hela den offentliga sektorn kring denna fråga?

Dagens slutsatser bär och formar framtidens elektroniska identifiering.

Att gå vidare: Utmaningar och möjligheter

Som avslut på den här boken vill vi väcka tio väsentliga teman som bär både utmaningar och möjligheter i sig. De kan med fördel tas med till fikarummet, på konferensen eller diskuteras tillsammans på månadsmötet. Slutsatser kring dessa teman bär och formar framtidens elektroniska identifiering.

- Vikten av att se elektronisk identifiering som en del av en helhet. Det leder förvisso till stor komplexitet. Man måste klara balansen mellan det komplexa och det alltför snäva perspektivet (fokus enbart på teknik).

- eID som artefakt finns i olika sammanhang och påverkar där såväl individer, organisationer som samhälleliga aspekter. Samspelet mellan dessa skikt är viktigt att förstå och beakta för att åstadkomma en fungerande helhet kring elektronisk identifiering.

• Rollen man är i när man använder eID påverkar vilka val man gör och hur man vill legitimera sig elektroniskt. Rollen påverkar också vad som fungerar att använda rent praktiskt, men också vad man känner tillit till och vad man är bekväm med.

• Vilken roll man har gör också att man uppfattar eID och problem relaterade till säkerhet på olika sätt. En teknikkonsult uppfattar med största sannolikhet eID på ett annat sätt än till exempel verksamhetsansvariga och användare.

• Högsta säkerhet är inte alltid rätt säkerhet. Värdet på informationen som ska skyddas måste sättas i relation till sammanhanget och användarna. Även i rätt tid är viktigt – informationen måste vara ”punktlig”.

• Även säkra lösningar måste uppfattas som enkla att använda. Krångliga säkerhetslösningar uppmuntrar till arbetssätt som inte alltid gynnar den faktiska säkerheten. Hög teknisk säkerhet och god användbarhet kan ofta vara svårt att kombinera.

Anteckningar:

• Tidigare erfarenheter av systeminförande spelar stor roll för hur man uppfattar införande av nya eID-lösningar.

• Sättet som eID kommuniceras och presenteras på har stor betydelse för hur användare uppfattar elektronisk identifiering. Med större förståelse följer en ökad benägenhet att använda eID.

• När en användare måste kunna använda flera olika system med olika slags säkerhetslösningar, vem tar då ansvar för att de samordnas och att användarna lär sig att se skillnader mellan dem?

• IT-systemens eller e-tjänstens användbarhet och deras anpassning till verksamhetsprocesser är en underliggande utmaning. Att det införs säkrare inloggningslösningar till dessa system löser inte det grundläggande problemet, snarare utgör det ett extra hinder i användningen. Hur kan vi balansera detta så att vi får nyttiga och verksamma säkerhetslösningar?

Författarpresentation

ESTER ANDRÉASSON är doktorand i statsvetenskap vid IEI, LiU. Hon forskar om IT-utveckling i den offentliga sektorn, och är intresserad av hur teknik samspelar med och påverkar politik och förvaltning. 2011 lade hon fram sin licentiatavhandling med titeln *"Det är väldigt mycket datoriserat är det." – En studie om IT-utveckling i ett landsting: policy, implementering och praktik*. Nu arbetar hon med sin doktorsavhandling, som fokuserar på makt och legitimitet i offentliga organisationer i relation till utvecklingen av e-förvaltning. Ester undervisar även på kurser om politisk teori och politiska system samt handleder studenter som skriver uppsats i statsvetenskap.

KARIN AXELSSON är professor i informatik vid IEI, LiU. Hennes forskning är inriktad mot hur offentlig sektor med stöd av IT, organisatoriska förändringar och nya kompetenser kan utveckla sin verksamhet på sätt som skapar största möjliga nytta i samhället. Resultatet av sådan utveckling benämns ofta elektronisk förvaltning. Offentliga e-tjänster riktade till medborgare och företag är centrala för att realisera e-förvaltning. Karin studerar bl.a. de dubbla målsättningar som utveckling av offentliga e-tjänster innebär; hur strävan efter myndighetseffektivisering och medborgarnytta kan samverka eller motverka varandra. Karin är även verksam i grund- och forskarutbildning samt i ledningsuppdrag inom universitetet.

MARIANA S. GUSTAFSSON är doktorand i statsvetenskap vid IEI, LiU. Hennes forskning fokuserar på säkerhetimplikationer av IKT-användning inom offentlig sektor för politisk legitimitetsbyggande. Tidigare har hon jobbat med EU-projekt inom innovation, arbetslivsforskning och informationssamhälle vid Lunds universitet. Därefter har hon jobbat som analytiker på Oxford Research med utvärderingar och konsultuppdrag inom NMP och organisationsutveckling för Europeiska kommissionen, RTD.

KARIN HEDSTRÖM är docent i informatik och verksam vid IEI, LiU samt vid Örebro universitet. Karin forskar om elektronisk förvaltning, informationssäkerhet och systemutveckling. Hon är framför allt intresserad av IT-systemens normerande roll, d v s hur IT-systemen påverkar oss som individer, olika organisationer och verksamheter samt samhället i stort. Vad händer i en verksamhet när man inför elektroniska system för identifiering? Hur prioriteras frågor om informationssäkerhet inom en verksamhet? Hur utvecklas säkerhetspolicies? Vems behov är det som får genomslag vid utveckling av IT-system?

ULF MELIN är biträdande professor i informatik vid IEI, LiU och arbetar med forskning och undervisning som fokuserar utveckling och införande av IT i organisationer. Samspelet mellan planer och införande samt förändring i samband med IT-införande har studerats i olika sektorer och sammanhang. Aktuella sammanhang och artefakter som har studerats teoretiskt och empiriskt är: myndigheters e-tjänster, digitala patientjournalsystem inom vården, lösningar för elektronisk identifiering som förutsättning för IT-användning och affärssystem. Ulf är aktiv inom flera informationssystemkonferenser och tidskrifter inom området samt i undervisning i systemvetenskap/informatik och IT-management.

FREDRIK SÖDERSTRÖM är doktorand vid avdelningen informatik vid IEI, LiU och fokuserar i sitt avhandlingsarbete på elektronisk identifiering inom offentlig sektor. Fredrik har ett särskilt intresse för hur olika organisatoriska och sociala aspekter påverkar utveckling såväl som införande och användning av elektronisk identifiering i olika verksamheter. Han har tidigare varit yrkesverksam som systemutvecklare inom privat sektor och har aktivt följt utvecklingen av den svenska e-legitimationen sedan 2011.

ELIN WIHLBORG är professor i statsvetenskap vid IEI, LiU. Hon har i sin forskning under lång tid intresserat sig för hur det framväxande IT-samhället påverkar lokal och kommunal politik och förvaltning. Särskilt har hon intresserat sig för små kommuners och glesbygders förändrade förutsättningar och även hur hållbar utveckling kan skapas i sådana sammanhang. Hennes forskning har på så sätt ofta kommit till nytta för förändringar i kommuner och andra organisationer. Forskningen har presenterats både i vetenskapliga publikationer och texter för praktiker, som denna. Hon undervisar i statsvetenskap och andra samhällsvetenskapliga ämnen, bland annat på lärarutbildningen och hon har ledningsuppdrag inom universitet.

Läs mer om oss och vår forskning på www.liu.se

Litteraturtips

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. (2013). Managing the development of secure identification – Investigating a national eID 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) pp. 143-151.

Vem är vem på nätet?
- en studie av elektronisk identifiering

Den här boken rymmer slutsatser och erfarenheter som vi samlat under ett tre år långt forskningsprojekt om framtidens säkra elektroniska identifiering. Syftet med boken är att sätta ljuset på ett antal teman som framstår som centrala för utveckling och användning av elektronisk identifiering. Vi beskriver tre exempel som hämtar inspiration från våra studier inom projektet. Utifrån dessa exempel lyfter vi fram och diskuterar ett antal teman samt sammanfattar utmaningar som vi sett i våra studier. Boken är tänkt att fungera som ett diskussionsunderlag för ansvariga beslutsfattare och tjänstemän inom offentlig sektor, men även för utvecklare av elektronisk identifiering och e-tjänster samt intresserade användare.






Linköpings universitet

Linköpings universitet
Institutionen för ekonomisk och industriell utveckling
581 83 Linköping | Tel: 013-281000 | www.liu.se