



RIKSREVISIONEN

RiR 2009:19

E-legitimation – en underutnyttjad resurs

ISBN 978 91 7086 192 5

RiR 2009:19

Tryck: Riksdagstryckeriet, Stockholm 2009

Till regeringen
Finansdepartementet

Datum: 2009-11-23
Dnr: 31-2009-0753

E-legitimation – en underutnyttjad resurs

Riksrevisionen har granskat systemet för e-legitimation. Resultatet av granskningen redovisas i denna granskningsrapport.

Företrädare för Regeringskansliet, Kammarkollegiet, Finansinspektionen, Datainspektionen, Post- och telestyrelsen och Statskontoret har fått tillfälle att faktagranska och i övrigt lämna synpunkter på utkast till rapport.

Rapporten överlämnas till regeringen i enlighet med 9 § lagen (2002:1022) om revision av statlig verksamhet m.m. Rapporten överlämnas samtidigt till Riksrevisionens styrelse.

Rapporten innehåller slutsatser och rekommendationer som avser Regeringskansliet. Riksrevisionen kommer att följa upp granskningen.

Riksrevisor *Claes Norgren* har beslutat i detta ärende. Revisionsdirektör *Marcus Pettersson* har varit föredragande. Programansvarig *Qaisar Mahmood* och revisionsdirektör *Philippe Jolly* har medverkat vid den slutliga handläggningen.

Claes Norgren

Marcus Pettersson

För kännedom:

Datainspektionen
Finansinspektionen
Post- och telestyrelsen
Kammarkollegiet
Statskontoret
Sveriges Kommuner och Landsting

Innehåll

Sammanfattning	7
1 Inledning	13
1.1 Motiv till granskningen	13
1.2 Syfte och revisionsfråga	13
1.3 Utgångspunkter för granskningen	14
1.4 Metod och avgränsningar	14
1.5 Disposition	15
2 Bakgrundsbeskrivning	19
2.1 Vad är en e-legitimation?	19
2.2 Aktörer	20
2.3 Riksdagens och regeringens hantering av frågan om e-legitimationer – en historisk exposé	22
3 Regeringens styrning och myndigheternas insatser	27
3.1 Regeringens generella mål- och resultatstyrning av e-politiken	28
3.2 Regeringens specifika åtgärder	30
3.3 Myndigheternas specifika åtgärder	33
3.4 Sammanfattande kommentarer	36
4 Rättssäkerhet	37
4.1 Integritet	37
4.2 Tillsyn och övervakning av systemet	40
4.3 Sammanfattning av iakttagelserna	43
5 Tillgänglighet och användbarhet	45
5.1 Tillgänglighet och teknisk plattform	45
5.2 Tillgänglighet i form av rätt att få en e-legitimation	47
5.3 Tillgänglighet i betydelsen användbarhet	48
5.4 Sammanfattning av iakttagelserna	51
6 Kostnadseffektivitet och konkurrens	53
6.1 Ramavtal	53
6.2 Kostnader för ett statligt alternativ är oklara	58
6.3 Sammanfattning av iakttagelserna	59
7 Teknik och teknikneutralitet	61
7.1 Myndigheternas förmåga att samverka	61
7.2 Organisationslegitimationer	63
7.3 Sammanfattning av iakttagelserna	65
8 Analys, slutsatser och rekommendationer	67
8.1 Sammanfattande bedömning	67
8.2 Är systemet för e-legitimationer rättssäkert?	68
8.3 Är systemet för e-legitimationer tillgängligt?	69
8.4 Är systemet för e-legitimationer kostnadseffektivt?	70
8.5 Har regeringen främjat konkurrens?	71
8.6 Är systemet för e-legitimationer teknikneutralt?	71
8.7 Rekommendationer	73
Bilaga 1	75

Sammanfattning

Riksrevisionen har granskat systemet för e-legitimation. Granskningen har utgått från följande frågor.

- Är systemet för e-legitimation rättssäkert, tillgängligt, kostnadseffektivt och teknikneutralt?
- Har regeringen och ansvariga myndigheter agerat i enlighet med riksdagens intentioner med avseende på utvecklandet av systemet för e-legitimationer?

God service till medborgare och företag är den viktigaste uppgiften för den offentliga verksamheten. För att verksamheten ska fungera effektivt är den i stora delar beroende av modern informations- och kommunikationsteknik. Tillgången till en väl fungerande e-legitimation är därmed av central betydelse.

En e-legitimation är en elektronisk identitetshandling för privatpersoner. Genom att använda sin e-legitimation kan en person visa sin identitet och genom detta på ett säkert sätt få tillgång till tjänster och uppgifter hos myndigheter och företag via internet. Det finns idag ett flertal tjänster hos olika myndigheter, kommuner och privata företag som använder sig av e-legitimation. Genom att använda e-legitimation får individen möjlighet till att bland annat deklarerar, anmäla vård av sjukt barn eller sköta bankärenden. Riksdagen har uttalat att:

”[s]tatens roll bör vara att gynna användningen av e-legitimationer, stimulera konkurrens mellan utfärdare av sådana legitimationer och att undanröja infrastrukturella, marknadsmässiga och konkurrensmässiga hinder. Likaså bör staten för att säkra en dynamisk utveckling av informationssamhällets säkerhetslösningar, samt för att gynna konkurrens och kostnadseffektivitet i säkerhetslösningar, verka för att det etableras teknikneutrala standarder för elektroniska signaturer inom offentlig sektor.”¹

Riksdagen har även uttalat:

” [D]et bör framhållas att utnyttjande av IT inte får försämra rättssäkerheten eller myndigheters förutsättningar att fungera.”²

¹ Trafikuskottets betänkande 2005/06:TU4, Från IT-politik för samhället till politik för IT-samhället.

² Ibid.

Riksrevisionens samlade bedömning

Riksrevisionens bedömning är att systemet för e-legitimation till stora delar uppfyller de krav på rättssäkerhet, tillgänglighet, kostnadseffektivitet och teknikneutralitet som riksdagen har uttalat. Riksrevisionens bedömning av aktörerna, det vill säga regeringen och ansvariga myndigheter, är att de inte fullt ut har agerat i enlighet med riksdagens intentioner för utvecklandet av systemet för e-legitimationer.

Den sammanlagda bilden är att systemet för e-legitimationer i sig har haft en positiv effekt på utvecklingen av e-förvaltningen. Det finns dock vissa förbättringsområden i e-legitimationssystemet om man ser till rättssäkerheten, tillgängligheten, kostnadseffektiviteten och teknikneutraliteten.

Riksrevisionen kan dock notera att E-delegationen, på uppdrag av regeringen, har presenterat ett antal förslag för att komma till rätta med flera av de brister som redovisas i granskningen. Förslagen kan ge regeringen och myndigheterna bättre förutsättningar för att få till den styrning och uppföljning som krävs för att tillgodose riksdagens krav på rättssäkerhet, användbarhet, kostnadseffektivitet och teknikneutralitet.

Är systemet för e-legitimation rättssäkert?

Riksrevisionen har inte funnit att rättssäkerheten och myndigheternas möjlighet att fungera har försämrats. Det finns snarare indikationer på att myndigheternas möjlighet att fungera har förbättrats genom tillgång till tjänster via e-legitimation. En ökad användning av e-legitimationer skulle även ytterligare öka individernas rättssäkerhet med tanke på den höga tekniska säkerhetsnivå som uppnås med hjälp av en e-legitimation.

Riksrevisionen konstaterar att tillsyn av själva systemet för e-legitimationer inte har förekommit. Användningen av e-legitimationer förväntas öka. Användningen medför även att stora mängder personuppgifter lagras hos leverantörerna. Riksrevisionen anser därför att tillsynsansvaret behöver preciseras för att nå upp till de krav som riksdagen har satt upp för skyddet av den personliga integriteten.

Är systemet för e-legitimation tillgängligt?

Riksrevisionen bedömer att systemet för e-legitimationer inte kan anses uppfylla kraven på tillgänglighet och användbarhet fullt ut. Utgångspunkten har varit ett produktionsperspektiv och inte ett användarperspektiv vid utvecklingen av systemet för e-legitimationer. Detta har resulterat i att det blivit onödigt krångligt för användaren att hantera lösningen.

Regeringen har inte varit tillräckligt tydlig i styrningen av övergången till e-förvaltning. Den svaga styrningen av myndigheterna har resulterat i att myndigheterna inte har prioriterat utvecklingen av e-tjänster. Bristen på e-tjänster har i sin tur inneburit att det saknats incitament för medborgarna att skaffa sig e-legitimationer. Detta innebär vidare att övergången från traditionell förvaltning till e-förvaltning inte utvecklats i tillräckligt snabb takt.

Ansvariga myndigheter har vidtagit vissa åtgärder och även påtalat behov av ytterligare åtgärder från regeringens sida. Riksrevisionen anser dock att myndigheterna kunde ha gjort mer för att marknadsföra e-legitimation och e-tjänster i syfte att öka användningen.

Är systemet för e-legitimation kostnadseffektivt?

Riksrevisionen bedömer att när det gäller kostnadseffektiviteten så uppfyller systemet i stora delar kraven från riksdagen. Den lösning som staten har valt i form av ramavtal har dock inneburit en begränsad konkurrenssituation som kan ha fått negativa konsekvenser både för prissättning och tekniska utvecklingsmöjligheter för den befintliga lösningen. Det bör dock framhållas att ett huvudsyfte med att välja den nuvarande lösningen var att bruka en befintlig och väl fungerande lösning för att snabbt få igång e-tjänster. Om staten hade utvecklat en egen lösning hade det för det första inneburit en längre startsträcka och för det andra att den statliga lösningen skulle konkurrera med möjliga privata alternativ.

Regeringen beslutade att ansvariga myndigheter skulle upphandla en lösning från den privata marknaden istället för att utveckla en lösning i statens regi. Vid en jämförelse mellan den finska och den svenska lösningen framstår det som att regeringens ställningstagande har inneburit lägre kostnader än alternativen. Skatteverkets och Försäkringskassans användning av e-legitimationstjänster har inneburit en mer kostnadseffektiv hantering jämfört med manuell hantering för dessa myndigheter. Riksrevisionen anser dock att om regeringen genom tydligare styrning hade främjat utvecklingen av fler e-tjänster som använder sig av e-legitimationslösning skulle kostnadseffektiviteten öka inte bara hos dessa två myndigheter utan i hela statsförvaltningen.

Myndigheterna får, precis som regeringen, anses ha gynnat kostnadseffektiviteten i det stora hela.

Flera myndigheter har dessutom påtalat vilka problem som finns angående styrning, finansiering av e-tjänster och val av lösning för e-legitimationer.

Har regeringen främjat konkurrens?

När det gäller konkurrensaspekten bedömer Riksrevisionen att valet av ramavtalsupphandling och önskemålet om utfärdare med en avtalsrelation med en betydande andel av befolkningen har medfört att priskonkurrensen inte har fungerat väl. En potentiell anbudslämnare var redan vid anbudsinlämning tvungen att ha både en stor redan elektroniskt validentifierad kundkrets och en omfattande teknisk infrastruktur för att kunna utfärda och hantera e-legitimationer i stora mängder.

En konsekvens av dessa båda krav är att tre grupper av leverantörer har varit aktuella som ramavtalsleverantörer från 2001 och framåt. Det rör sig om ett antal banker inom BankID-sfären, banker som står utanför BankID och erbjuder en egen lösning samt några företag, såsom Telia och Steria. Genom att välja nuvarande lösning skapade man ett system som inte byggde på öppna standarder utan kunderna var ”inlåsta” till sina respektive banker och kundernas rörlighet mellan olika alternativ var därmed ytterst begränsad. Systemet har också höga inträdesbarriärer för potentiella leverantörer.

Regeringens beslut att inte bygga en statligt utvecklad lösning utan i stället upphandla den nuvarande lösningen av privata aktörer har inneburit en inlåsnings effekt på systemet för e-legitimation. Ansvariga myndigheter har därmed haft små möjligheter att stimulera konkurrens och det är därför svårt att kritisera deras passiva agerande.

Är systemet för e-legitimation teknikneutralt?

Riksrevisionen bedömer att när det gäller kravet på teknikneutralitet kan systemet för e-legitimationer inte anses uppfylla riksdagens krav. Regeringen kan inte heller anses ha främjat etableringen av teknikneutrala standarder för elektroniska signaturer eller ha säkrat en dynamisk utveckling av informationssamhällets säkerhetslösningar.

E-legitimationssystemet är i dag inte utformat på ett sätt som möjliggör samverkan med andra system, det vill säga en interoperabel lösning. Ett problem med e-legitimationerna är att gränssnitten inte är standardiserade. För att åstadkomma interoperabla system för hela den offentliga sektorn krävs en tydlig styrning från regeringen i fråga om systemkrav och val av teknik.

Ansvariga myndigheter har med anledning av regeringens ställningstagande haft små möjligheter att vidta några åtgärder för att främja teknikneutrala lösningar. Den tekniska lösningen för e-legitimation bygger på specifikationer framtagna i slutet på 90-talet, och lösningen ser i stort sett likadan ut i dag som den gjorde då. Den begränsade konkurrenssituationen som blev följden av regeringens ställningstagande har förmodligen inneburit minskad teknisk utveckling och innovation.

Rekommendationer

E-delegationen har lämnat förslag till framtida lösning för e-legitimationer och Riksrevisionen vill framhålla att flera av de brister som har framförts i denna rapport skulle kunna lösas genom E-delegationens förslag. Det gäller exempelvis förslagen om att införa en federationsarkitektur för e-legitimationer och att standardisera gränssnitten. Eftersom dessa förslag behandlas utförligt i E-delegationens nyligen publicerade rapport nämns de inte som rekommendationer nedan.

Några av de brister som Riksrevisionen har iakttagit riskerar dock att kvarstå även om E-delegationens förslag genomförs.

Riksrevisionen rekommenderar därför regeringen att

- genomföra en översyn av tillsynen av systemet för e-legitimationer och överväga att tydliggöra mandatet rörande tillsyn och peka ut en enskild aktör som får ansvar
- vidta åtgärder för att skapa öppna standarder och konkurrensutsätta identifieringsprocessen i syfte att undanröja konkurrensmässiga hinder
- vidta åtgärder för att öka tillgängligheten och skapa en framtida lösning för e-legitimationer utifrån användarnas behov
- genomföra informationssatsningar för medborgare, företag och myndigheter om fördelarna med att använda e-legitimationer.

1 Inledning

God service till medborgare och företag är den viktigaste och mest centrala uppgiften för den offentliga verksamheten. För att verksamheten ska fungera effektivt är den i stora delar beroende av modern informations- och kommunikationsteknik³. Hur och i vilken utsträckning myndigheterna och medborgarna använder IT påverkas i hög grad av flera olika drivkrafter. En stark drivkraft är naturligtvis IT-teknikens snabba utveckling i sig. En annan är regeringens krav på effektivisering av statförvaltningen genom myndigheternas IT-utveckling. Ytterligare en pådrivande kraft i sammanhanget är EU, vilket bland annat resulterat i EU-kommissionens handlingsprogram i2010-strategi⁴ och Europaparlamentets och Europarådets direktiv⁵ om en samlad reglering av förvaltningens informationshantering.

1.1 Motiv till granskningen

Tillgången till en väl fungerande e-legitimation är av central betydelse för förtroendet, rättssäkerheten, kostnadseffektiviteten och den framtida utvecklingen inom e-förvaltningen. Det finns emellertid tecken på att dagens system med e-legitimationer är behäftat med problem och svårigheter som riskerar att försvåra utvecklingen av e-förvaltningen inom staten. Riksrevisionen har i en förstudie funnit indikationer på att dagens system för e-legitimation inte uppfyller de krav som riksdagen ställt.

1.2 Syfte och revisionsfråga

Riksrevisionens granskning syftar till att

- belägga och analysera de problem som är förknippade med e-legitimationer och orsakerna till dessa
- bedöma vilka negativa konsekvenser som följer av detta
- lämna rekommendationer i syfte att minska eller undanröja problemen i fråga.

³ Den internationella förkortningen av informations- och kommunikationsteknik är IKT. I denna granskningsrapport används det mer etablerade begreppet IT (informationsteknik).

⁴ I2010-strategin antogs av medlemsländerna år 2005 och syftar bland annat till att skapa ett gemensamt europeiskt informationsområde, främja investeringar och innovation samt att uppmuntra medborgare, företagare och myndigheter att använda sig mer av informations- och kommunikationsteknik.

⁵ Direktivet (2003/98/EG), Direktivet (2006/123/EG), Direktivet (2007/2/EG).

Granskningen ska besvara följande tudelade fråga:

- a) Är systemet för e-legitimation rättssäkert, tillgängligt, kostnadseffektivt och teknikneutralt?
- b) Har regeringen och ansvariga myndigheter agerat i enlighet med riksdagens intentioner med avseende på utvecklandet av systemet för e-legitimationer?

Frågorna bedöms åtskilt eftersom systemets utformning är beroende av andra aktörer än regeringens och myndigheternas insatser.

1.3 Utgångspunkter för granskningen

Ansvar för utvecklingen av e-förvaltning är delat mellan riksdagen, regeringen, de av regeringen utsedda tillsyns- och stödmyndigheterna (expertmyndigheterna) samt de enskilda myndigheternas ledning. En utgångspunkt för bedömning av regeringens och myndigheternas åtgärder gällande systemet för e-legitimation är riksdagens syn på vilken roll staten ska ha i utvecklandet av e-legitimationer.

Riksdagen har uttalat att *"[s]tatens roll bör vara att gynna användningen av e-legitimationer, stimulera konkurrens mellan utfärdare av sådana legitimationer och att undanröja infrastrukturella, marknadsmässiga och konkurrensmässiga hinder. Likaså bör staten för att säkra en dynamisk utveckling av informations-samhällets säkerhetslösningar, samt för att gynna konkurrens och kostnadseffektivitet i säkerhetslösningar, verka för att det etableras teknikneutrala standarder för elektroniska signaturer inom offentlig sektor."*⁶

Riksdagen har även uttalat följande *"[D]et bör framhållas att utnyttjande av IT inte får försämra rättssäkerheten eller myndigheters förutsättningar att fungera."*⁷

1.3.1 Regeringens ansvar

Bedömningsgrunden för att granska regeringens insatser hämtas från riksdagens syn på e-legitimationssystemet, 1 kap. 6 § regeringsformen (1974:152) samt 1 § lagen (1996:1059) om statsbudgeten (budgetlagen). Av 1 kap. 6 § regeringsformen framgår att regeringen styr riket och är ansvarig inför riksdagen samt att av lagen om statsbudget framgår att staten ska eftersträva hög effektivitet och god hushållning i sin verksamhet (1 § budgetlagen).

⁶ Trafikutskottets betänkande 2005/06:TU4, Från IT-politik för samhället till politik för IT-samhället.

⁷ Ibid.

Riksrevisionen utgår i granskningen från att regeringens ansvar är att genom styrning

- gynna användningen av e-legitimationer
- stimulera konkurrensen mellan utfärdare av sådana legitimationer och undanröja infrastrukturella, marknadsmässiga och konkurrensmässiga hinder
- säkra en dynamisk utveckling av informationssamhällets säkerhetslösningar
- gynna kostnadseffektiviteten i säkerhetslösningarna,
- verka för att det etableras teknikneutrala standarder för elektroniska signaturer inom offentlig sektor samt
- säkerställa att rättssäkerheten eller myndigheters förutsättningar inte har försämrats med anledning av e-legitimationer.

1.3.2 *Myndigheternas ansvar*

Riksrevisionens bedömning är att regeringen på ett bra sätt formulerat myndigheternas ansvar i myndighetsförordningen (2007:515) och i förordningen (2003:770) om statliga myndigheters elektroniska informationsutbyte. Därför används dessa förordningar som bedömningsgrund i granskningen.

Riksrevisionen utgår i granskningen från att myndigheternas ansvar är att

- fortlöpande utveckla verksamheten (6 § myndighetsförordningen) samt att främja utvecklingen av ett säkert och effektivt elektroniskt informationsutbyte inom den offentliga förvaltningen (2 § förordning om statliga myndigheters elektroniska informationsutbyte)
- verka för att genom samarbete med myndigheter och andra ta till vara de fördelar som kan vinnas för enskilda samt för staten som helhet (6 § myndighetsförordningen)
- uppmärksamma regeringen på de hinder som försvårar myndighetens åtaganden enligt ovan (3 § myndighetsförordningen).

1.4 **Metod och avgränsningar**

Granskningen bygger på dokumentstudier och intervjuer med företrädare för berörda myndigheter, näringslivet och Regeringskansliet. Valet av kvalitativ metod baseras på att avsikten med granskningen är att belysa systemet för e-legitimation och problem förenade med området snarare än att mäta frekvenser eller fastställa kvantitativa skillnader.

Urvalet av både dokument och intervjupersoner har gjorts för att få så stor variation på anknytningen till området som möjligt. Därför har vi intervjuat företrädare för både kommunal och statlig sektor och även företrädare för e-tjänstleverantörer, beställare och tillhandahållare av identifieringstjänster. Intervjuerna har genomförts både som ostrukturerade och som semi-strukturerade intervjuer. Revisionsobjekt i granskningen är:

- Regeringen
- Verva
- Statskontoret
- Kammarkollegiet

Flertalet av de personer som har intervjuats var tidigare anställda på Verva och innan dess på Statskontoret. De har från början varit involverade i processen med att ta fram systemet. Flera av dem har därför intervjuats med anledning av deras roll i processen och inte utifrån var de har sin anställning i dag. Utöver revisionsobjekten har vi även intervjuat företrädare för Sveriges Kommuner och Landsting och för Finansiell ID-teknik AB.

Vi har även ställt ett antal frågor om tillsyn och e-legitimationer till Finansinspektionen, Datainspektionen och Post- och telestyrelsen.

Som en del av granskningen har vi anlitat professor Mats Bergman vid Södertörns högskola som har yttrat sig om den teoretiska utgångspunkten vad gäller konkurrensfrågor och ramavtalsupphandling som kan knytas till dagens lösning för e-legitimationer. Yttrandet finns som bilaga till rapporten och ligger tillsammans med de iakttagelser som Riksrevisionen har gjort till grund för analysen av den ramavtalsmodell som har valts för att tillgodose statens behov av e-legitimationer.

För att kvalitetssäkra våra iakttagelser och slutsatser har vi bjudit in en fokusgrupp bestående av olika sakkunniga på området. Fokusgruppen har bestått av:

- Roland Höglund, E-delegationen
- Predrag Mitrovic, mynethouse.se
- Leif Karlsson, Swedbank
- Kenneth Tessem, Finansiell ID-teknik AB
- Bengt Svensson, Sveriges Kommuner och Landsting
- Hans Sundström, Kammarkollegiet
- Johan Olvegård, Försäkringskassan
- Göran Lindberg, Försäkringskassan

Granskningen har varit inriktad på frågeställningar med direkt anknytning till e-legitimationer. På vissa områden har det dock varit nödvändigt att övergripande beröra problem kopplade till e-förvaltningsområdet i stort.

1.5 Disposition

I kapitel 2 beskrivs kortfattat vad en e-legitimation är och vilka olika roller och aktörer som finns i systemet. Därefter följer en kort beskrivning av riksdagens och regeringens ställningstaganden till e-legitimation och av regeringens handlingsplan för eFörvaltning samt E-delegationens uppdrag. Kapitel 3 innehåller en redogörelse av regeringens styrning och myndigheternas åtgärder. I kapitel 4 redogörs för de iakttagelser som vi gjort om rätts-säkerhet. I kapitel 5 följer iakttagelser om tillgänglighet och användbarhet. I kapitel 6 redogörs för iakttagelser som rör kostnadseffektivitet och konkurrens. I kapitel 7 beskriver vi teknik och teknikneutralitet. Riksrevisionens analys, slutsatser och rekommendationer presenteras i kapitel 8.

2 Bakgrundsbeskrivning

Kapitlet inleds med en kortfattad beskrivning av vad en e-legitimation är samt vilka aktörer och parter som finns inom dagens system för e-legitimationer. Därefter följer en kort beskrivning av riksdagens och regeringens hantering av frågan rörande e-legitimationer.

2.1 Vad är en e-legitimation?

En *e-legitimation* är en elektronisk identitetshandling i form av en programvara som innehåller en privat och en publik krypteringsnyckel och ett elektroniskt certifikat som identifierar innehavaren (legitimerande part).⁸

Ett *certifikat* är en informationsstruktur. Certifikatet innehåller bland annat information om den publika nyckeln, vem som har givit ut certifikatet, till vem certifikatet har givits ut, ett unikt nummer för certifikatet, en underskrift från utfärdaren för att garantera informationens riktighet och övriga uppgifter som utfärdaren kan ha valt att koppla till innehavarens identitet.⁹

För att tekniken ska kunna användas av fler än två parter krävs en struktur som involverar en tredje part. En sådan struktur med regler för användandet av elektroniska signaturer kallas *public key infrastructure (PKI)*.

Själva PKI:n utgörs av regler för hur utfärdaren ska hantera certifikat, hur innehavarna ska hantera sin privata nyckel, krav på tekniken i lösningen, hur ett certifikat spärras eller återkallas med mera.

Tre parter i en PKI-lösning

I ett system som använder en elektronisk identifieringslösning baserad på PKI finns normalt tre olika parter. Dessa parter är utfärdare, legitimerande part och förlitande part.

*Utfärdaren*¹⁰ är den som utfärdar en e-legitimation. För att kunna utfärda en e-legitimation krävs att man säkerställer identiteten hos användaren (den legitimerande parten). Det krävs också en avtalsrelation mellan utfärdaren och användaren för att säkerställa ansvar och skyldigheter mellan parterna.

⁸ Eklöf, Rashid, *Hinder och problem i utvecklingen av e-legitimationer och myndigheters e-tjänster*, s10.

⁹ Ibid.

¹⁰ Exempel på utfärdare i det svenska systemet är BankID, Telia och Nordea.

Den *legitimerande parten* är huvudsakligen en privatperson som behöver en e-legitimation för att kunna styrka sin identitet gentemot någon annan person, företag eller myndighet. Den legitimerande parten vänder sig då till utfärdaren. När personen väl har fått en e-legitimation kan han eller hon använda den elektroniskt gentemot ett företag eller en myndighet. Detta sker genom att användaren loggar in på en e-tjänst med hjälp av e-legitimationen.

Den *förlitande parten* är normalt sett en myndighet eller ett företag. För att kunna utföra vissa uppgifter via en e-tjänst krävs att den förlitande parten vet att det är rätt person som får tillgång till e-tjänsten. När den legitimerande parten använder sin e-legitimation överförs uppgifter om partens identitet. Den förlitande parten kan inte själv avgöra om dessa uppgifter är giltiga och därför görs en förfrågan till den *utfärdande parten*. Om den förlitande parten får ett svar att e-legitimationen är giltig så ges användaren en möjlighet att logga in på e-tjänsten. För att den förlitande parten ska kunna göra en förfrågan om giltigheten hos en e-legitimation krävs att det på förhand har upprättats ett *avtal mellan den förlitande parten och den utfärdande parten som reglerar skyldigheter och rättigheter parterna emellan*.

2.2 Aktörer

Leverantörer: banker och Telia Sonera

I Sverige är leverantörerna tre banker, Handelsbanken, Swedbank och Nordea, samt Telia Sonera Sverige AB.¹¹ Det är bara de tre bankerna och Telia Sonera som är avtalsparter i det ramavtal som staten har tecknat för att få tillgång till e-legitimation åt medborgarna. Därutöver har totalt nio banker ett samarbete som innebär att de erbjuder en *gemensam teknisk lösning kallad BankID*.¹² Det betyder att totalt nio banker inom BankID, Nordea och Telia Sonera Sverige AB agerar som utfärdare av certifikat. Den tekniska lösningen BankID utvecklas och ägs av ett företag som heter Finansiell ID-Teknik AB. Bolaget ägs i sin tur av ett antal banker.¹³

¹¹ Det är bara Handelsbanken, Swedbank, Nordea och Telia Sonera som är avtalsparter gentemot Kammarkollegiet i ramavtalet. De banker som ingår i BankID utfärdar e-legitimation utifrån Swedbanks eller Handelsbankens avtal.

¹² De nio banker som erbjuder BankID är Handelsbanken, SEB, Swedbank, Skandiabanken, Länsförsäkringar Bank, Danske Bank, Sparbanken Finn, Sparbanken Gripen och Ikano Bank.

¹³ Ägare till Finansiell ID-Teknik är Danske Bank, Handelsbanken, Ikano Bank, Länsförsäkringar Bank, SEB, Skandiabanken och Swedbank.

Ramavtalsansvarig: Kammarkollegiet

Kammarkollegiet är sedan den 1 januari 2009 ramavtalsansvarig myndighet för ramavtalet gällande e-legitimationer.¹⁴ I uppgiften ingår förvaltning av befintligt avtal, vilket innebär att följa upp och övervaka befintliga avtal.

Ramavtalsupphandlingen är baserad på en kravspecifikation som ursprungligen togs fram av Riksskatteverket.¹⁵ Sverige har till skillnad från vissa andra länder, exempelvis Finland, Belgien och Estland, valt att inte skapa en statlig lösning för identifieringstjänster utan i stället valt att via avtal säkra tillgången till identifieringstjänster från den privata marknaden.

Övervakning av systemet: delat på flera parter

Det finns ingen myndighet som utövar någon direkt tillsyn över de e-legitimationer som utfärdas med stöd av ramavtalen.

Post- och telestyrelsen har ett tillsynsansvar när en leverantör utfärdar en kvalificerad elektronisk signatur vilket är en mer komplicerad och säkrare hantering. De e-legitimationer som utfärdas enligt ramavtalet utgör dock inte kvalificerade signaturer utan i stället avancerade signaturer (en enklare och något mindre säker hantering).¹⁶ Myndigheten har dock i uppgift att främja tillgången till säkra och effektiva elektroniska kommunikationer. Den ska också se till att samhällsomfattande tjänster finns tillgängliga och främja tillgången till ett brett urval av elektroniska kommunikationstjänster.¹⁷

Finansinspektionen har tillsyn över bankerna och därmed även över de e-legitimationer som bankerna utfärdar. Det är dock inte helt tydligt på vilket sätt och i vilken omfattning tillsynen av e-legitimationer sker eller borde ske.

Behandlingen av personuppgifter är reglerad i personuppgiftslagen (1998:204) och tillsynsmyndighet för lagen är Datainspektionen. Datainspektionen har ett övergripande tillsynsansvar för behandling av personuppgifter med anknytning till e-legitimationer, eftersom både den interna hanteringen hos bankerna och frågan om autentisering vid inloggning till en e-tjänst med åtkomst till personuppgifter har anknytning till lagen.

¹⁴ Nuvarande gällande ramavtal har benämningen Elektronisk identifiering (eID) 2008.

¹⁵ Riksskatteverket, Vägledning till myndigheter inför införandet av elektronisk identifiering och underskrifter. Grunden för uppdraget var beslut av regeringen den 21 december 2000 (Ju2000/4939).

¹⁶ Se 4 § p14 samt 6 och 7 §§ i lagen (2000:832) om kvalificerade elektroniska signaturer.

¹⁷ 4 § p1 i förordningen (2007:951) med instruktion för Post- och telestyrelsen.

Myndigheterna och e-tjänster

Statliga myndigheter, kommuner och landsting är det offentliga kontaktyta mot medborgare och företag. De har ett ansvar för att i praktiken förverkliga övergången från traditionell förvaltning till e-förvaltning. Detta sker genom att tillhandahålla olika former av e-tjänster åt medborgaren.

Myndigheterna har också en skyldighet att bedriva en kostnadseffektiv verksamhet och att fortlöpande utveckla verksamheten. Mer specifikt för e-förvaltning är att myndigheterna är skyldiga att i sin verksamhet främja utvecklingen av ett säkert och effektivt elektroniskt informationsutbyte inom den offentliga förvaltningen. Gentemot den enskilde medborgaren har myndigheterna en service- och informationskyldighet och en skyldighet att handlägga snabbt, rättssäkert och enkelt.

2.3 Riksdagens och regeringens hantering av frågan om e-legitimationer – en historisk exposé

2.3.1 Regeringens arbete med 24-timmarsreformen

I den förvaltningspolitiska propositionen (1997/98:136) och det förvaltningspolitiska handlingsprogrammet från år 2000 angavs ett antal vägledande utgångspunkter för styrningen av övergången till elektronisk förvaltning. De handlade om att regeringen skulle skapa goda förutsättningar för reformen. Några punkter som nämndes var bland annat behov av bättre mål, bättre styrmedel, bättre styrdialoger och bättre återrapportering. Regeringen skulle vara aktiv i reformarbetet genom att driva på, följa upp, ge stöd åt förvaltningen och öka kvaliteten i beslutsunderlagen. Förvaltningen skulle dock vara huvudaktören för att genomföra reformen på ett kostnadseffektivt sätt.

Viktiga insatsområden för regeringen angavs vara att skapa till exempel regler och standarder för säker e-kommunikation, för myndigheternas arbete med att utveckla e-tjänster. Regeringen gav vissa myndigheter i uppdrag att utveckla kunskap, metoder och standarder. Statskontoret och Riksskatteverket kom att spela viktiga roller i detta arbete. Statskontoret fick 2001 bland annat i uppdrag från regeringen att ”stimulera och stödja utvecklingen av 24-timmarsmyndigheter genom att tillsammans med myndigheterna tillhandahålla metoder, vägledningar och avtal samt att initiera och genomföra samverkansprojekt”. Syftet med uppdraget var ”att stimulera myndigheterna till att bedriva ett aktivt utvecklingsarbete för att förbättra sin tillgänglighet och service med hjälp av informationstekniken”. Statskontoret lämnade med anledning av uppdraget lägesrapporter halvårsvis till regeringen, och uppdraget slutrapporterades till regeringen vid halvårsskiftet 2003.¹⁸

¹⁸ Statskontoret, *Samverkande 24-timmarsmyndigheter – sammanhållen elektronisk förvaltning*, 2003:18.

Utöver detta beslutade regeringen i början av år 2002 om en samlad översyn av lagar och förordningar i syfte att undanröja onödiga hinder för elektronisk kommunikation och elektronisk dokument- och ärendehantering.¹⁹

I juni 2003 beslutade regeringen att inrätta en delegation för utveckling av offentliga tjänster. Delegationen fick namnet 24-timmarsdelegationen, och enligt direktiven skulle delegationen stimulera utvecklingen och användningen av elektroniska tjänster i offentlig sektor. Delegationen avrapporterade sitt uppdrag i SOU 2005:119.

Regeringen inrättade också en nämnd för elektronisk förvaltning från och med januari 2004. Nämnden hade enligt sin instruktion till uppgift att stödja utvecklingen av ett säkert och effektivt elektroniskt informationsutbyte mellan myndigheter och enskilda.²⁰

2.3.2 Första upphandlingen 2001

Under mitten av 1990-talet påbörjades utvecklingen av elektroniska tjänster. En förutsättning för att sådana tjänster skulle kunna utföras med förtroende var att de kunde ske säkert i form av elektronisk identifiering till exempel genom pinkoder eller koder som skrapas fram på särskilt utfärdade kort. För att få ett mer samlat grepp på lösningar för elektronisk identifiering gjorde Statskontoret sin första upphandling inom området redan 2001. Sedan dess har flera upphandlingar inom området följt.

Upphandlingarna hanterades inledningsvis av Statskontoret, sedan Ver-va och numera sköts de av Kammarkollegiet. Den huvudsakliga styrningen utgörs i dag av regeringens "Handlingsplan för e-förvaltning".²¹ För att bidra till att genomföra handlingsplanen för e-förvaltning inrättade regeringen den 26 mars 2009 Delegationen för e-förvaltning.²²

¹⁹ Ju2002/462.

²⁰ Förordningen 2003:769 med instruktion för Nämnden för elektronisk förvaltning.

²¹ Dnr Fi2008/491.

²² Dir. 2009:19.

2.3.3 Handlingsplanen

Det övergripande målet i regeringens handlingsplan för e-förvaltning beskrivs på följande sätt:

Det tidigare målet med 24-timmarsmyndigheter bör utvecklas till ett övergripande mål för förvaltningen som helhet:

År 2010 ska det vara så enkelt som möjligt för så många som möjligt att utöva sina rättigheter och fullgöra sina skyldigheter samt ta del av förvaltningens service. Där det är till fördel för medborgare och företagare samt där kvaliteten, säkerheten och produktiviteten kan höjas ska myndigheterna samverka sektorsvis. Därigenom ska Sverige återta en ledande position inom området elektronisk förvaltning.

I början av 2007 tillsatte regeringen en statssekreterargrupp för elektronisk förvaltning för att stärka styrningen av den förvaltningsgemensamma utvecklingen av e-förvaltningen. Dessutom tillsattes en arbetsgrupp, e-gruppen, med representanter för olika departement för att bistå statssekreterargruppen. De båda grupperna ska slutredovisa sitt arbete den 31 december 2009. Ett resultat av gruppernas arbete hittills är nyss nämnda Handlingsplan för eFörvaltning.

Handlingsplanen är tänkt att förbättra möjligheterna för myndighetsövergripande samverkan och integration. Enligt handlingsplanens intentioner räcker det inte att samordna statliga myndigheter. Kommunernas arbete med e-förvaltning är också av stor vikt. Det är därför viktigt att statssekreterargruppen samordnar det statliga arbetet med det som görs inom Sveriges Kommuner och Landsting.

Det övergripande målet för handlingsplanen ska uppnås via delmål inom fyra insatsområden, där det första och andra avser förutsättningar, det tredje stödprocesser och det fjärde resultat. Det är främst inom insatsområde 2 som e-legitimation behandlas. Där anges att *"elektronisk identifiering är en viktig faktor för tilliten och dialogen mellan myndigheter, medborgare och företag, då det i många ärenden finns ett tydligt behov av säker identifiering och skydd för den personliga integriteten. En av de frågor som statssekreterargruppen för arbetet med elektronisk förvaltning ska hantera och samordna är därför infrastrukturella förutsättningar för säker elektronisk kommunikation. En sådan förutsättning utgörs av väl fungerande och säkra system för elektronisk identifiering, kommunikation och informationsutbyte, vilket är avgörande för utvecklingen av såväl e-förvaltning som samhällets e-handel"*.

Även på EU-nivå bearbetas frågor om e-förvaltning. Inom ramen för Lissabonstrategins 2010-arbete antogs i september 2007 en ministerdeklaration om e-förvaltning. Deklarationen lyfter fram den ökande vikten av e-förvaltning i genomförandet av ett flertal direktiv, till exempel tjänstedirektivet.²³

²³ http://ec.europa.eu/information_society/events/ict_riga_2006/doc/declaration_riga.pdf.

2.3.4 E-delegationen

En delegation för samordning och genomförande av handlingsplanen

För att ta till vara möjligheterna till förbättringar och effektivitet i en utvecklad e-förvaltning krävs ett strategiskt synsätt på e-förvaltning som omfattar staten som helhet. Regeringen anser att det behövs ett myndighetsövergripande arbete i delegationsform för att koordinera enskilda myndigheters insatser. Regeringen har därför inrättat en e-delegation som inriktas på att genomföra regeringens handlingsplan för e-förvaltning.

E-delegationen ska komma till rätta med de styrnings- och samordningsproblem som finns på vissa håll inom statsförvaltningen, till exempel när myndigheter upphandlar och utvecklar skilda lösningar inom likartade områden. Det förekommer också att samverkansprojekt försvåras på grund av oklara förutsättningar för finansiering, organisation, teknik och rättsliga aspekter.

E-delegationen ska i nära samspel med statssekreterargruppen samordna och utveckla det fortsatta arbetet med e-förvaltningen. Den ska även samordna den offentliga sektorns deltagande i den internationella IT-standardiseringen av e-förvaltning. Samordningen ska ske på en myndighetsövergripande nivå. Delegationens huvuduppdrag är att

- utforma en strategi för myndigheternas arbete med e-förvaltning
- koordinera arbetet med e-förvaltning
- följa upp det samlade arbetet med e-förvaltning
- inventera och utveckla E-nämndens och Vervas vägledningar och rapporter.

En strategi för e-förvaltningens utveckling

E-delegationens första uppgift är att ta fram en strategi för e-förvaltningens utveckling i Sverige. Strategin ska omfatta tio områden, varav ett specifikt avser e-legitimationer. Detta område beskrivs som

- hur den offentliga sektorns försörjning av elektroniska legitimationer, det vill säga hanteringen av identifiering och underskrifter, bör genomföras i framtiden med utgångspunkt i rapporten *Säkert elektroniskt informationsutbyte och säker hantering av elektroniska handlingar*.²⁴

²⁴ Verva 2008:12.

Strategin lämnades den 19 oktober över till regeringen. E-delegationen föreslår bland annat att

- ett särskilt utvecklingsansvar för e-förvaltningen ges till utpekade myndigheter
- delegationen koordinerar utvecklingen
- en styrmodell med extern finansiering från Vinnova tas fram
- delegationen ska ta fram en kalkylmodell för att beräkna nyttan av och kostnaden för strategiska e-förvaltningsprojekt
- mallar för överenskommelser i samverkansprojekt tas fram
- en vägledning för myndigheternas verksamhetsplanering tas fram och utifrån planeringen ska myndigheternas åtgärder och initiativ kategoriseras i infrastrukturella tjänster, bastjänster för informationsförsörjning, egenproducerade tjänster och gemensamt producerade tjänster
- det tillsätts en nämnd inom Skatteverket som får rätt att meddela föreskrifter i fråga om bland annat standarder
- vissa myndigheter får i uppdrag att i försöksverksamhet utveckla så kallade gemensamma administrativa verksamhetsstöd
- regeringen bör ställa krav på att myndigheterna tar fram en strategi för sin försörjning av IT-tjänster
- en samordningsfunktion för e-legitimationer inrättas i form av en nämnd med föreskriftsrätt inom Skatteverket
- ett nytt system för e-legitimation skapas baserat på federationsteknik²⁵

²⁵ Federationsteknik innebär i korthet att man skapar en sammanslutning (federation) med en gemensam policy för säkerhetsnivåer och hur identitet ska fastställas. Vilken lösning eller teknik som används för identifiering spelar ingen roll i en federativ lösning, utan federativ teknik möjliggör att passa in olika tekniska lösningar och integrera dessa i e-tjänsteleverantörens system. Programvaran är normalt öppen och standardiserad. Exempel på federationsteknik är SAML.

3 Regeringens styrning och myndigheternas insatser

I detta avsnitt redogör vi för våra iakttagelser rörande regeringens och de ansvariga myndigheternas åtgärder inom systemet för e-legitimationer. Avsnittet beskriver också i korthet på vilket sätt regeringen har styrt övergången till elektronisk förvaltning under åren 1998 till 2004. Syftet med avsnittet är att ge en översiktlig bild av regeringens generella styrning och vilka förutsättningar den har skapat för de myndigheter som sedan har haft i uppdrag att förverkliga övergången.²⁶ Skälet till att göra en beskrivning av regeringens styrning av övergången till elektronisk förvaltning är att regeringens och myndigheternas hantering av systemet för e-legitimationer inte kan ses isolerad från frågan om utveckling och finansiering av e-tjänster och en gemensam elektronisk infrastruktur för den offentliga förvaltningen.

Utgångspunkten för iakttagelserna i detta kapitel är riksdagens uttalande om att regeringen och ansvariga myndigheter ska

- gynna användningen av e-legitimationer
- stimulera konkurrensen mellan utfärdare av sådana legitimationer och undanröja infrastrukturella, marknadsmässiga och konkurrensmässiga hinder
- säkra en dynamisk utveckling av informationssamhällets säkerhetslösningar
- gynna kostnadseffektiviteten i säkerhetslösningarna
- verka för att det etableras teknikneutrala standarder för elektroniska signaturer inom offentlig sektor
- säkerställa att rättssäkerheten eller myndigheters förutsättningar inte har försämrats med anledning av e-legitimationer.

²⁶ Genomgången är en sammanställning av ett kapitel ur Riksrevisionens rapport *Vem styr den elektroniska förvaltningen?* (RiR 2004:19). Avsnittet är i stort sett en ordagrann men förkortad återgivning av bilagan i den tidigare rapporten.

3.1 Regeringens generella mål- och resultatstyrning av e-politiken

En viktig utgångspunkt för regeringens styrning var att myndigheterna skulle ha en betydande självständighet att själva avgöra vilka e-tjänster som skulle utvecklas, hur och när. Enligt vad Riksrevisionen kunde konstatera 2004²⁷ ledde det till att fackdepartementen under åren 1999 till 2002 inte styrde myndigheterna med mål och återrapporteringskrav rörande elektronisk förvaltning i regleringsbreven.²⁸ Under 2003 började dock regeringen använda en mer formell styrdialog för att få en tydligare styrning av statliga myndigheter mot målen för elektronisk förvaltning, och i budgetpropositionen för 2003 angav regeringen att det är nödvändigt med en tydligare styrning av statliga myndigheter mot målen för 24-timmarsmyndigheten.

Regeringens val av aktiviteter för att styra och påverka arbetet med att införa elektronisk förvaltning byggde enligt uppgifter från Regeringskansliet främst på följande

- Regeringen definierade inledningsvis sin roll som att sätta övergripande mål för den elektroniska förvaltningen, att undanröja hinder, att via Statskontoret med flera ge stöd till myndigheterna samt verka för att en gemensam infrastruktur för elektronisk kommunikation upphandlas.
- Myndigheterna gavs en betydande självständighet att själva avgöra hur de ska använda sina resurser för att uppnå eftersträvat resultat.
- Huvudansvaret för att utveckla den elektroniska förvaltningen åvilade myndigheterna själva, eftersom de ansågs känna till "kundernas" behov bäst och därmed bäst kunde avgöra vilka e-tjänster som skulle prioriteras.
- Förvaltningens satsning på elektronisk förvaltning skulle bygga på kostnadseffektiva lösningar kopplade till verksamhetsutvecklingen. Utveckling av e-tjänster skulle rymmas inom anslaget.

Även om myndigheterna har givits en betydande självständighet i arbetet med e-politiken är myndigheterna skyldiga att förse regeringen med underlag för riksdagens och regeringens långsiktiga ställningstagande.

Riksrevisionen konstaterade 2004²⁹ att regeringen hade tagit del av andra länders satsningar på elektronisk förvaltning. Flera regeringar angav mycket precisa mål, till exempel prioritering av e-tjänster som skulle utvecklas, tidpunkter när e-tjänsterna skulle finnas tillgängliga och vilken grad av användning e-tjänsterna skulle uppnå. Den svenska regeringen valde dock att inte använda denna typ av mer riktad central styrning av övergången till

²⁷ RiR 2004:19.

²⁸ Det fanns dock vissa undantag såsom Riksskatteverket och Tullen.

²⁹ RiR 2004:19.

elektronisk förvaltning, utan valde i stället att styra genom att utveckla förutsättningar för e-tjänsterna och låta myndigheterna själva avgöra vilka tjänster som skulle utvecklas.

Vad gäller regeringens uppföljning av 24-timmarmyndigheten så utgick den från de avrapporteringar som Statskontoret lämnade halvårsvis. Utöver detta så gav regeringen även Institutet för tillväxtpolitiska studier uppdraget att utvärdera regeringens IT-politik. Regeringen beställde även en granskning av myndigheternas IT-baserade verksamhetsutveckling i form av ett så kallat kontrollprojekt av Riksrevisionsverket.³⁰ Utöver själva huvuduppdraget påtalade Riksrevisionsverket även vissa problem i förvaltningens satsning på e-tjänster, bland annat vikten av att regeringen skapar bra förutsättningar, inte minst starka incitament, för ökad samverkan mellan myndigheter beträffande e-tjänster. RRV pekade särskilt på att en försvårande omständighet inträder då kostnader och besparingsmöjligheter är ojämnt fördelade mellan de myndigheter som har möjligheter att etablera en gränsöverskridande verksamhetsprocess. RRV konstaterade att detta var ett betydande hinder för uppbyggnaden av integrerade processer i samverkan. RRV föreslog att finansieringslösningar skulle tas fram av den av regeringen aviserade Delegationen för utveckling av offentliga e-tjänster.

3.1.1 *Styrning genom finansiering av utveckling av e-tjänster*

Regeringen ställde som ett viktigt krav att e-tjänster skulle vara till nytta för medborgare och företag samt vara kostnadseffektiva och att utvecklingskostnaderna skulle rymmas inom förvaltningsanslaget. Konsekvensen av detta blev att regeringen i princip inte ökade enskilda myndigheters anslag för utveckling av e-tjänster. I praktiken utvecklade även myndigheter e-tjänster inom ramen för sina sakanslag. Regeringen anvisade dock i enstaka fall särskilda medel för utvecklingen av e-tjänster, bland annat för Arbetsmarknadsstyrelsen, Konsumentverket och länsstyrelserna. Viss finansiering av bland annat forskning om elektronisk förvaltning skedde genom forskningsråd. Vinnova var en av flera statliga myndigheter som bedrev forskning om elektronisk förvaltning. Angående finansieringsfrågan uttalade regeringen i budgetpropositionen 2002/03 att

”Regeringens bedömning utifrån arbetet hittills är att det finns stora möjligheter till serviceförbättringar genom elektroniska samhällstjänster, till stor nytta för medborgare och företag, och därmed för demokrati och tillväxt. Ett problem är emellertid att de utvecklingsinsatser som krävs för att uppnå de av regeringen

³⁰ IT i verksamhetsutvecklingen, Bättre styrning av myndigheternas investeringar i IT-baserad verksamhetsutveckling, RRV 2002:30.

uppsatta målen inte alltid leder till omedelbara myndighetsinterna effektivitetsvinster som kan finansiera grundinvesteringarna i de nya elektroniska tjänsterna. Vinsterna uppstår istället hos företag och medborgare och kan således inte kapitaliseras av myndigheterna. Under de närmaste åren finns därför skäl att utreda behovet av särskilda insatser för att stimulera utvecklingen av elektroniska samhällstjänster³¹”.

3.2 Regeringens specifika åtgärder

3.2.1 Övergripande ansvar

Regeringen har under den period som e-legitimationer har existerat valt att lägga det övergripande ansvaret för e-frågor på två olika myndigheter, Statskontoret och sedan Verva.

Statskontoret har, fram till dess uppgifterna överfördes till Verva 2006, varit den myndighet som regeringen pekat ut som särskilt ansvarig för bland annat IT-frågor och förvaltningens utveckling. I regleringsbrevet för Statskontoret under perioden 2000 till 2003 gav regeringen myndigheten i uppdrag att

- erbjuda myndigheterna stöd på IT- och teleområdet så att en enhetlig, säker och stabil elektronisk infrastruktur utvecklas samt så att villkoren förbättras och kostnaderna sänks för myndigheternas användning av tjänster och utrustning på området
- bidra till utvecklingen av den tekniska infrastrukturen för data- och telekommunikation genom att i samverkan med dels statliga myndigheter, dels kommuner och landsting främja utvecklingen och användningen av gemensamma standarder och tillämpningar
- göra en bedömning av hur det fortsatta arbetet med att vidareutveckla den elektroniska infrastrukturen bör inriktas
- i samverkan med statliga myndigheter, kommuner, landsting samt företrädare för forskning och näringsliv driva pilotprojekt på strategiska områden för utvecklingen av den tekniska infrastrukturen i förvaltningen
- främja utvecklingen av offentliga elektroniska tjänster och därvid även verka för effektivisering av informationsförsörjningen i samhället.

I regleringsbrevet för Verva åren 2006 till 2008 framgår att myndigheten ska

- driva på utvecklingen och användningen av elektroniska tjänster för att öka nyttan för medborgare och företag
- bidra till ökad användning av förvaltningen gemensamma grundfunktioner för elektroniska tjänster och elektronisk kommunikation

³¹ Budgetpropositionen 2002/03:1 Utgiftsområde 2, s. 28.

- verka för att utvecklingen av elektronisk förvaltning står sig väl i internationell jämförelse och för att en harmonisering med europeisk utveckling av elektroniska tjänster och elektronisk kommunikation blir möjlig
- se till att förvaltningen tillämpar en säker, effektiv och samordnad informationshantering
- utveckla förvaltningsgemensamma specifikationer som kan ligga till grund för myndigheternas utvecklingsarbete
- främja användningen av ändamålsenliga varor och tjänster inom området informationsteknik genom upphandling till effektiva villkor och låga kostnader.

3.2.2 *Specifika uppdrag*

Den 21 december 2000³² uppdrog regeringen åt Riksskatteverket att under ett inledningsskede ha ett sammanhållande ansvar för administrationen av certifikat för elektronisk identifiering och elektroniska signaturer inom statsförvaltningen. I uppdraget ingick att för statsförvaltningen utarbeta allmänna riktlinjer och gemensamma rutiner för elektronisk identifiering, signering och stämpling av elektroniska handlingar med metoder baserade på så kallad PKI-teknik och certifikat. Samverkansprojektet fick beteckningen Samset-projektet och hade i uppdrag att under ett inledningsskede ansvara för administrationen av elektroniska id-handlingar (e-legitimationer), elektronisk identifiering och elektroniska underskrifter inom statsförvaltningen. Här ingick såväl juridiska som tekniska och ekonomiska frågor. De senare handlade främst om hur medborgare och företag kunde förses med e-legitimationer och om hur dessa skulle finansieras. Uppdraget genomfördes i samverkan mellan Riksskatteverket, Riksförsäkringsverket, Patent- och Registreringsverket samt Statskontoret.

Samset-projektets uppgifter överfördes under 2004 och 2005 till den nyinrättade *e-nämnden* (Nämnden för elektronisk förvaltning). I uppdraget till e-nämnden ingick bland annat aktiv förvaltning av vägledning om myndigheters användning av elektroniska legitimationer.³³ Inom uppdraget skulle nämnden

- förvalta den grundläggande vägledningen för myndigheternas användning av e-legitimationer och elektroniska underskrifter
- förvalta vägledningen för användargränssnitt som uppfyller legala krav och genomföra användbarhetstester av gränssnittens grafiska element (ikoner)

³² Ju2000/4939.

³³ e-nämnden dnr 2004/19-3.

- informera om och marknadsföra arbetet med vägledningarna för myndigheternas användning av e-legitimationer och elektroniska underskrifter
- följa upp användningen av vägledningarna.

Den 30 november 2006 beslutade³⁴ regeringen att Verva skulle leda och samordna statsförvaltningens utvecklingsarbete med säkert elektroniskt informationsutbyte och säker hantering av elektroniska handlingar.

Verva fick i uppdrag att

- ge myndigheterna vägledning i deras införande av lösningar för säkert elektroniskt informationsutbyte och säker hantering av elektroniska handlingar. Verket skulle därvid beakta arbete som bedrivs av andra myndigheter med ansvar på området
- utveckla riktlinjer och specifikationer som skulle vara gemensamma för förvaltningen och som kunde ligga till grund för myndigheters och kommuners säkra elektroniska informationsutbyte och hantering av elektroniska handlingar samt för såväl centrala ramavtalsupphandlingar som andra upphandlingar av tjänster och teknik på området
- bedöma behovet av reglering på området
- vid behov utfärda föreskrifter inom ramen för verkets bemyndigande enligt förordningen (2003:770) om statliga myndigheters elektroniska informationsutbyte.

Verva fick i sitt regleringsbrev för år 2006³⁵ i uppdrag att se över gällande ramavtal som är av betydelse för användningen av elektronisk identifiering. Syftet med översynen var att främja förvaltningens användande av elektroniska legitimationer i verksamheten. Myndigheten skulle redovisa sina förslag till åtgärder senast den 31 januari 2006. Med anledning av Vervas översyn av ramavtalen fick man i juni 2006 i uppdrag av regeringen³⁶ att genomföra ett treårigt program med syfte att främja användningen av e-legitimationer i offentlig förvaltning.

Som ett resultat av sin handlingsplan för e-förvaltning gav regeringen Verva i uppdrag att göra en uppföljning av myndigheternas strategiska åtgärder inom området e-förvaltning. I uppdraget stod bland annat att myndigheterna ska redovisa pågående och planerade åtgärder som är av strategisk betydelse för e-förvaltningsarbetet och som rör

- användning av e-legitimationer
- IT-standardiseringsarbete med betydelse för e-förvaltning

³⁴ Fi2006/6773, Fi2006/967.

³⁵ Fi2005/6390 .

³⁶ Fi2006/3207.

- pågående och planerade IT-investeringar som är av strategisk betydelse för utvecklingen av e-förvaltning
- e-tjänster som skulle kunna integreras till nytta för medborgare och företagare.

Verva fick i uppgift att utveckla riktlinjer för berörda myndigheters redovisning av ovan beskrivna åtgärder. Dessa skulle publiceras senast den 29 februari 2008. Baserat på myndigheternas redovisningar skulle Verva sammanställa och analysera egna och berörda myndigheters insatser och resultat såvitt avser den strategiska utvecklingen av elektronisk förvaltning. Resultaten skulle rapporteras till Regeringskansliet (Finansdepartementet) senast den 15 oktober 2008.³⁷

3.3 Myndigheternas specifika åtgärder

I en skrivelse till regeringen³⁸ den 16 april 1999 redovisade Statskontoret förslag till fortsatt arbete rörande strukturer för hantering av certifikat och kryptonycklar. Statskontoret föreslog att regeringen skulle ge Riksskatteverket i uppdrag att i samarbete med Riksförsäkringsverket, PRV och Statskontoret att arbeta vidare med förutsättningarna för att etablera en statlig certifikatutgivare för e-legitimationer. Uppdraget skulle innebära att myndigheterna skulle föreslå en lämplig finansieringsmodell och vilken myndighet som borde ges uppdraget att vara statlig utgivare av e-legitimationer. De ansvariga myndigheterna föreslogs även få ett ansvar att vidare utreda kraven på elektronisk signatur i statsförvaltningen.

Den 21 december 2000 uppdrog regeringen enligt Statskontorets förslag åt Riksskatteverket att under ett inledningsskede ha ett sammanhållande ansvar för administrationen av certifikat för elektronisk identifiering och elektroniska signaturer inom statsförvaltningen. Resultatet av detta blev att Riksskatteverket, Statskontoret och några av de större myndigheterna utarbetade riktlinjer och tog fram en vägledning till riktlinjerna. Statskontoret och RSV upphandlade tjänster för elektronisk identifiering och signering. Upphandlingen baserades på de krav med mera som framtagits i ett samarbete mellan de fyra myndigheterna och representanter från bland andra universitet och landsting.

Upphandlingen resulterade i att Statskontoret tecknade ramavtal med fem leverantörer av tjänster för elektronisk identifiering av privatpersoner. De leverantörer som valdes i den första upphandlingen 2001, och som fick teckna ramavtal, är i stort sett identiska med de leverantörer som har ramav-

³⁷ Verva, *69 myndigheter redovisar 915 strategiska insatser för utveckling av e-förvaltning*, 2008:14.

³⁸ Ju 1999/2004/F.

tal 2009. Den tekniska lösningen är också i stort sett densamma 2009 som 2001.

Den vägledning som Samset tog fram gällde för användningen av id- och infratjänster som upphandlats av Statskontoret. Dessa tjänster avsågs stödja 24-timmarsmyndigheterna vid införandet av e-legitimationer och elektroniska underskrifter. Användare av dessa tjänster är myndigheter och fysiska personer i deras egenskap av privatpersoner eller företrädare för företag, till exempel firmatecknare eller ombud. Andra sätt att företräda ett företag omfattas inte av vägledningen och sådana tjänster har heller inte upphandlats. Vägledningens syfte var att

- göra användningen av e-legitimationer lika enkel och begriplig som användningen av traditionella identitetshandlingar och att ensa hanteringen så att användarna känner igen sig från tjänst till tjänst
- ta till vara vedertagna juridiska synsätt även i myndigheternas e-tjänster.

Vägledningen innehöll en gemensam begreppsapparat som utarbetats med bland annat utfärdarna av e-legitimationer och dessas underleverantörer och syftade till att använda termer som är lätta för användare att förstå. Den byggdes emellertid på med ensade formuleringar för vissa grundläggande och återkommande funktioner. En viktig del i arbetet var att "vanliga" användare skulle kunna förstå vad de gjorde och om ifall deras agerande kunde leda till rättshandlingar eller föra med sig andra betydelsefulla verkningar.

Som ett svar på regeringens uppdrag att se över då gällande ramavtal föreslog Verva följande åtgärder:

- För att lösa kostnadsfrågan; centrala medel ställs till förfogande så att de myndigheter, som ännu inte ingått avtal för eID och infratjänst, får kostnader täckta under en inledande period, när nya tjänster går i drift.
- För att lösa avtalsfrågan; när medel har avsatts får Verva i uppdrag att skapa en överblick över de aktuella myndigheternas planer på e-tjänster som förutsätter eID samt ta fram standardiserade former för avrop under ramavtalen Elektronisk identifiering (eID) 2004 och Infratjänst 2003, som stöd till både myndigheters avrop och fördelning av ekonomiska garantier.
- För att lösa fördelningsfrågan; Verva får i uppdrag att använda de centrala medel som ställs till förfogande till att, under en begränsad inledande period, för de myndigheter som sätter nya e-tjänster i drift, svara för nyuppkomna kostnader för eID och infratjänst till stöd för eID.

Verva fick i juni 2006 i uppdrag av regeringen att genomföra ett treårigt program med syfte att främja användningen av e-legitimationer i offentlig förvaltning. Arbetet avrapporterades 2008 i rapporten *Tre års främjande av e-tjänster med e-legitimation*³⁹ och de slutsatser som drogs var:

³⁹ Verver 2008:16.

- Verva hade bidragit till att fler organisationer använde sig av e-legitimationer genom programmet.
- De organisationer som hade fått stöd använde e-tjänster med e-legitimation relativt begränsat. Därtill byggde transaktionerna huvudsakligen på identifieringar. Området behövde enligt Verva analyseras vidare.
- E-tjänster är ofta krävande att införa. Flera offentliga organisationer frågar efter stöd. Flera organisationer har haft problem med att integrera e-id i sina e-tjänster. Bland annat ska delsystem och processer integreras med varandra och en rad leverantörer blandas in. Trots att kommunerna erbjöd liknande e-tjänster, samordnade de sällan sitt arbete.
- Prismodeller för e-id borde baseras på rörliga priser, dvs. betala efter användning. Prismodeller där man köper och förbetalar paket med fri användning av e-id ger en trygghet och ett slags skydd mot kostnadsökningar vid kraftiga ökningar i användningen av e-tjänster. Rapporten visade dock att ökningstakten var måttlig. De förbetalade paketen blir därmed en dyr ”försäkring”. Eventuellt framtida ekonomiskt stöd borde därför bygga på den modell som Verva presenterade i sin rapport.
- Verva bidrog till en lägre prisbild för elektronisk identifiering. I samband med ramavtalsupphandlingarna 2004 halverade leverantörerna sina priser.

Verva publicerade, inom ramen för det uppdrag man 2006 fick av regeringen, 2007 rapporten *Säkert informationsutbyte och säker hantering av elektroniska handlingar*⁴⁰, vilken var en färdplan för e-legitimationens utveckling i Sverige. I korthet var slutsatserna i färdplanen att

- den nuvarande modellen inte skulle störas. Det fanns redan väl spridda och fungerande lösningar för eID
- det fanns en likhet med fysiska legitimationer. En innehavare av en godkänd elektronisk e-legitimation skulle kunna använda detta för alla tjänster
- man byggde vidare på den svenska modellen med marknadslösning och konkurrens
- det nationella ID-kortet som utfärdas av RPS skulle kunna bli bärare av e-legitimation
- det skulle skapas fler unika identifierare än personnummer. Detta skulle kunna lösa problematiken för dem som saknar personnummer
- det skulle skapas tydliga regelverk, godkännandekriterier som differentierade säkerhetsnivåer och informationsklasser samt standardisering. Man skulle gå mot certifiering av lösningar
- integritetsfrågor beaktades
- avtals- och betalningsmodeller förenklades
- tekniska lösningar utvecklades.

⁴⁰ Verver 2007:13.

I Vervas "Slutrapport om säkert informationsutbyte och säker hantering av elektroniska handlingar"⁴¹ lämnade man ett antal förslag till regeringen om framtidens svenska e-legitimation. Verva utvecklades den 31 december 2008 och Vervas uppdrag gick över till ett antal andra myndigheter, bland annat Kammarkollegiet som fick ansvar för upphandling och ramavtal för e-legitimationer. E-delegationen inrättades 2009 och lämnade den 19 oktober ett förslag till strategisk plan för utvecklingen av den svenska e-förvaltningen. Planen innehåller flera konkreta förslag till åtgärder inom området e-legitimation.

3.4 Sammanfattande kommentarer

Sammanfattande kommentarer om de åtgärder som vidtagits av regeringen och ansvariga myndigheter i relation till de utgångspunkter som redovisades i inledningen till kapitel 3:

- Regeringen och ansvariga myndigheter har vidtagit vissa åtgärder för att gynna användningen av e-legitimationer. En sådan åtgärd var det treåriga finansieringsprogrammet där myndigheter, kommuner och landsting fick ansöka om finansieringsstöd hos Verva för att införa e-legitimationer i sina system.
- Regeringen och ansvariga myndigheter kan inte sägas ha vidtagit några direkta åtgärder för att stimulera konkurrensen och undanröja infrastrukturella, marknadsmässiga och konkurrensmässiga hinder. En indikation på detta är att de leverantörer som har ramavtal 2009 med Kammarkollegiet är i stort sett desamma som de leverantörer som fick ramavtal 2001 med Statskontoret.
- Regeringen och ansvariga myndigheter kan inte heller sägas ha säkrat en dynamisk utveckling av informationssamhällets säkerhetslösningar. Den tekniska lösningen i dagens e-legitimation är i princip densamma som 2001. Informationssamhällets säkerhetslösningar har visserligen utvecklats, men denna utveckling kan inte tillskrivas regeringen och ansvariga myndigheter.
- Kostnadseffektiviteten i systemet för e-legitimationer har blivit bättre med åren men det är svårt att härleda dessa förbättringar till några åtgärder som regeringen och ansvariga myndigheter vidtagit.
- Regeringen och ansvariga myndigheter har inte vidtagit några specifika åtgärder för att etablera teknikneutrala standarder för elektroniska signaturer inom offentlig sektor. Regeringen och ansvariga myndigheter har vidtagit vissa åtgärder för att säkerställa att rättssäkerheten eller myndigheters förutsättningar inte försämras med anledning av e-legitimationer.

⁴¹ Vervar 2008:12.

4 Rättssäkerhet

I detta avsnitt redogörs för de iakttagelser som vi har gjort med anknytning till rättssäkerhet. Riksdagen har uttalat att utnyttjandet av IT inte får försämrade rättssäkerheten eller myndigheternas förutsättningar att fungera. Kravet på rättssäkerhet gäller för all statlig verksamhet, således även e-legitimationer.

4.1 Integritet

Integritetsfrågor med anknytning till e-legitimation kan delas upp i två olika delar. En del rör integritet i bemärkelsen skydd av personuppgifter, vilket innebär att obehöriga inte får tillgång till uppgifterna. Den andra delen rör frågor kring vem som ska hantera personuppgifter och på vilket sätt denna aktör ska få hantera uppgifterna.

4.1.1 Skydd för personuppgifter

Skydd av personuppgifter innebär att obehöriga inte ska kunna få tillgång till dem. När det gäller åtkomst av personuppgifter i samband med hanteringen av e-legitimationer uppstår främst frågor om den tekniska lösningen och om den är tillräckligt säker för att kunna användas för exempelvis inloggning hos en myndighet då detta kan ge tillgång till en mängd personuppgifter.

Hanteringen av personuppgifter och de krav som ställs till följd av sådan hantering regleras främst av personuppgiftslagen.⁴² Syftet med personuppgiftslagen är enligt lagens 1 § att skydda människor mot att deras personliga integritet kränks genom behandling av personuppgifter. Systemet med e-legitimationer berör också bankerna, som hanterar personuppgifter i form av kundregister, och dessa faller under personuppgiftslagens tillämpningsområde. Det gör också de personuppgifter som registreras när en kund tecknar ett avtal om e-legitimation.

Av 10 § personuppgiftslagen framgår att personuppgifter bara får behandlas om den registrerade har lämnat sitt samtycke till behandlingen eller om behandlingen är nödvändig för att

⁴² Personuppgiftslag (1998:204).

- a) ett avtal med den registrerade skall kunna fullgöras eller åtgärder som den registrerade begärt skall kunna vidtas innan ett avtal träffas,
- b) den personuppgiftsansvarige skall kunna fullgöra en rättslig skyldighet,
- c) vitala intressen för den registrerade skall kunna skyddas,
- d) en arbetsuppgift av allmänt intresse skall kunna utföras,
- e) den personuppgiftsansvarige eller en tredje man till vilken personuppgifter lämnas ut skall kunna utföra en arbetsuppgift i samband med myndighetsutövning, eller
- f) ett ändamål som rör ett berättigat intresse hos den personuppgiftsansvarige eller hos en sådan tredje man till vilken personuppgifterna lämnas ut skall kunna tillgodoses, om detta intresse väger tyngre än den registrerades intresse av skydd mot kränkning av den personliga integriteten.

Vidare framgår av 31 § i personuppgiftslagen ett uttryckligt krav på att den personuppgiftsansvarige ska vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Säkerhetsnivån ska enligt samma paragraf vara lämplig med beaktande av de tekniska möjligheter som finns, vad det skulle kosta att genomföra åtgärderna, de särskilda risker som finns med behandlingen av personuppgifterna och hur pass känsliga de behandlade personuppgifterna är.

Bankernas val av tekniska lösningar för att skydda kundregister eller uppgifter som registreras i samband med att kunden tecknar ett avtal om e-legitimation är en fråga som får betydelse även för de personuppgifter som finns åtkomliga hos myndigheten. Om det är möjligt för en obehörig att ta sig in i en enskild persons Internetbank så är det sedan möjligt för den obehörige att ladda ner en e-legitimation och använda den gentemot en myndighets e-tjänst. Det innebär att säkerhetsnivån på själva e-legitimationen blir betydelselös i ett sådant fall. Den tekniska lösningen för inloggning på en Internetbank faller under såväl Finansinspektionens tillsyn som Datainspektionens. Lösningen för inloggning ska uppfylla de krav som följer av 31 § i personuppgiftslagen, och Datainspektionen har ett ansvar för att granska att så är fallet.

Det skydd som gäller för de personuppgifter som återfinns hos en myndighet och som kan nås genom e-tjänster och e-legitimation är också beroende av hög teknisk säkerhet hos själva e-legitimationen. Dagens tekniska lösning för e-legitimationer baseras på specifikationer framtagna av Skatteverket på uppdrag av regeringen.⁴³ Kraven för vilken säkerhetsnivå lösningen ska uppfylla definieras i ramavtalsupphandlingen. Datainspektionen ställer vidare krav när det gäller autentisering vid hanteringen av känsliga personuppgifter. Kraven innebär att den bör byggas på säkra metoder, såsom

⁴³ Verva, *Förstudie eID 2007 Elektronisk identifiering och underskrift*, 2007:16.

e-legitimation, engångslösenord eller motsvarande.⁴⁴ Riksrevisionen har vid dokumentstudier, intervjuer och vid ett seminarium med en fokusgrupp, inte kunnat finna några indikationer på att dagens lösning för e-legitimationer är bristfällig vad gäller den tekniska säkerheten. Vid kvalitetssäkringen i fokusgruppen uppgav exempelvis företrädare för Försäkringskassan att man endast hade haft två incidenter rörande säkerhet sedan myndigheten införde möjligheten att använda e-legitimation.

4.1.2 Tillgång till personuppgifter

Den andra aspekten av integritet handlar om vem som överhuvudtaget ska ha tillgång till personuppgifter och hur dessa ska behandlas. Det har av Sveriges Kommuner och Landsting framförts viss kritik mot att bankerna baserar e-legitimationerna på sina kundregister.⁴⁵ Det faktum att myndigheterna frågar bankerna om giltigheten innebär att banken får tillgång till information om mot vem och när den enskilde använder sin e-legitimation. Sveriges Kommuner och Landsting anser att det bör vara en statlig uppgift att utfärda och garantera medborgarnas identitet, särskilt med tanke på att folkbokföringen är en statlig angelägenhet. Skälen för att identitetshantering bör vara en statlig uppgift blir enligt Sveriges Kommuner och Landsting ännu tydligare om nya säkerhetslösningar som inkluderar exempelvis fingeravtryck eller dna tas i bruk i framtiden.⁴⁶ När användaren brukar en e-tjänst lagras information om detta hos utfärdaren. Eftersom e-legitimationen innehåller personuppgifter i form av bland annat personnumret och gentemot vem och när användaren använder e-legitimationen innebär det i sin tur att stora mängder personuppgifter finns lagrade hos olika utfärdare.

Med tanke på den förväntade ökningen av användandet av e-legitimationer i kombination med att ingen aktör verkar ha gjort en grundlig teknisk granskning av e-legitimationer för att skaffa sig en övergripande bild av vilka eventuella risker som finns i systemet kan stora mängder personuppgifter bli tillgängliga för en obehörig vid ett intrång i systemet.⁴⁷

Eftersom hanteringen innefattar behandling av personuppgifter är personuppgiftslagen tillämplig, och det finns därför ett regelverk som styr hur hanteringen ska skötas och hur tillsynsmyndigheten, Datainspektionen, ska utöva tillsyn över hanteringen. Det bör även uppmärksammas att det utöver

⁴⁴ Datainspektionen, IT-säkerhet och myndigheters e-tjänster.

⁴⁵ Intervju med företrädare för Sveriges Kommuner och Landsting.

⁴⁶ Intervju med företrädare för Sveriges Kommuner och Landsting.

⁴⁷ Detta problem kan lösas genom till exempel det förslag som e-delegationen har fört fram angående federationsteknik där det finns möjligheter att dölja identiteten men samtidigt behålla spårbarheten.

personuppgiftslagen även råder banksekretess.⁴⁸ Den omfattar alla uppgifter som rör en bankkunds mellanhavanden med banken, oavsett om uppgiften är skriftlig eller muntlig. Sekretessen gäller även kundens tidigare förbindelser med banken, det vill säga sekretessen upphör inte i och med att någon slutar att vara kund i banken. Dessutom gäller sekretessen för evigt.⁴⁹

4.2 Tillsyn och övervakning av systemet

4.2.1 Ansvaret för tillsyn och övervakning

E-legitimationer för identifiering av individer som vill använda e-tjänster är i dag en frekvent använd lösning bland annat av Skatteverket och Försäkringskassan. E-legitimationer är också ett verktyg för att skydda den enskilde individens integritet. Detta borde motivera ett intresse från statens sida att följa upp och säkerställa kvalitet och säkerhet hos e-legitimationer. Ett möjligt verktyg för detta är tillsyn.

Kammarkollegiet är den myndighet som tecknar ramavtal för statsförvaltningen som helhet om elektroniska identifieringstjänster. Ramavtalet innehåller specifikationer för de tekniska villkoren och även för leverantörernas skyldigheter i övrigt. Kammarkollegiet har i uppdrag att följa upp de ramavtal man tecknar. Något formellt tillsynsansvar har dock inte Kammarkollegiet.

Finansinspektionen har enligt sin instruktion ansvarar för tillsynen, regelgivningen och tillståndsprovningen som rör finansiella marknader och finansiella företag.⁵⁰ Myndigheten har också till uppgift att verka för ett gott konsumentskydd inom sitt ansvarsområde.⁵¹ Finansinspektionen har i ett dokument om verksamhetens inriktning för år 2009 uppgivit att *"FI har traditionellt endast bedrivit begränsad tillsyn över IT:n i företagen. Det har huvudsakligen ingått i vår tillsyn över hur företagen mäter och hanterar operativa risker" och "IT-tillsyn ur konsumentens perspektiv har varit förhållandevis begränsad"*.⁵²

Datainspektionen har enligt sin instruktion till uppgift att verka för att människor skyddas mot att deras personliga integritet kränks genom behandling av personuppgifter och för att god sed iakttas i kreditupplysnings- och inkassoverksamhet. Myndigheten ska följa och beskriva utvecklingen på IT-området när det gäller frågor som rör integritet och ny teknik.⁵³ Myndigheten är tillsynsmyndighet enligt personuppgiftslagen.⁵⁴

⁴⁸ Se 10 § lagen (2004:297) om bank- och finansieringsrörelse.

⁴⁹ Se http://www.konsumentbankbyrå.se/artikel/article.asp?_tp_article_id=151&avd=&menu=ART_%C3%96VT.

⁵⁰ 1 § förordning (2007:841) med instruktion för Finansinspektionen.

⁵¹ 2 § förordning (2007:841) med instruktion för Finansinspektionen.

⁵² Finansinspektionen, Inriktningsdokument 2009, promemoria upprättad 2008-10-06.

⁵³ 1 § förordning (2007:975) med instruktion för Datainspektionen.

⁵⁴ Personuppgiftsförordningen (1998:1191).

Post- och telestyrelsen är enligt sin instruktion förvaltningsmyndighet med ett samlat ansvar inom postområdet och området för elektronisk kommunikation. Myndigheten ska beskriva och analysera utveckling och resultat inom sitt ansvarsområde och rapportera detta till regeringen. Myndigheten ska särskilt uppmärksamma och analysera eventuella problem inom området och, när det är påkallat, vidta eller lämna förslag till lämpliga åtgärder.⁵⁵

4.2.2 Vilken tillsyn genomförs?

Riksrevisionen har ombett myndigheterna att beskriva den tillsyn de bedriver i relation till e-legitimationer. Resultatet av denna enkät är följande.

Post- och telestyrelsen har uppgivit att de avancerade signaturer som används inom dagens system för e-legitimation inte omfattas av myndighetens tillsynsansvar. Myndigheten uppger även att lagen om elektronisk kommunikation primärt avser elektroniska kommunikationsnät och tjänster och att den inte är direkt tillämplig på elektroniska signaturer. Myndigheten har enligt egen uppgift således inget tillsynsansvar för dagens system för e-legitimationer.

Finansinspektionen har uppgivit att inspektionens tillsyn omfattar bankernas användning av och erbjudande om e-legitimation, i den mån som finansinstitut använder sig av e-legitimation i sin verksamhet, till exempel för att uppfylla kravet i lagen (2009:62) om åtgärder mot penningtvätt och finansiering av terrorism på att kunderna ska identifieras. Myndigheten uppger dock att man inte utövar någon tillsyn över produkten som sådan utan att det snarare är institutets hantering av produkten som faller under Finansinspektionens tillsyn. Finansinspektionen godkänner inte i förväg de produkter eller tjänster som företagen under tillsyn erbjuder eller använder sig av. Genom att en banks kunder kan använda e-legitimation för att identifiera sig på distans blir bankernas användande av e-legitimation något som Finansinspektionen kan komma att granska ur penningtvättshänseende i ett enskilt fall. Det är i ett sådant fall fråga om att ha tillsyn över att bankerna uppfyller kravet på kundkännedom i penningtvättslagstiftningen. Finansinspektionen anser sig dock inte ha tillsynsansvar vare sig för e-legitimation som sådan eller över bankernas utfärdande av e-legitimation. I den produktklassificering utifrån riskperspektiv som myndigheten gjort har e-legitimation inte ansetts vara någon produkt eller tjänst med hög risk. Därför har Finansinspektionen hittills inte haft anledning att särskilt granska institutets hantering av e-legitimationer. Det har heller inte enligt myndigheten funnits skäl att närmare diskutera eventuella problem med gränsdragningen mellan Finansinspektionens tillsyn och andra myndigheters tillsyn.

⁵⁵ 1 § förordning(2007:951) med instruktion för Post- och telestyrelsen.

Datainspektionen har uppgivit att alla som behandlar personuppgifter i Sverige faller under *Datainspektionens* tillsyn, om inte en annan tillsynsmyndighet är utpekad. Tillsynen kan omfatta både teknisk granskning och granskning av rutiner och hantering. *Datainspektionen* uppger att myndigheten vid flera tillfällen i samband med inspektioner och skrivbordstillsyn har förordat att till exempel e-legitimationer ska användas när personuppgifter av känslig natur överförs eller när det är viktigt med en säker identifiering av avsändare eller mottagare. Myndigheten uppger dock att man inte har vidtagit några riktade aktiviteter specifikt mot e-legitimationer. Vad gäller tillsyn över e-legitimationer uppger myndigheten att man inte heller har uppfattat att man skulle ha en särskild roll inom detta område, annat än att inspektionen förordar användning av e-legitimation i vissa fall.

4.2.3 *Otydliga gränser för myndigheternas ansvar*

Det finns med andra ord flera statliga myndigheter som har ett tillsynsansvar som omfattar vissa delar eller aspekter av frågorna kring e-legitimationer, men det är oklart vem som ska göra vad och hur detta förhåller sig till övriga beskrivna aktörers ansvar när det gäller e-legitimationer specifikt. Det finns även skillnader mellan Telia Sonera och bankerna, eftersom Telia Sonera inte är föremål för tillsyn av *Finansinspektionen*.

Kammarkollegiet är den myndighet som ansvarar för ramavtalen.

Därmed utgör Kammarkollegiet den part som ska tillgodose statens krav i avtalen med leverantörerna av e-legitimationer. Kammarkollegiet är därmed ingen tillsynsmyndighet. Myndighetens uppdrag handlar snarare om att tillgodose behov i statsförvaltningen genom att samordna inköp och på så sätt åstadkomma besparingar i statens inköp av vissa varor och tjänster. En uppföljning av ett ramavtal sker normalt i slutet av ramavtalsperioden och är ofta inriktad på de ekonomiska aspekterna. Kammarkollegiet uppger dock att myndigheten inte har följt upp ramavtalen genom teknisk revision.

Myndigheternas övervakning och tillsyn skiljer sig delvis åt men överlappar också delvis varandra. Vad gäller aktörer så övervakar *Datainspektionen* och Kammarkollegiet samtliga ramavtalsleverantörer, men *Datainspektionen* har även ett ansvar att granska myndigheterna som har själva e-tjänsten. *Finansinspektionen* utövar å sin sida endast tillsyn över bankerna.

Vad gäller teknisk lösning så har *Finansinspektionen* och *Datainspektionen* tillsyn över den lösning bankerna använder för inloggning på Internetbanken. *Datainspektionen* har dessutom tillsynsansvar för den tekniska lösningen som utgör själva e-legitimationen och även Kammarkollegiet har ett ansvar att övervaka den lösningen.

Vad gäller bedömningsnorm så utgår *Datainspektionen* och *Finansinspektionen* från en författning som har som syfte att skydda ett visst bestämt

värde eller mål, medan Kammarkollegiet övervakar att den faktiska lösningen uppfyller de krav som specificerades i upphandlingsunderlaget. De författningar som Datainspektionen och Finansinspektionen granskar utifrån är olika författningar med olika syften och mål.

Sammantaget innebär detta att det finns risk för att de olika aktörerna bedömer frågor olika och att krav man ställer på de olika ramavtalsleverantörerna är olika.

4.3 Sammanfattning av iakttagelserna

Sammantaget noterar Riksrevisionen å ena sidan att inga tecken på problem för skyddet av den personliga integriteten i dagens system för e-legitimationer har kunnat identifierats inom ramen för granskningen. Å andra sidan menar Riksrevisionen att tillsynen av det nuvarande systemet inte varit tillräcklig, vilket kan medföra att tillräcklig kunskap om riskbild saknas. Vi har under granskningen gjort följande iakttagelser:

- Ingen har vad Riksrevisionen kunnat finna gjort en utförlig granskning av säkerheten i e-legitimationer.
- Vad gäller integritetsskyddet för personuppgifter kan det konstateras att det finns lagstiftning som reglerar hur hanteringen av personuppgifter ska gå till och att Datainspektionen utövar tillsyn över detta.
- Ramavtalen har inte följts upp genom teknisk revision.
- Ansvaret för tillsyn och övervakning är överlappande och det baseras på olika bedömningsgrunder.

5 Tillgänglighet och användbarhet

I detta avsnitt redogör vi för iakttagelser som rör tillgänglighet och användbarhet. Anledningen till att vi belyser dessa aspekter är att det är problematiskt från demokratisynpunkt om teknikutvecklingen och transformationen från traditionell förvaltning till e-förvaltning innebär att vissa medborgare systematiskt utesluts från viktiga samhällsfunktioner. Utgångspunkten för våra iakttagelser om tillgänglighet och användbarhet är riksdagens uttalande att *”statens roll bör vara att gynna användningen” av e-legitimationer.*

Statens institut för kommunikationsanalys (Sika) påpekar⁵⁶ att informationsteknikens snabba framväxt ger möjligheter för myndigheter, företag och organisationer att effektivisera sitt arbete. Inom exempelvis bankvärlden utträttas många bankärenden i dag via internetbank. Kunder som vill fortsätta betala räkningar via post- eller bankgiro eller direkt på banken får betala en extra avgift för detta. Enligt Sika gäller att om valet står mellan en effektiv lösning och en betydligt mer resurskrävande hantering, prioriteras ofta effektiviteten. Personer som inte har ekonomiska förutsättningar, tillräcklig kunskap eller saknar möjligheter att tillgodogöra sig den digitala informationen riskerar därmed att uteslutas.⁵⁷ I detta avseende ställs särskilt höga krav på förvaltningen i jämförelse med privata företag med tanke på att förvaltningen inte kan, och heller inte ska, välja sina kunder.

5.1 Tillgänglighet och teknisk plattform

En första aspekt på tillgänglighet är de tekniska förutsättningarna.⁵⁸ E-legitimationer är beroende av att det finns en viss typ av teknisk plattform för att de ska fungera. E-legitimationen har tidigare enligt uppgift från Finansiell ID-teknik haft problem att fungera på vissa plattformar. Problemet har avsett såväl olika fabrikat (till exempel Microsoft och Mac) som olika versioner av dessa fabrikat. Detta har gjort att grupper av medborgare inte kunnat få tillgång till e-legitimationer, trots att de så önskat och haft tillgång till dator. När upphandlingen av e-legitimationer har gjorts har utgångspunkten varit

⁵⁶ Se bl a Sikas rapport 2007:6, *Digitala klyftor – Insatser för att överbrygga dessa.*

⁵⁷ Ibid.

⁵⁸ Det bör observeras att rapporten endast behandlar tillgänglighetsfrågor som direkt berör e-legitimation. Tillgänglighet i ett vidare perspektiv, såsom möjligheten att över huvud taget använda sig av datorer eller internet, behandlas inte.

ett förfrågningsunderlag som deltagarna i upphandlingen ska besvara.⁵⁹ I förfrågningsunderlaget har den ansvariga för upphandlingen ställt olika krav i form av bör och ska. Vad gäller operativsystemplattform har det ställts krav på att komponenterna bör

- finnas i svensk version
- finnas till plattformarna Microsoft Windows ME/98, Microsoft Windows NT4/2000/XP, Mac OS och Linux.

Funktionalitet i webbläsare har formulerats så att "leverantörens produkter som behöver installeras i användares eller myndigheters datorer bör fungera med alla aktuella och använda versioner av webbläsare". Ansvariga för upphandlingen har, enligt upphandlingsunderlaget, alltså inte valt att ställa ska-krav på funktionalitet vare sig i äldre eller nyutvecklade operativsystem och webbläsare. Exakt hur väl respektive leverantörs lösning har fungerat vid olika tillfällen sedan 2001 varierar. Det har, åtminstone tidigare, förekommit problem med användningen i främst operativsystemet Linux och i Mac OS. Detta problem har uppmärksammats av leverantörerna av e-legitimationer som successivt har försökt att lösa problemet. Förbättringar sker genom att leverantörer av e-legitimationer utökar antalet fabrikat och lägger till nya versioner av befintliga sådana. Leverantörerna testar kontinuerligt kommande operativsystem av flera fabrikat i så kallade beta-versioner för att kunna ha färdiga lösningar för e-legitimationer när operativsystemen lanseras.⁶⁰

Vid en kontroll av vilken funktionalitet som leverantörernas lösningar har i dag framgår, enligt uppgift från leverantörerna själva, att olika operativsystem, hårdvara och webbläsare är kompatibla med de flesta lösningar som i dag kan tänkas användas av privatpersoner.⁶¹

Kravet på att en teknisk lösning som e-legitimation ska fungera med alla tänkbara versioner av hårdvara och mjukvara obegränsat bakåt i tiden måste ställas mot kravet på att den tekniska lösningen ska hålla en hög säkerhetsnivå. Den teknikutveckling som sker får som konsekvens att man måste öka kraven på säkerhetslösningen, vilket i sin tur ofta innebär att gammal hårdvara eller mjukvara helt enkelt inte räcker till.

⁵⁹ Förfrågningsunderlagen för Eid2004 och Eid2008 finns tillgängliga på www.avropa.se.

⁶⁰ Enligt uppgift vid intervju med företrädare för Finansiell ID-teknik.

⁶¹ Angående påstådda problem se, <http://forum.macworld.se/index.php?showtopic=51222> eller http://sv.wikinews.org/wiki/BankID_drar_in_st%C3%B6d_f%C3%B6r_GNU/Linux_-_kunder_bli_rutan_e-legitimation.

5.2 Tillgänglighet i form av rätt att få en e-legitimation

En annan aspekt på tillgänglighet handlar om möjligheten att över huvud taget få en e-legitimation. Eftersom en e-legitimation är en identitetshandling, innebär det att utfärdandet är knutet till att personen som e-legitimationen ska utfärdas till faktiskt har en identitet som är känd. Den identitet som vi använder oss av i Sverige i dag utgörs av personnumret. Det har fram till den 1 juni 2009 varit ett krav att man ska ha ett svenskt personnummer för att kunna få en e-legitimation. Det har inneburit att personer som kan ha behövt kommunicera med svenska myndigheter har varit utestängda från möjligheten att göra detta elektroniskt med hjälp av en e-legitimation.

Från och med den 1 juni 2009 har personer som saknar ett svenskt personnummer möjlighet att få ett identitetskort som innehåller en e-legitimation utfärdad. Det förutsätter dock att personen kan styrka sin identitet genom en godkänd identitetshandling eller genom en skriftlig försäkran från en intygsgivare. Personen ska också vara folkbokförd i Sverige. Denna förändring innebär att många människor som tidigare inte kunde få en e-legitimation nu har fått möjlighet till det.⁶²

Numera kan även personer med svenskt personnummer som bor utomlands få en e-legitimation. Det har tidigare varit ett problem. Anledningen har varit att utfärdaren av e-legitimation måste göra en kontroll gentemot SPAR-registret och bekräfta personens identitet innan e-legitimationen utfärdas.⁶³ Personer som inte är folkbokförda i Sverige och som saknar svenskt personnummer kan dock fortfarande inte få en e-legitimation utfärdad till sig.⁶⁴

En begränsande faktor som fortfarande kvarstår är ålder. Ingen av leverantörerna utfärdar i dag e-legitimationer till personer under 13 år.⁶⁵ Det innebär att cirka en miljon människor inte kan få en e-legitimation. Det är ett problem, men det är svårt att uppskatta hur stort behovet av e-legitimationer för denna grupp är med tanke på att de saknar rättshandlingsförmåga. Kommunerna har dock sagt sig behöva bygga skolportaler och det skulle i så fall innebära att även barn under 13 år behöver kunna få e-legitimation.

⁶² Förordningen (2009:284) om identitetskort för folkbokförda i Sverige.

⁶³ Enligt uppgifter från Finansiell ID-teknik AB kräver regelverket för bankernas ID-tjänst inte längre att kontrollen måste göras mot folkbokföringsregistret vid utfärdande. Utfärdande bank kan i stället kontrollera mot sitt kundregister att personuppgifterna stämmer, även om de inte kan uppdatera personers uppgifter i kundregistret genom slagning mot folkbokföringsregistret.

⁶⁴ Detta utgör ett problem för exempelvis styrelseledamöter i bolag som behöver kommunicera elektroniskt med Bolagsverket eller personer som av någon anledning vistas i landet endast tillfälligt. Det har riktats kritik mot att det har blivit svårare för asylsökande att få ett ID-kort utfärdad med anledning av förändringarna från 1 juni och det innebär i sin tur att de inte heller kan få en e-legitimation. Se <http://www.nt.se/norrkoping/artikel.aspx?articleid=5513212>.

⁶⁵ Detta framgår av villkoren för utfärdande av e-legitimation som finns på respektive utfärdares webbplats.

5.3 Tillgänglighet i betydelsen användbarhet

5.3.1 4 av 10 internetanvändare har e-legitimation

Enligt Finansiell ID-Teknik AB⁶⁶ använder två miljoner privatpersoner deras e-legitimation BankID. E-legitimationer ges också ut av andra aktörer men enligt uppskattningar från Finansiell ID-teknik AB står BankID för 75 procent av marknaden vilket innebär att cirka 2,6-2,7 miljoner individer i Sverige har en e-legitimation.⁶⁷ Enligt World Internet Institute's studie World Internet Project 2009 använder cirka 80 procent av alla svenskar över 18 år internet, vilket innebär cirka 5,8 miljoner⁶⁸ potentiella användare av e-legitimation i Sverige som fyllt 18 år. Det innebär vidare att andelen svenskar över 18 år som använder e-legitimation är som mest⁶⁹ cirka 40 procent av alla internetanvändare. Personer över 18 år är mest intressanta i detta sammanhang, eftersom det är dessa som i högst utsträckning interagerar med myndigheter, gör bankärenden, etc.

En jämförelse kan göras mellan antalet användare av e-legitimationer och antalet användare av banktjänster via internet. Proceduren att använda internetbank och att skaffa sig och använda e-legitimation kan liknas vid varandra i komplexitet. Antalet människor som gör banktjänster via internet är enligt en uppskattning från Svenska bankföreningen i slutet av 2007 cirka 7 miljoner individer, vilket ska sättas i relation till en befolkning på 9 miljoner. En del av dessa individer är dock kunder i mer än en bank. Tidigare konstaterade vi att cirka 2,3 miljoner individer har en e-legitimation. Det borde kunna vara fler med tanke på att det trots att det inte är enkelt att göra bankärenden via internet är en väsentligt större grupp som använder internetbank än e-legitimation.

5.3.2 Flera sätt att identifiera sig

Det har funnits olika sätt att identifiera sig för att komma åt vissa tjänster i IT-systemen långt före e-legitimationens inträde. För att få tillgång till IT-system används i dag också många andra lösningar än e-legitimation.

⁶⁶ Finansiell ID-Teknik BID AB äger, förvaltar och vidareutvecklar BankID. Företaget som startades 2002 ägs av Danske Bank, Handelsbanken, Ikano Bank, Länsförsäkringar Bank, SEB, Skandia-banken och Swedbank. Deras kunder är de flesta av de stora svenska bankerna, som i sin tur säljer och förmedlar BankID till myndigheter, företag, organisationer och privatpersoner.

⁶⁷ Vilket inte är liktydigt med att de använder den.

⁶⁸ Baserat på statistik från SCB:s befolkningsstatistikdatabas som anger att det 2009 finns ca 7 275 000 människor över 18 år i Sverige.

⁶⁹ Enligt statistik från BankID är det cirka 1% av alla som använder e-legitimation som är under 18 år.

De alternativa lösningarna för identifiering har tagits fram för att passa de tjänster och den säkerhet som hanteringen bedömts kräva. Vanligen identifierar sig användaren genom en kod för användar-id och en kod för lösenord. Säkerhetskontrollen vid utdelandet av koder görs av den utfärdande organisationen.

Ett annat sätt är att den individ som ska ges tillgång till ett IT-system redan finns i en myndighets eller ett företags register och att lösenordet därför kan skickas separat till folkbokföringsadressen. Är individen inte känd sedan tidigare kan denne ansöka om tillgång till registret via nätet eller skriftligen med underskrift. Lösenord skickas sedan till folkbokföringsadressen. Det sker till exempel när Skatteverket på deklarationsblanketten bifogar koder för sms-godkännande. I vissa fall kan både användar-id och lösenord skickas via e-post. Det gäller när uppgifterna inte är känsliga men då den verksamhetsansvarige behöver veta vem som är kopplad till ett visst ärende för att (exempelvis vid upphandlingar) kunna skicka kompletterande information. Dessa lösningar har inte lika hög säkerhet som e-legitimation, men utifrån säkerhetskraven på det enskilda systemet eller på den enskilda informationsmängden kan enklare lösningar vara tillräckliga.

5.3.3 *Brister i användbarheten*

Flera av de personer som vi har intervjuat om det svenska e-legitimations-systemet har lyft fram brister i användbarhet⁷⁰ som ett problem och en anledning till att inte fler individer skaffat sig eller använder e-legitimation.⁷¹ Att skaffa sig och använda e-legitimation kan uppfattas som krångligt. Det finns flera faktorer som talar för att brister i användbarheten är en viktig anledning till att inte fler individer har eller använder e-legitimation. Proceduren att skaffa sig en e-legitimation börjar med att man först och främst måste ha en identitet, det vill säga ett personnummer. För det andra måste man antingen vara kund i en bank eller betala 800 kronor till Telia för ett kort med e-legitimation.⁷² För det tredje måste bankkunder ta sig in på sina personliga banksidor, ofta med hjälp av koddosor eller pinkoder, och för det fjärde måste man hitta rätt domän där man kan ladda ned sin e-legitimation.

Att ladda ned mjukvara på sin hårddisk kan också kännas osäkert för många individer och hänger ihop med bristande tillit till datorer, internet etcetera. Slutligen måste bankkunder ta sig igenom nedladdningsproceduren och ange det lösenord som ska användas vid framtida identitets-

⁷⁰ Användbarhet definieras enligt ISO-normen 9241-11 som "den grad i vilken användare i ett givet sammanhang kan bruka en produkt för att uppnå specifika mål på ett ändamålsenligt, effektivt och för användaren tillfredsställande sätt".

⁷¹ Även Verva påtalade detta i sin rapport 2008:12.

⁷² Ett s.k. hårt certifikat.

kontroller. När man väl har skaffat sig en e-legitimation och laddat ned den på sin hårddisk, måste man sålunda komma ihåg lösenord, vilken typ av e-legitimation man har och vilken dator e-legitimationen finns nedladdad på. För en datorvan person är denna process kanske inte särskilt komplicerad, men för många användare kan det upplevas som krångligt och svårt att skaffa sig och använda e-legitimation.

En fjärde anledning till att så många personer använder internetbank men inte e-legitimation kan hänga samman med hur systemen lanserades. När internetbanker lanserades fick bankkunder instruktioner av bankpersonal om hur man loggade in i systemet och hur man använde tjänsterna på internetbanken. När systemet för e-legitimationer lanserades lade man från statens håll inte ned samma möda på att förklara hur människor skulle skaffa sig och använda e-legitimationer. Det gjordes heller inga stora pedagogiska insatser för att förklara vilken nytta e-legitimationer kunde göra.⁷³ Det förutsattes att medborgarna själva skulle anamma systemet för e-legitimationer. Förmodligen hoppades de statliga aktörerna som var med om att sätta systemet för e-legitimationer i Sverige på draghjälp från bankerna genom att bankerna själva skulle övergå till e-legitimation för inloggning i banksystemet. I dag har någon eller några banker övergått till e-legitimation som identifieringslösning, men det är fortfarande flertalet banker som, trots att de tillhandahåller e-legitimationer, är kvar i sina gamla system för identifiering. Att e-legitimationer inte är mer spridda och använda i Sverige kan också eventuellt förklaras med det innovationssystem som e-legitimationer utvecklats i. Enligt Vinnova är innovationssystem

”... ett begreppsligt ramverk för förståelse av innovationsprocesser. Genom att använda ett systemperspektiv beaktas alla faktorer som har betydelse såväl ekonomiska som sociala och politiska.

Central är uppfattningen att innovationer uppstår i interaktion eller samspel mellan olika aktörer. Samspelet karaktäriseras av ömsesidigt lärande, och sker till exempel mellan ett företag å ena sidan och kunder, underleverantörer, konkurrenter, universitet eller forskningsinstitut å den andra. Dessa aktörers handlande styrs av rådande spelregler, som exempelvis lagar, regler, rutiner och attityder. Systems förmåga att generera innovationer beror på hur väl samspelet mellan berörda aktörer fungerar, liksom av spelreglernas utformning.”⁷⁴

⁷³ Det finns exempel på enskilda undantag, exempelvis inrättade Försäkringskassan en helpdesk för e-legitimationer.

⁷⁴ <http://www.vinnova.se/Verksamhet/Kunskap-om-innovationssystem/Innovationssystemsanalyser/Sa-analyseras-innovationssystem/>

En analys av detta system är alltför krävande att göra här, varför vi tills vidare nöjer oss med att konstatera att den blygsamma användningen av e-legitimationer i Sverige kan härledas till olika faktorer i innovationssystemet.

5.4 Sammanfattning av iakttagelserna

Sammantaget anser Riksrevisionen att det nuvarande systemet för e-legitimationer uppvisar brister i tillgängligheten. Det är krångligt och omständligt för en brukare att skaffa sig och använda en e-legitimation. För vissa aktörer, som kommuner och landsting, har det varit kostsamt att införa lösningen. Vi konstaterar följande:

- E-legitimationer är kompatibla med de flesta operativsystem, hårdvaror och webbläsare som i dag kan tänkas användas av privatpersoner.
- Personer som inte är folkbokförda i Sverige och som saknar svenskt personnummer kan fortfarande inte få en e-legitimation.
- Ingen av leverantörerna utfärdar e-legitimationer till personer under 13 år. Det innebär att cirka en miljon människor inte kan få en e-legitimation.
- Andelen svenskar över 18 år som använder e-legitimation är som mest cirka 40 procent av alla internetanvändare.
- Det är krångligt för brukare eller användare att skaffa sig och använda dagens e-legitimation.

6 Kostnadseffektivitet och konkurrens

I detta avsnitt redogör vi för iakttagelser som rör kostnadseffektivitet och konkurrens. Utgångspunkten för våra iakttagelser i detta avsnitt är att riksdagen har uttalat att *"statens roll ska vara att stimulera konkurrens mellan utfärdare, undanröja konkurrensmässiga hinder och ... gynna kostnadseffektivitet i säkerhetslösningen"*.

6.1 Ramavtal

Statsförvaltningen och huvuddelen av kommunerna och landstingen får tillgång till tjänsten e-legitimation via ramavtal. Dessa ramavtal har tidigare upphandlats av Statskontoret och Verva. Kammarkollegiet har det nuvarande ansvaret för att förvalta ramavtalen. Genom detta förfarande har e-legitimationer kunnat tillhandahållas till ett stort antal mottagare (statliga myndigheter, kommuner etcetera) och användare (privatpersoner). Genom upphandlingarna och ökningen av transaktionsvolymerna har också kostnaderna för användningen av e-legitimation sjunkit kontinuerligt från det första ramavtalet. Nedanstående text bygger på Riksrevisionens iakttagelser och på ett yttrande från professor Mats Bergman. Yttrandet i sin helhet finns i en bilaga till denna rapport.

6.1.1 Ramavtal har flera fördelar

Ett ramavtal är en variant av upphandling som används för att tillgodose flera köparens behov av en viss vara eller tjänst.

Anledningarna till att använda ramavtal är i huvudsak två. Den första anledningen är att minska de kostnader som är förknippade med själva upphandlingen (så kallade transaktionskostnader). Genom att låta en specialiserad myndighet göra upphandlingen för förvaltningen som helhet antas kvaliteten på upphandlingen bli bättre. Varje enskild myndighet slipper dessutom göra en egen upphandling.

Den andra anledningen är att åstadkomma förmånligare inköpsvillkor genom att samla det statliga inköpet. Tanken är att en samordnad upphandling av stora kvantiteter leder till hårdare konkurrens och därmed lägre priser. Själva upphandlingen kan arrangeras på olika sätt vad gäller både hur man får fram leverantörer som får delta i upphandlingen och på vilket sätt man ordnar själva budgivningen i upphandlingen.

I en ramavtalsupphandling finns normalt två sätt att gå till väga när man väljer modell.

Det ena tillvägagångssättet är att myndigheten gör en fullständig upphandling där samtliga villkor fastställs redan i upphandlingen. De avropsberättigade myndigheterna kan därmed inte förhandla om några villkor med leverantörerna utan sluter ett avtal i enlighet med de fastställda villkoren i ramavtalet. I ramavtalet kan den ramavtalsansvariga myndigheten välja att rangordna leverantörerna. Om leverantörerna rangordnas, måste den avropande myndigheten vända sig till den högst rangordnade leverantören först. Det är bara om den leverantören inte kan leverera den önskade tjänsten som myndigheten kan vända sig till den näst högst rangordnade.

Det andra tillvägagångssättet innebär att den ramavtalsansvariga myndigheten inte fastställer samtliga villkor i ramavtalet, utan att ramavtalet endast innebär en urvalsprocess för att begränsa antalet potentiella leverantörer. När leverantörerna är fastställda i ramavtalet sker en förnyad konkurrensutsättning vid varje tillfälle en myndighet gör ett avrop från ramavtalet.

Ramavtalsupphandlingen av e-legitimationer bygger på en kombination av de två ovan beskrivna varianterna. Myndigheterna kan därmed välja att gå på de priser som är fastställda i avtalet eller att konkurrensutsätta på nytt vid avropstillfället.

Enligt professor Bergmans expertutlåtande, som presenteras i sin helhet i bilaga 1, bör den framtida metodiken för att väga samman pris och kvalitet ändras. I dag räknas pris om till kvalitetspoäng. I den framtida upphandlingslösningen bör kvalitet räknas om till pris eftersom det är svårt att på ett rimligt sätt värdera kvalitet.

6.1.2 *men konkurrensen kan bli lidande*

Den lösning för systemet för e-legitimation som tillämpas i dag är en fortsättning av den ramavtalsupphandling som gjordes av Statskontoret 2001. Statskontorets upphandling 2001 byggde i sin tur på tekniska specifikationer som upprättades av en grupp på Skatteverket kallad Samset.

I förfrågningsunderlaget till upphandlingen framgår att *"privatpersoner i Sverige enkelt och snabbt skall kunna få tillgång till en e-legitimation som går att använda för alla e-tjänster som myndigheterna erbjuder. Anbudssökande ska kunna visa på konkreta förutsättningar för att man omgående kan förse mycket stora befolkningsgrupper med e-legitimation"*. Det framgår även att anbudssökanden *"skall redan vid sista datum för anbudssökande ha ett mycket stort antal personer, omfattande breda befolkningsgrupper i Sverige, som är elektroniskt välidentifierade och som därmed redan har eller omgående kan förse med e-legitimationer i enlighet med kraven i e-nämndens vägledning nr 04:02"*.

Dessa två krav innebär att en potentiell anbudslämnare redan när anbudet lämnas måste ha både en stor redan elektroniskt välidentifierad kundkrets och en omfattande teknisk infrastruktur för att kunna utfärda och hantera e-legitimationer i stora mängder.

En konsekvens av dessa båda krav är att tre grupper av leverantörer har varit aktuella som ramavtalsleverantörer från 2001 och framåt. Det rör sig om ett antal banker inom BankID-sfären, banker som står utanför BankID och erbjuder en egen lösning samt några företag, såsom Telia och Steria. Dessa grupper av potentiella leverantörer har sedan fått lämna anbud i ramavtalsupphandlingen. Utifrån de kriterier som angavs i förfrågningsunderlaget har sedan Statskontoret beslutat vilka parter som fått teckna ramavtal.

En fördel med ramavtalsmodellen är att den innebär att transaktionskostnaderna minskar, men modellen har också väsentliga nackdelar. Det är svårt för myndigheter att bara erbjuda e-tjänster till vissa bankers kunder och detta vet givetvis de banker som kan erbjuda e-legitimation om. Om upphandlaren (staten) är pressad att köpa av alla, eller i stort sett alla budgivare, finns det små incitament att konkurrera med priset. Varje utfärdare har i det närmaste monopol på sina legitimerande parter (sina anslutna kunder) och kan därför begära ett högt pris.⁷⁵

En ytterligare nackdel med ramavtalsupphandlingar är att den osäkerhet som råder om inköpsvolym riskerar att höja prisnivån. Säljaren ger köparen en option att köpa till visst pris och måste därmed hålla kapacitet i beredskap, kapacitet som kanske inte kommer att utnyttjas. Säljaren måste kompenseras för detta, vilket i allmänhet höjer prisnivån. Om denna effekt är stark nog att motverka övriga besparingseffekter beror självfallet på omständigheterna.⁷⁶

Om, å andra sidan, upphandlaren försöker skapa en verklig konkurrenssituation, innebär detta att man måste vara villig att riskera att utestänga stora grupper av legitimerande parter – om den aktuella utfärdaren begär ett alltför högt pris. Situationen liknar i viss mån det termineringsmonopol som varje teleoperatör anses ha, hur liten marknadsandel operatören än har. Monopolet innebär att endast den operatör hos vilken en viss kund köper teletjänster kan koppla samtal till just den kunden, det vill säga terminera samtal till den aktuella kunden. På telemarknaden har detta motiverat att termineringstjänster är prisreglerade också för mycket små aktörer.⁷⁷

Med andra ord är upphandling, i form av ramavtal eller på annat sätt, inte en lämplig modell när köparen avser att köpa av alla eller så gott som alla budgivare. När budgivarna vet att alla kommer att få sälja, i det närmaste oavsett prisnivån och oavsett om deras bud är högst eller lägst, så

⁷⁵ Stycket är i sin helhet hämtat från Mats Bergmans yttrande i bilaga 1.

⁷⁶ Ibid.

⁷⁷ Ibid.

försvinner incitamenten att konkurrera med priset. Marknader med dessa egenskaper brukar prisregleras – eller så sköts uppgifterna av den offentliga sektorn själv.⁷⁸

De banker som ingår i sammanslutningen BankID har alla haft möjlighet att lämna ett eget anbud där banken kan utfärda e-legitimation för samtliga kunder i de banker som ingår i sammanslutningen. Själva utfärdandet av e-legitimationen sköts av respektive bank inom sammanslutningen. Den banken får sedan ersättning för kostnaden av den bank inom sammanslutningen som har utsetts till ramavtalsleverantör. Samtliga betalningar från de myndigheter som tecknar ett avropsavtal tillfaller den bank inom sammanslutningen som är ramavtalspart. Vilka villkor som gäller inom sammanslutningen BankID vad gäller kostnadstäckning är inte känt för Riksrevisionen.

De övriga två grupperna består som nämnts av banker utanför BankID och av några andra företag. Eftersom samtliga ramavtalsleverantörer endast kan erbjuda e-legitimation till sina egna kunder, krävs det att en privatperson antingen byter bank eller vänder sig till något av de utvalda företag som inte är banker för att de olika kundstockarna ska konkurrensutsättas .

Den svenska bankmarknaden har enligt flera undersökningar av Konkurrensverket en struktur som kan liknas vid ett oligopol, och kundörligheten mellan banker är låg.⁷⁹ Detta innebär förmodligen att sannolikheten är låg för att en privatperson skulle byta bank eller skaffa ytterligare en bank för att få en annan e-legitimation. Det finns, utöver bankerna, Telia som tillhandahåller e-legitimationer och en person kan vända sig till detta företag för att få en e-legitimation utfärdad. Telia tar dock ut en avgift för att utfärda e-legitimationer, jämfört med bankerna där själva utfärdandet av e-legitimation är kostnadsfritt i det fall personen är kund i banken. En privatperson som är kund i en bank har redan tillgång till en e-legitimation utan att det kostar extra, och sannolikheten att personen skulle vända sig till ett annat företag och betala för tjänsten är därmed låg.⁸⁰ Vad gäller e-legitimation kan konstateras att konkurrenterna inte är jämnstarka med tanke på att BankID har en marknadsandel på uppskattningsvis 75 procent och produkterna är differentierade eftersom en identifierad kundstock innefattas i produkten. Eftersom rörligheten mellan kundstockarna är låg och tanken bakom modellen är att leverantören säljer sin kundstock, är konkurrensen mellan företagen begränsad.

Den delen av marknaden där det finns utrymme för faktisk konkurrens är mellan de banker som ingår i BankID, eftersom de konkurrerar om hela den totala kundstocken. Det är dock svårt att avgöra hur stor den konkurrensen är, eftersom vi inte vet hur affärsuppgörelserna mellan dessa banker ser ut.

⁷⁸ Ibid.

⁷⁹ Konkurrensverket – *Åtgärder för bättre konkurrens*.

⁸⁰ En förutsättning för att man ska kunna dra denna slutsats är givetvis att kunden uppfattar kvaliteten på de två tjänsterna som någorlunda likvärdig.

Huruvida detta är en fungerande konkurrens eller inte är helt avhängigt den avtalskonstruktion som bygger upp BankID och de beslut som finns om ersättningar från avtalslutande bank till den faktiska utfärdaren. Den ersättning mellan bankerna inom BankID som beslutats om lägger ett golv för det pris som den avtalslutande banken kan erbjuda gentemot den statliga ramavtalsparten.

Det är också så att alla banker som ingår i sammanslutningen har möjlighet att erbjuda lösningen till sina kunder och att kostnaden för denna tjänst ersätts av den bank som är ramavtalsleverantör. Vinstmarginalen för den bank som blir leverantör avgör förmodligen hur stora incitament bankerna har att konkurrera om att bli ramavtalsleverantör. Om det rör sig om en liten marginal, kan en effekt bli att bankerna nöjer sig med att kunna erbjuda tjänsten till sina kunder till ingen eller åtminstone subventionerad kostnad och att intresset för att konkurrera i budgivningen därmed är lågt.

6.1.3 *Oklart om transaktionskostnaderna minskar*

En av huvudorsakerna till att använda ramavtal är möjligheten att minska de totala transaktionskostnaderna, det vill säga i det här fallet samtliga kostnader förknippade med statsförvaltningens köp av e-legitimationer. Genom att man samlar inköpen för samtliga myndigheter till en enda upphandling undviker man att alla myndigheter gör egna upphandlingar av samma sorts tjänst, var för sig eller möjligen i mindre grupper. Det antas i sin tur innebära att den totala kostnaden för statsförvaltningen som är förknippad med att köpa en lösning för e-legitimationer blir lägre än om en samlad upphandling inte hade gjorts.

De upphandlingar som har gjorts av e-legitimation innebär dock att varje myndighet eller kommun som har tänkt använda e-legitimation som identifieringsteknik i en e-tjänst måste teckna avtal med samtliga leverantörer i ramavtalet för att kunna erbjuda tjänster till alla medborgare.

Avropet kan i sin tur göras på så sätt att myndigheten endast tecknar ett avtal med de villkor som framgår av ramavtalet eller att myndigheten gör en förnyad konkurrensutsättning. Utöver detta krävs också att myndigheten köper programvara och hårdvara för att kunna integrera e-legitimationerna i sina egna system och tjänster. Normalt innebär det att myndigheten måste göra ytterligare ett avrop från ett ramavtal kallat Infratjänst, där myndigheten kan få hjälp med det gränssnitt som krävs för integration mellan myndighetens egna system och e-legitimationen. Själva hanteringen för varje enskild myndighet är därför ganska komplicerad och omfattande, trots att tanken med ramavtal är att förenkla administrationen.

6.2 Kostnader för ett statligt alternativ är oklara

Det har riktats kritik mot den lösning med en marknadsmodell som regeringen valt för e-legitimationer.⁸¹ Kritiken är mångfasetterad och har olika utgångspunkter. Den har handlat om att möjligheten till en statligt styr nationellt sammanhållen lösning inte tagits till vara. Det har också framförts att nuvarande lösning är dyrare än alternativen. Gemensamt är emellertid att ingen har presenterat ett tydligt alternativ och än mindre kostnader och konsekvensbeskrivningar.⁸²

Som ett hypotetiskt exempel kan vi föreställa oss ett helt statligt alternativ. Ett sådant skulle ha inneburit att hela utvecklings- och hanteringskostnaden för e-legitimation legat på staten. Kostnaden kan enligt uppgift från personer som tidigare arbetat på Verva och Statskontoret uppskattas till minst 200 miljoner kronor. Finansiell ID-teknik har uppgivit att en grov uppskattning av investeringarna hittills i deras system är drygt 400 miljoner kronor.

Totalt har staten, kommunerna och landstingen under perioden 2001–2009 (2009 fram till och med andra kvartalet) betalat drygt 111 miljoner kronor till de privata utfärdarna av e-legitimationer. Betalningarna avser kontrollfrågor om personers identitet vid elektroniska ärenden. Kostnaden för enbart statliga aktörer uppgår till 91 miljoner kronor. Denna siffra kan tolkas som ett mått på statens kostnader för systemet för e-legitimationer. I de 91 miljoner kronorna ryms inte kostnader för att integrera systemet för e-legitimationer i myndigheternas IT-system. Där ryms inte heller drift och förvaltning av systemet för e-legitimationer eller kostnader för upphandling, skrivande av ramavtal eller myndigheternas tecknande av kontrakt med enskilda leverantörer.

Det är svårt att jämföra siffror mellan olika länder, men man kan ändå nämna det finska systemet för e-legitimationer, som kostat den finska offentliga förvaltningen 40 miljoner euro i utvecklings- och driftskostnader under perioden 1999 till 2007 enligt finska Revisionsverket. Några djupare jämförelser går dock inte att göra, bland annat eftersom de svenska siffrorna inte innehåller myndigheternas kostnader för utveckling och drift.

Det troliga är att staten har haft lägre kostnader för nuvarande lösning än vad den skulle ha haft med ett rent statligt alternativ. Vid en jämförelse bör man även beakta att staten fick tillgång till bankernas alla kunder och att de erbjöds e-legitimation utan kostnad.⁸³

⁸¹ Kritiken har framförts vid en intervju med företrädare för Sveriges Kommuner och Landsting.

⁸² Bland annat Sveriges Kommuner och Landsting har framfört denna kritik. Den framkommer även tydligt ur remissammanställningen som gjorts med anledning av Vervas rapport 2008:12.

⁸³ Vid en jämförelse av alternativen bör det även nämnas att om staten hade varit tvungen att göra en ursprungsidentifiering av alla användare, skulle kostnaderna bli ännu högre. Om man räknar med en kostnad av ungefär 300 kronor per identifiering och 2,5 miljoner användare, blir det en merkostnad på 750 miljoner.

En rent statlig lösning innehåller dessutom ytterligare ett riskmoment. Om staten bygger upp en egen lösning finns risken att denna inte i tillräcklig grad tar hänsyn till de behov näringslivet och bankerna har för den egna verksamheten. Om så blir fallet kan dessa komma att utveckla egna lösningar. Skulle ett sådant scenario bli verklighet riskerar den statliga lösningen att tappa kunder och därmed även att äventyra utvecklingen av e-förvaltningen. Ett liknande scenario har inträffat i Finland, där det finns flera statliga lösningar parallellt med en som utvecklats av banksektorn.

6.3 Sammanfattning av iakttagelserna

Sammantaget konstaterar Riksrevisionen att dagens system för e-legitimationer inte har skapat en bra konkurrenssituation på marknaden för e-legitimationer. Vad gäller kravet på kostnadseffektivitet har vi gjort följande iakttagelser:

- Om upphandlaren (staten) är pressad att köpa av alla, eller i stort sett alla, budgivare finns det små incitament att konkurrera med priset. Varje utfärdare har i det närmaste monopol på sina anslutna kunder och kan därför begära ett högt pris.
- Eftersom samtliga ramavtalsleverantörer endast kan erbjuda e-legitimation till sina egna kunder, krävs det att en privatperson antingen byter bank eller vänder sig till något av de företag som inte är banker för att kundstockarna ska konkurrensutsättas.
- Själva hanteringen för avrop för varje enskild myndighet är komplicerad och omfattande, trots att tanken med ramavtal är att förenkla administrationen.
- De finns ingen beräkning av kostnaderna för en statlig lösning som alternativ till dagens system, men vid en försiktig jämförelse med den finska lösningen verkar den svenska lösningen ha inneburit lägre kostnader.

7 Teknik och teknikneutralitet

I det här avsnittet beskrivs iakttagelser som rör teknik och teknikneutralitet. Att vi valt att belysa frågor som rör detta ämne har sin förklaring i riksdagens uttalande att *staten ska verka för att det etableras teknikneutrala standarder för elektroniska signaturer och därigenom säkra en dynamisk utveckling av informationssamhällets säkerhetslösningar.*

7.1 Myndigheternas förmåga att samverka

7.1.1 *Interoperabilitet = förmågan att samarbeta*

En väl fungerande e-förvaltning bygger i hög grad på samverkansförmåga, eller med andra ord interoperabilitet, mellan bland annat statliga myndigheter och kommuner. Med interoperabilitet avses förmågan hos ett system eller en komponent att fungera ihop med andra system eller komponenter utan särskilda åtgärder. I ett första skede erbjuds medborgarna avgränsade e-tjänster hos en aktör. I en senare utvecklingsfas förväntas enskilda myndigheter hämta uppgifter från andra myndigheters register eller informationsmängder utan att den enskilde behöver ägna detta en tanke. En väl utvecklad e-förvaltning innebär bland annat att myndigheter och kommuner samverkar och delar information.

7.1.2 *Informationsutbyte mellan myndigheter allt viktigare*

Den svenska förvaltningsmodellen ger varje myndighet och kommun ansvaret för att utveckla och utföra sin verksamhet. Det gör att modellen i sig inte är skapad för samverkan. Syftet med interoperabilitet är emellertid att öka möjligheten för myndigheter att kommunicera med varandra samt att utveckla och tillhandahålla tjänster som sträcker sig över flera verksamhetsområden utan att det kräver stora ingrepp i befintliga system eller IT-plattformar.

Det finns redan i dag ett utbrett informationsutbyte på elektronisk väg inom förvaltningen. Sådant utbyte sker mellan de centrala dataregister som byggts upp under lång tid och har utvecklats successivt och utan plane-

rad samordning.⁸⁴ Registren regleras i ett flertal olika registerförfattningar. Informationsutbytet mellan registren har skapats när behov uppstått och registerhållande myndigheter har kommit överens om det. Utbytet har hittills fyllt sin funktion, även om det varit kostnadskrävande att både utveckla och underhålla. Med ökade krav på effektiviseringar i statlig förvaltning och med de möjligheter IT erbjuder har informationsutbyte mellan myndigheter blivit allt viktigare. Utvecklingen har dock hittills inte varit tillräckligt gynnsam utan nya lösningar måste till.

Regeringen har i sin handlingsplan för eFörvaltningen framhållit:

”...med de tekniska lösningar som nu finns tillgängliga kan Sverige använda en decentraliserad samverkansmodell – ibland kallad en federativ eller tjänstebaserad IT-arkitektur. En sådan modell bygger på att myndigheternas datorsystem kommunicerar med varandra på ett standardiserat sätt utan att vara fast kopplade till varandra. En sådan modell tillåter å ena sidan en snabbare och mer dynamisk utveckling av e-förvaltningen, å andra sidan kräver den en högre grad av IT-standardisering”.

7.1.3 Stora förändringar krävs

För att åstadkomma en smidigare samverkan är det nödvändigt med stora förändringar i hela informationsutbytesstrukturen inom offentlig förvaltning och då avses inte enbart den tekniska nivån. Förändringar och anpassningar måste ske även på högre så kallade logiska nivåer, som semantisk, organisatorisk och rättslig nivå. Regeringen har också i direktiven till E-delegationen för den kommande strategin för e-förvaltning poängterat vikten av samverkan och teknisk interoperabilitet mellan systemen.

För att en användare vid en inloggning ska tillåtas få tillgång till olika informationsmängder, kanske hos skilda organisationer, krävs en säker identifiering. Olika statliga myndigheter har skapat flera gränssnitt och identifieringslösningar, vilket skapar problem för till exempel kommuner som ska samverka med många myndigheter. Å andra sidan ska varje tillhandahållare av e-tjänster kunna erbjuda lösningar för samtliga varianter av e-legitimationer i ramavtalet. Det gör att ingen blir utestängd rent tekniskt, men det kan få hanterings- och kostnadsmässiga konsekvenser.

Problem kvarstår och riskerar därmed att vara en hämsko på kommunernas vilja att skapa e-tjänster och utveckla sin verksamhet mot e-förvaltning. Myndigheterna kan dock motverka detta genom att samarbeta för att om möjligt finna lösningar för att minska detta problem för kommunerna. Det finns följaktligen betydande tekniska och användarmässiga uppgifter att lösa

⁸⁴ Spridnings- och hämningssystemet (SHS) är ett exempel på ett system som utvecklats för att aktörer i offentlig sektor ska kunna utbyta information.

bland annat mellan myndigheter och mellan kommuner och myndigheter när det gäller att skapa en sammanhållen e-förvaltning.

I fråga om e-legitimationer är problemen med interoperabilitet knutna till de gränssnitt som har skapats för att själva certifikatet i e-legitimationen ska kunna kopplas samman med e-tjänsten hos myndigheten eller kommunen. Det har inte fastställts några standarder för detta gränssnitt. Eftersom de olika utfärdarna använder sig av olika gränssnitt måste tjänsteleverantören skapa flera olika lösningar för att kunna integrera de olika utfärdarnas e-legitimationer i sin tjänst. Med anledning av detta upphandlade Statskontoret ett ramavtal kallat Infratjänst. Ramavtalet innebär i korthet att ett företag hanterar de olika gränssnitten från utfärdarna och skapar en väg in i myndighetens e-tjänst. Myndigheten behöver därmed inte själv utveckla olika lösningar för samtliga leverantörer.

7.2 Organisationslegitimationer

7.2.1 *Också företrädaren bör kunna identifieras*

Den form av e-legitimation som hittills har berörts i rapporten är e-legitimation för en fysisk person för privat bruk. En fysisk person kan dock agera i flera olika roller, både som privatperson och som företrädare för någon annan fysisk person, ett företag eller organisation.

När man agerar som privatperson är det tillräckligt att motparten kan fastställa identiteten. När en fysisk person agerar som ombud eller representant för någon annan är det oftast inte tillräckligt att endast fastställa den fysiska personens identitet. Man måste också på något sätt identifiera förhållandet mellan den fysiska personen och det objekt som den fysiska personen säger sig företräda.

Eftersom en organisation, en myndighet eller ett företag inte kan utföra rättshandlingar på egen hand krävs det att en fysisk person företräder organisationen. De två grundläggande aktiviteter som kräver en företrädare är dels att företa någon form av handling som innebär ett offentligt maktutövande gentemot en person, en organisation eller ett företag, dels att företa en rättshandling av något slag som binder den man representerar juridiskt till en tredje man.⁸⁵

Man kan till dessa två grundläggande syften även lägga de rent praktiska aspekterna av att kunna identifiera någon för att han eller hon ska ha rätt att ta del av information eller för att i efterhand kunna bevisa vem som har gjort vad.

⁸⁵ Inom juridiken har detta främst tagit sig uttryck i den s. k. fullmaktsläran som är ett klassiskt område inom förmögenhetsrätten. I myndighetsvärlden återfinns frågan om ställföreträdarskap exempelvis i en myndighets instruktion, myndighetsförordningen och en myndighets arbetsordning.

I den digitala världen, precis som i den fysiska, behöver en fysisk person ibland kunna företräda någon annan. I informationsutbytet mellan myndigheter eller mellan företag har man länge använt olika lösningar i form av stämpelcertifikat eller servercertifikat för att garantera att informationen härrör från en viss specifik myndighet eller ett visst företag.⁸⁶ Ytterligare en variant är att man skapar en elektroniskt säker kommunikation från system till system.⁸⁷ Nackdelen med de beskrivna lösningarna är att de identifierar organisationen eller företagets men inte den fysiska personen. För detta krävs det en elektronisk lösning som identifierar både organisationen och personen, det vill säga en sorts e-tjänstelegitimation.⁸⁸

I en e-tjänstelegitimation kan det också behövas uppgifter om personens roll i organisationen och därmed tillhörande behörighet. Frågan om roller och behörighet kan antingen lösas genom att sådan information inkluderas i själva legitimationen, att den förlitande parten har en behörighetslista där enskilda personers eller rollers behörighet framgår eller att man skapar en behörighetskatalog som den förlitande parten kan kontrollera emot.⁸⁹

I dag finns ingen sådan lösning som kan användas inom eller gentemot den statliga förvaltningen. Det gör det däremot i den kommunala sektorn och vårdsektorn.

7.2.2 *Behovet av en e-tjänstelegitimation känt sedan länge*

Behovet av en e-tjänstelegitimation påpekades av Statskontoret redan år 2000. Men trots att det sedan dess har skett tre upphandlingar av den privata e-legitimationen, har det fortfarande inte tagits fram en lösning för e-tjänstelegitimation.⁹⁰ Avsaknaden av en e-tjänstelegitimation har inneburit att det förekommer att anställda tvingats använda sina privata e-legitimationer både inom förvaltningen och i privata företag. Med anledning av

⁸⁶ Ett stämpelcertifikat är en elektronisk stämpel som låser en viss informationsmängd till en myndighet eller ett företag. Genom att använda ett stämpelcertifikat garanterar man att den här informationen kommer från innehavaren av certifikatet. Ett servercertifikat garanterar identiteten på en specifik server, och när en webbläsare eller en annan server kommunicerar med servern så kontrolleras identiteten.

⁸⁷ Exempel på sådana system är SGSI (Swedish Government Secure Intranet) eller SHS (Spridnings- och hämtningssystemet)

⁸⁸ Det förekommer olika termer för att beteckna en sådan lösning. De två mest använda termerna är organisationslegitimation eller e-tjänstelegitimation.

⁸⁹ Den nationella lösningen för vårdsektorn använder sig av vad som kallas SITHS och HSA som kan sägas vara en e-tjänstelegitimationslösning med central behörighetskatalog. SITHS är en e-tjänstelegitimation som placerats på ett ID-kort. HSA är en standardiserad katalog för att hantera personal- och verksamhetsinformation inom vård och omsorg som innebär central lagring av aktuella uppgifter kring organisationer, enheter, funktioner och individer samt distribution av information mellan olika system.

⁹⁰ Statskontoret, *Elektroniska signaturer och elektronisk identifiering för myndigheters e-tjänster*, 2004:40, s. 23 ff.

detta har det framkommit kritik mot att det finns en förväxlingsrisk mellan personligt ansvar och tjänsteansvar. Det finns också en oro över att behöva exponera sin identitet i transaktioner med motparter utanför den egna arbetsgivaren. Kritikerna understryker dessutom att e-legitimationen är privat egendom.⁹¹

Verva uppmärksammade under våren 2008 genom en enkätundersökning ett behov av e-tjänstelegitimationer ute i förvaltningarna. Med anledning av detta beslutade man att inleda en förstudie som togs över av Kammarkollegiet när Verva lades ned.⁹² Kammarkollegiet publicerade förstudien den 29 maj 2009. Ärendet bereds för närvarande, och enligt uppgift från Kammarkollegiet kan en ramavtalsupphandling tidigast påbörjas under hösten 2009.

7.3 Sammanfattning av iakttagelserna

Riksrevisionen konstaterar att dagens system för e-legitimationer inte är ett interoperabelt system, främst på grund av att gränssnitten inte är standardiserade. Dessa problem har lett till högre kostnader för bland andra de offentliga aktörerna i systemet. Vad gäller kravet på teknik och teknikneutralitet har vi gjort följande iakttagelser:

- Problemen med interoperabilitet hos e-legitimationer beror på att tjänsteleverantören och utfärdaren oftast använder olika gränssnitt.
- Det finns i dag inget system för organisationslegitimationer, men det finns flera myndigheter som skulle behöva ett sådant. Ett relativt stort antal tjänster är i bruk redan i dag, där man använder sig av myndighets-specifikt utvecklade lösningar och där en e-tjänstelegitimation skulle underlätta hanteringen.

⁹¹ Kammarkollegiet, *Organisationslegitimering*, FS:2009-4, s. 16 f.

⁹² Ibid. s. 14.

8 Analys, slutsatser och rekommendationer

I detta kapitel redovisas de bedömningar som Riksrevisionen gjort utifrån de iakttagelser som presenterats i föregående kapitel. Bedömningarna baseras på de normer som redogjorts för i kapitel 1. Kapitlet och rapportern avslutas med Riksrevisionens rekommendationer.

8.1 Sammanfattande bedömning

I rapportens inledande kapitel fastslogs att Riksrevisionens granskning ska besvara följande tudelade fråga:

- a) *Är systemet för e-legitimation rättssäkert, tillgängligt, kostnadseffektivt och teknikneutralt?*
- b) *Har regeringen och ansvariga myndigheter agerat i enlighet med riksdagens intentioner med avseende på utvecklandet av systemet för e-legitimationer?*

Granskningen belyser sålunda hanteringen av e-legitimationer ur två perspektiv – systemperspektivet och aktörsperspektivet.

Riksrevisionens bedömning av revisionsfrågans första del (a) är att *systemet* för e-legitimation till stora delar uppfyller de krav på rättssäkerhet, tillgänglighet, kostnadseffektivitet och teknikneutralitet som riksdagen har uttalat.

Riksrevisionens bedömning av revisionsfrågans andra del (b) är att *aktörerna*, det vill säga regeringen och ansvariga myndigheter, inte fullt ut har agerat i enlighet med riksdagens intentioner med avseende på utvecklandet av systemet för e-legitimationer.

Den sammanlagda bilden är att systemet för e-legitimationer i sig har haft en positiv effekt på utvecklingen av e-förvaltningen, särskilt för myndigheter som Skatteverket och Försäkringskassan. Detta kan låta som en motsägelse, men bedömningen ska ses mot bakgrund av att Sverige trots allt har ett tämligen väl fungerande system för e-legitimationer som till stora delar främjat utvecklingen av e-förvaltningen. Det finns dock vissa förbättringsområden i e-legitimationssystemet om man ser till rättssäkerheten, tillgängligheten, kostnadseffektiviteten och teknikneutraliteten. Ur ett aktörsperspektiv hade

regeringen och ansvariga myndigheter också kunnat göra mer än vad de faktiskt har gjort. Framför allt hade regeringen kunnat vara tydligare i sin styrning av myndigheterna.

Riksrevisionen kan dock notera att E-delegationen, på uppdrag av regeringen, har presenterat ett antal förslag för att komma till rätta med flera av de brister som redovisas i granskningen. Detta kan ge regeringen och myndigheterna bättre förutsättningar för att få till den styrning och uppföljning som krävs för att tillgodose riksdagens krav när det gäller att nå ökad rättssäkerhet, användbarhet, kostnadseffektivitet och teknikneutralitet.

Nedan redogör vi för den analys som gjorts utifrån revisionsfrågans två perspektiv, dels systemperspektivet, dels aktörsperspektivet.

8.2 Är systemet för e-legitimationer rättssäkert?

Riksrevisionen har inte funnit att rättssäkerheten och myndigheternas möjlighet att fungera har försämrats. Det finns snarare indikationer på att myndigheternas möjlighet att fungera har förbättrats genom tillgång till tjänster via e-legitimation. En ökad användning av e-legitimationer skulle även ytterligare öka individernas rättssäkerhet med tanke på den höga tekniska säkerhetsnivå som uppnås med hjälp av en e-legitimation.

De problem som rör integritet handlar främst om den principiella frågan om privata aktörer ska hantera integritetskänslig information eller om det enbart ska vara en offentlig angelägenhet. Det nuvarande systemet för e-legitimationer har bland annat inneburit att privatpersoners personuppgifter spridits till olika register och lagrats där. Riksrevisionen har inte funnit att detta skulle vara ett stort problem i dag. Ett ökat användande av e-legitimationer skulle expandera det totala skyddet för den personliga integriteten i samhället med tanke på att säkerheten i lösningen är hög. Att använda e-legitimation ger alltså ett bättre personligt skydd än att inte använda e-legitimation.

Tillsynen av ett system är viktig för att dels upptäcka fel och brister i systemet, dels förebygga problem. Riksrevisionen har kunnat konstatera att tillsyn av själva systemet för e-legitimationer inte har förekommit. Ansvaret för tillsyn är dessutom splittrat på tre aktörer. Av de iakttagelser som har gjorts framgår att e-legitimationen anses vara en säker lösning, och det kan givetvis vara en bidragande orsak till att ingen myndighet har granskat systemet. Kammarkollegiet, den myndighet som har ett särskilt ansvar för uppföljning av ramavtalen, har inte följt upp ramavtalen genom teknisk revision. Användningen av e-legitimationer förväntas öka och användningen i sig medför att stora mängder personuppgifter lagras hos leverantörerna. Riksrevisionen anser därför att tillsynsansvaret behöver preciseras för att nå upp till de krav som riksdagen har satt upp för skyddet av den personliga integriteten.

8.3 Är systemet för e-legitimationer tillgängligt?

Riksrevisionen bedömer att systemet för e-legitimationer inte kan anses uppfylla kraven på tillgänglighet och användbarhet fullt ut. Det faktum att e-legitimationer är tekniskt komplicerade och att gränssnittet upplevs som svårhanterligt från användarsynpunkt är konsekvenser av valet av teknisk lösning. Utgångspunkten har varit ett produktionsperspektiv och inte ett användarperspektiv vid utvecklingen av systemet för e-legitimationer. Detta har resulterat i att det blivit onödigt krångligt för användaren att hantera lösningen. För att skaffa sig en e-legitimation behöver användaren ta sig igenom en process som består av flera steg. Processen har sett olika ut beroende på vilken bank användaren av e-legitimationer varit kund i. När användaren väl skaffat sig en e-legitimation har han eller hon varit tvungen att komma ihåg vilken typ av e-legitimation det handlar om, vilken pinkod han eller hon har och på vilken dator e-legitimationen är nedladdad. Om användaren tycker att tekniken är för krånglig innebär det minskad användning, och det kan i sin tur påverka kostnadseffektiviteten och utvecklingen av e-tjänster. Med tanke på att det är långt fler individer som gör bankärenden via internet än som använder e-legitimation, finns det en stor potential att utveckla användandet av internet och elektroniska tjänster i Sverige.

Det finns en rad lärdomar att dra inför lanseringen av nästa generations e-legitimation. Systemet bör i ökad utsträckning utgå från användarens behov och kunskaper. Användaren måste kunna se och förstå nyttan med att skaffa en e-legitimation. Aktiva insatser måste göras för att marknadsföra e-legitimationen, och pedagogiska insatser måste till för att förklara värdet för individen av att använda sig av en e-legitimation. Regeringens uppgift för att gynna användningen av e-legitimationer har varit att skapa förutsättningar för myndigheter, kommuner och landsting att kunna använda sig av lösningen i ökad utsträckning.

Enligt vad som framgår av avsnitt 3 gav regeringen Statskontoret och sedan Verva i uppdrag att främja användningen av e-legitimationer. Regeringen har även vidtagit vissa ytterligare åtgärder som exempelvis finansieringsprogrammet för e-legitimationer.

Regeringen har dock inte varit tillräckligt tydlig i styrningen av övergången till en e-förvaltning. Den svaga styrningen av myndigheterna har resulterat i att myndigheterna inte har prioriterat utvecklingen av e-tjänster. Bristen på e-tjänster har vidare inneburit att det saknats incitament för medborgarna att skaffa sig e-legitimationer. Detta innebär i sin tur att övergången från traditionell förvaltning till e-förvaltning inte utvecklas i tillräcklig snabb takt.

Ansvariga myndigheter har vidtagit vissa åtgärder och även påtalat behov av ytterligare åtgärder från regeringens sida. Riksrevisionen anser dock att myndigheterna kunde ha gjort mer för att marknadsföra e-legitimation och e-tjänster i syfte att öka användningen.

8.4 Är systemet för e-legitimationer kostnadseffektivt?

Riksrevisionen bedömer att när det gäller kostnadseffektiviteten så uppfyller systemet i stora delar kraven från riksdagen. Vad gäller riksdagens uttalande om att staten ska undanröja konkurrensmässiga hinder och stimulera konkurrens kan lösningen inte anses uppfylla kraven enligt våra bedömningsgrunder. En marknad som innehåller konkurrensmässiga hinder får i sin tur negativa konsekvenser för kostnadseffektiviteten.

Den lösning som staten har valt i form av ramavtal har inneburit en begränsad konkurrenssituation som kan ha fått negativa konsekvenser både vad gäller prissättning och tekniska utvecklingsmöjligheter för den befintliga lösningen. Den analys som utförts av professor Mats Bergman tillsammans med de iakttagelser som Riksrevisionen gjort tyder på att systemet borde ha utformats på ett delvis annorlunda sätt för att främja konkurrensen och sänka transaktionskostnaderna.

Det bör dock framhållas att ett huvudsyfte med att välja den privata lösningen var att bruka en befintlig och väl fungerande lösning för att snabbt få igång e-tjänster. Om staten hade utvecklat en egen lösning hade det för det första inneburit en längre startsträcka och för det andra att den statliga lösningen skulle konkurrera med de privata lösningar som erbjöds av bland andra bankerna. Vid en försiktig jämförelse med Finland där man valt en statligt utvecklad lösning verkar kostnaderna för det svenska systemet ha varit lägre. Detta ger en fingervisning om de risker som föreligger vid egenutveckling av komplexa system.

Regeringen får i stort anses ha gynnat kostnadseffektiviteten i säkerhetslösningen. Regeringen beslutade att ansvariga myndigheter skulle upphandla en lösning från den privata marknaden istället för att utveckla en lösning i statens regi. Vid en jämförelse mellan den finska och den svenska lösningen framstår regeringens ställningstagande ha inneburit lägre kostnader än alternativen. Skatteverkets och Försäkringskassans användning av e-legitimationstjänster har inneburit en mer kostnadseffektiv hantering jämfört med manuell hantering för dessa myndigheter. Riksrevisionen anser dock att om regeringen genom tydligare styrning hade främjat utvecklingen av fler e-tjänster som använder sig av e-legitimationslösning skulle kostnadseffektiviteten öka inte bara hos dessa två myndigheter utan i hela statsförvaltningen.

Myndigheterna får, precis som regeringen, anses ha gynnat kostnadseffektiviteten på en övergripande nivå. Flera myndigheter har dessutom påtalat vilka problem som finns angående styrning, finansiering av e-tjänster och val av lösning för e-legitimationer.

8.5 Har regeringen främjat konkurrens?

När det gäller konkurrensaspekten bedömer Riksrevisionen att valet av ramavtalsupphandling och önskemålet om utfärdare med en avtalsrelation med en betydande andel av befolkningen har medfört att priskonkurrensen inte har fungerat väl. Regeringen ville inte finansiera utvecklingen av en svensk e-legitimation och ålade därmed ansvariga myndigheter att välja en befintlig lösning på den privata marknaden. Valet att upphandla en befintlig lösning motiverades bland annat utifrån den risk som var förenad med att staten skulle utveckla en teknisk lösning. I jämförelse med andra länders val av elektronisk identifiering har den svenska modellen dessutom med största sannolikhet varit ett kostnadseffektivare alternativ. Genom att välja banklösningen skapade man dock ett system där den tekniska lösningen inte byggde på öppna standarder utan kunderna var "inlåsta" till sina respektive banker och kundernas rörlighet mellan olika alternativ var därmed ytterst begränsad. Systemet har också höga inträdesbarriärer för potentiella leverantörer.

Regeringens beslut att inte bygga en statligt utvecklad lösning utan i stället upphandla den nuvarande lösningen av privata aktörer har inneburit en inlåsnings effekt på systemet för e-legitimation. Ansvariga myndigheter har därmed haft små möjligheter att stimulera konkurrens och man kan svårigen kritisera deras passiva agerande.

8.6 Är systemet för e-legitimationer teknikneutralt?

Riksrevisionen bedömer att när det gäller kravet på teknikneutralitet kan systemet för e-legitimationer inte anses uppfylla riksdagens krav. Regeringen kan inte heller anses ha främjat att det etableras teknikneutrala standarder för elektroniska signaturer eller ha säkrat en dynamisk utveckling av informationssamhällets säkerhetslösningar.

Avsaknaden av en e-tjänstelegitimation innebär effektivitetsbrister då myndigheterna får använda sig av alternativa sätt för att lösa frågor kring företrädare. Ansvar för att det i dagsläget inte finns någon lösning för e-tjänstelegitimationer faller på den upphandlingsansvariga myndigheten⁹³, men förvaltningen som helhet har inte heller lyckats att ge uttryck för behovet på ett tydligt sätt.

E-legitimationssystemet är i dag inte utformat på ett sätt som möjliggör samverkan med andra system, det vill säga en interoperabel lösning. Ett problem med e-legitimationerna är att gränssnitten inte är standardiserade.

⁹³ I dagsläget är det Kammarkollegiet som är ansvarig myndighet, men även Statskontoret och Verva har ett ansvar för att det i dag saknas en fungerande lösning.

En möjlig lösning på problemen rörande interoperabilitet är att gå över till federationsteknik⁹⁴ och fastställda standarder för gränssnitt, vilket även är en av huvudpunkterna i E-delegationens förslag för att åtgärda bristerna rörande e-legitimationssystemet.⁹⁵

När det gäller främjandet av teknikneutrala standarder för elektroniska signaturer visar granskningen att regeringen inte fullt ut har tagit sitt ansvar.

Regeringens ställningstagande i fråga om e-legitimationer innebar att man valde en PKI-lösning framtagen av bankerna och några ytterligare leverantörer. Lösningen i sig är inte teknikneutral, och den bygger inte på öppna standarder. I uppdraget till ansvariga myndigheter att ta fram specifikationer för e-legitimationer i form av certifikat fanns inte heller några krav på teknikneutralitet. För att åstadkomma interoperabla system för hela den offentliga sektorn krävs en tydlig styrning från regeringen i fråga om systemkrav och val av teknik.

Ansvariga myndigheter har med anledning av regeringens ställningstagande haft små möjligheter att vidta några åtgärder för att främja teknikneutrala lösningar, och därmed kan man svårigen rikta kritik mot deras agerande. Verva har även vid ett flertal tillfällen föreslagit federationsteknik som en möjlig lösning för att uppnå teknikneutralitet. E-delegationen lämnar samma förslag i sitt betänkande. Riksrevisionen tillstyrker också detta förslag.

E-legitimation bygger på specifikationer framtagna i slutet på 90-talet, och lösningen ser i stort sett likadan ut i dag som den gjorde då. Den begränsade konkurrenssituation som blev följden av regeringens ställningstagande har förmodligen inneburit minskad teknisk utveckling och innovation. Att de stora myndigheterna investerade i teknik och utveckling av tjänster som knöt an till e-legitimationslösningen resulterade i att lösningen även fortsättningsvis var tvungen att finnas tillgänglig. Det innebär i sin tur små incitament att utveckla nya eller bättre lösningar. Den enda större ansatsen till utveckling som har förekommit är bankernas försöksverksamhet med e-legitimation i mobilen. Den satsningen skedde dock på bankernas eget initiativ.

Ansvariga myndigheter har med anledning av regeringens ställningstagande haft små möjligheter att vidta några åtgärder för att säkra en dynamisk utveckling av informationssamhällets säkerhetslösningar.

⁹⁴ Federationsteknik innebär i korthet att man skapar en sammanslutning (federation) med en gemensam policy för säkerhetsnivåer och hur identitet ska fastställas. Vilken lösning eller teknik som används för identifiering spelar ingen roll i en federativ lösning, utan federativ teknik möjliggör att passa in olika tekniska lösningar och integrera dessa i e-tjänsteleverantörens system. Programvaran är normalt öppen och standardiserad. Exempel på federationsteknik är SAML.

⁹⁵ SOU 2009:86, s. 98 f.

8.7 Rekommendationer

Med anledning av det förslag som lämnats av E-delegationen angående framtidens lösning för e-legitimationer vill Riksrevisionen framhålla att flera av de brister som har framförts i denna rapport skulle kunna lösas genom E-delegationens förslag. Det gäller exempelvis förslagen om att införa en federationsarkitektur för e-legitimationer och att standardisera gränssnitten. Detta är förslag som Riksrevisionen också bedömer som lämpliga och eftersom dessa förslag behandlas utförligt i E-delegationens rapport nämns de inte som rekommendationer nedan. Några av de brister som Riksrevisionen har iakttagit riskerar dock att kvarstå även om E-delegationens förslag genomförs.

Riksrevisionen rekommenderar därför regeringen att

- genomföra en översyn av tillsynen av systemet för e-legitimationer och överväga att tydliggöra mandatet rörande tillsyn och peka ut en enskild aktör som får ansvar
- vidta åtgärder för att skapa öppna standarder och konkurrensutsätta identifieringsprocessen i syfte att undanröja konkurrensmässiga hinder
- vidta åtgärder för att öka tillgängligheten och skapa en framtida lösning för e-legitimationer utifrån användarnas behov
- genomföra informationssatsningar för medborgare, företag och myndigheter om fördelarna med att använda e-legitimationer.

Bilaga 1

E-legitimationer – samhällsekonomiska aspekter statlig marknadsstyrning
Mats Bergman

31 oktober 2009

Analysen i denna *pm* bygger på en endast översiktlig kunskap om marknaden för E-legitimationer, i huvudsak inhämtade från den preliminära versionen av Riksrevisionens *Förstudie om elektronisk legitimering, e-legitimationer samt från E-delegationens betänkande Strategi för myndigheternas arbete med e-förvaltning*, SOU 2009:86. Syftet är att, vad gäller marknaden för e-legitimationer:

- Belysa för- och nackdelar med statlig samordning av upphandling, särskilt ramavtalsupphandling,
- Beskriva de förutsättningar som krävs för att ramavtal skall vara en effektiv mekanism,
- Analysera om den ramavtalskonstruktion som använts varit effektiv.

Analysen görs med utgångspunkt från relevant ekonomisk teoribildning, utifrån kunskap om hur marknader med liknande egenskaper fungerar med och utan statlig reglering samt utifrån kunskap om hur offentlig upphandling kan organiseras.

Inledningsvis ges en kort beskrivning av hur så kallade tvåsidiga marknader fungerar, eftersom marknaden för E-legitimationer kan beskrivas som en sådan och eftersom dessa marknadsaspekter har betydelse för analysen.

E-legitimationer som en tvåsidig marknad

Tvåsidiga marknader kännetecknas av nätverkseffekter som verkar mellan två *olika* typer av aktörer. Ett exempel är kreditkort, där kortinnehavarna inte interagerar med varandra, men har nytta av att många detaljhandlare accepterar kort; omvänt interagerar inte olika handlare med varandra, men de har större fördel av att acceptera en typ av kort som många kortinnehavare använder sig av. Ett annat sätt att definiera tvåsidiga marknader är att dessa är marknader där olika aktörer interagerar via en *plattform*. Det finns ett stort antal marknader som kan beskrivas som tvåsidiga. Några exempel

är förmedlingstjänster (mötesplatser för köpare och säljare; datingtjänster), köpcenter (butiker och kunder) och operativsystem (datoranvändare och företag som utvecklar dataprogram).

För att tvåsidiga marknader skall fungera väl måste prissättningen balanseras mellan de två sidorna. Orsaken är att när en aktör tillkommer så ökar nyttan på den *andra* sidan av marknaden, dvs. det uppstår en positiv externalitet. Händelsevis kan detta innebära att båda sidor betalar ungefär de kostnader som uppstår på den egna sidan, men generellt är det i princip optimalt att helt eller delvis låta en sida subventionera den andra sidan.⁹⁶ Ett exempel på en marknad med subventioner är marknaden för kreditkort, där kortinnehavare indirekt subventioneras av handlare som tar emot kort. Mekanismen fungerar så, att handlarna betalar relativt höga avgifter till sina banker ("inlösande banker") när de tar emot kortbetalningar. Genom ett avtalssystem har inlösande banker förbundit sig att betala relativt höga avgifter till kortinnehavarnas banker ("kortutgivande banker"). Dessa har i sin tur incitament att konkurrera om kortkunder och att erbjuda dem förmånliga villkor, eftersom en kortkund som använder sitt kort genererar en intäktström från inlösande banker. Ibland kan man därför få kreditkort gratis – och ibland även få bonus på inköpsbeloppet. Ett ännu mer uttalat exempel är Adobe Acrobat, där mjukvara för att läsa pdf-filer är gratis, medan den som vill ha mjukvaran för att producera pdf-filer måste betala.

När ett företag tillhandahåller tjänster på båda sidor av marknaden kan ett system för "korssubventionering" mellan de två sidorna, enligt ovan, enkelt skötas genom företagets avgiftsstruktur. System där samma företag är part i transaktionerna på båda sidor av marknaden brukar benämnas trepartssystem. Exempelvis opererar American Express ett trepartssystem och tidigare nämnda Adobe Acrobat kan också anses vara ett trepartssystem.⁹⁷

När många företag tillhandahåller tjänster, och en del av dem kanske bara på ena sidan av marknaden, kan det vara nödvändigt med en mekanism som balanserar prissättningen mellan de två sidorna. Mekanismen kan bestå av en central plattform som ägs gemensamt av företagen på marknaden eller av ett avtalspaket. Genom en lämplig fördelning av kostnader mellan de två sidorna och eventuellt också betalning från den ena sidan till den andra, så kan en effektiv prisstruktur med en lämplig grad av korssubventionering mellan de två sidorna åstadkommas. En sådan plattform kan ofta också sänka transaktionskostnaderna. System av den här typen brukar, något oegentligt, kallas fyrpartssystem; två exempel är de internationella kreditkortssystemen Visa och MasterCard. Dels sänker dessa fyrpartssystem transaktionskostna-

⁹⁶ Hänsyn bör också tas till transaktionskostnader. I frånvaro av transaktionskostnader skulle den positiva tvåsidiga externaliteten kunna hanteras genom direkta ersättningar mellan de två sidorna.

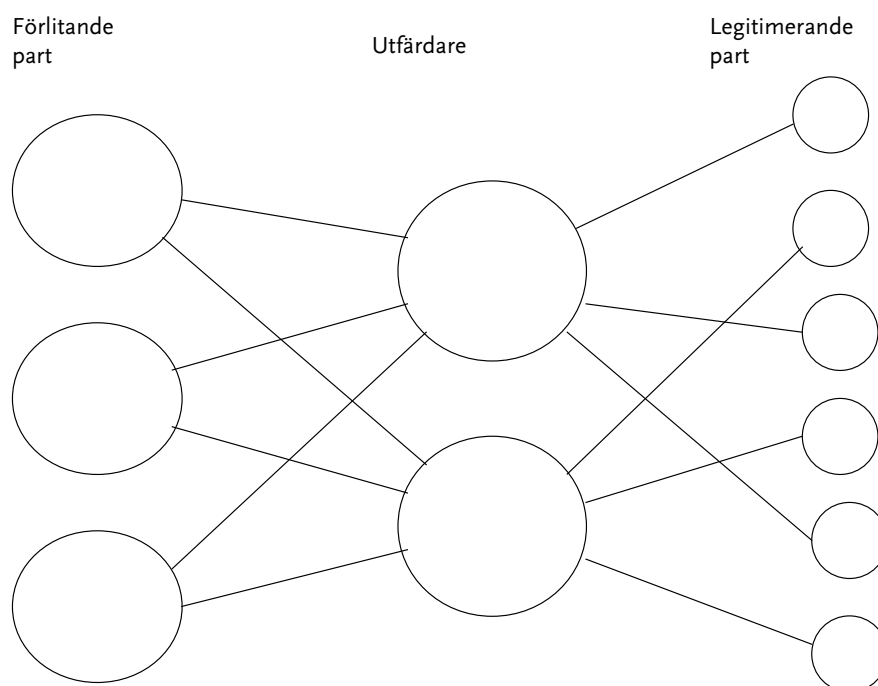
⁹⁷ Detta hindrar inte att American Express, exempelvis, kan avtala med andra finansiella företag om att distribuera deras tjänster eller med dataföretag om att sköta den tekniska hanteringen.

derna, genom att världens alla banker inte behöver sluta avtal med varandra, utan bara med Visa och MasterCard. Dels har de koordinerat prissättningen mellan de två sidorna genom ett centralt avgiftssystem.

I frånvaro av ett fyrpartssystem kan, paradoxalt nog, hård konkurrens på marknads båda sidorna omöjliggöra att en effektiv prisstruktur upprätthålls – dvs. att en lämplig grad av korssubventionering sker. Ett fyrpartssystem kan emellertid ofta lösa detta problem. Samtidigt kan sådana system – som ju i praktiken är överenskommelser om priser mellan många företag – ha konkurrensbegränsande effekter. Av detta skäl har just Visas och MasterCards prisstruktur granskats noga av konkurrensmyndigheterna och, med anledning av detta, modifierats.

Marknaden för E-legitimering kan beskrivas som en tvåsidig marknad. På den ena sidan finns den legitimerande parten, dvs individen som vill identifiera sig med hjälp av en E-legitimation. På den andra sidan finns den förlitande parten, dvs det företag eller den myndighet som ger tillgång till vissa tjänster och delar ut vissa rättigheter sedan legitimering skett. Transaktioner mellan de två sidorna koordineras av en plattformsoperatör, utfärdaren. Den svenska marknaden fungerar i huvudsak som en marknad med flera, delvis konkurrerande trepartssystem. Den legitimerande parten anlitar vanligen en enda utfärdare, medan den förlitande parten oftast sluter avtal med alla utfärdare. Situationen illustreras nedan. (Bankernas egna E-legitimationssystem kan möjligen beskrivas som tvåpartssystem, eftersom bankerna är både utfärdare och förlitande part i förhållande till de egna kunderna.)

Figur 1. Marknaden för E-legitimationer – ett trepartssystem



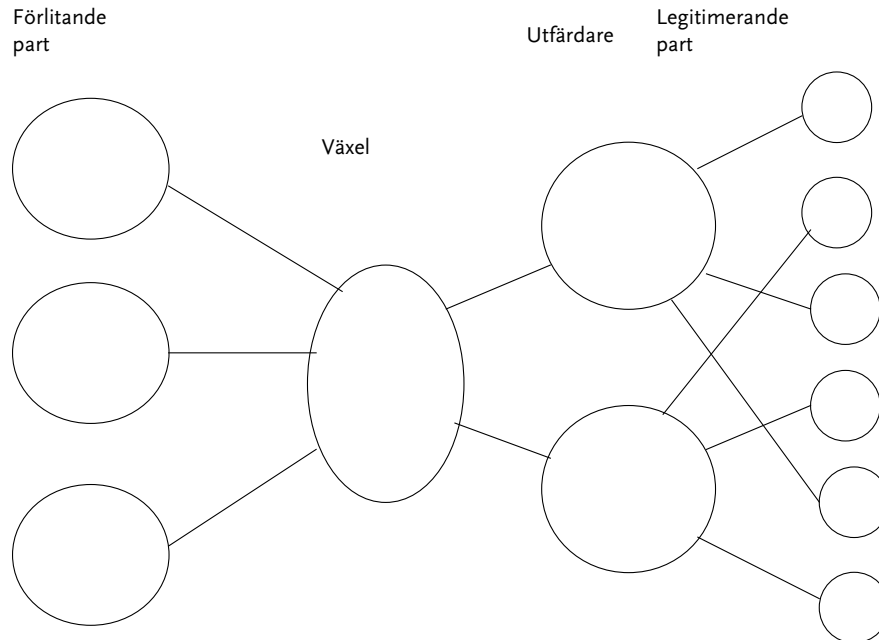
En välkänd nackdel med trepartssystem är att aktörerna på den ena sidan måste sluta avtal med alla eller i varje fall flertalet plattformar (i det här fallet utfärdare). Trots det agerar ofta trepartssystem framgångsrikt, även i konkurrens med fyrpartssystem. Att American Express erbjuder ett trepartssystem nämndes ovan och det sker ju i konkurrens med två stora fyrpartssystem.

Marknaden för E-legitimationer förefaller ha sådana egenskaper att det är motiverat med en prissättning som är utformad så att incitamenten mellan de två sidorna balanseras, dvs en prissättning som innebär en subvention från ena sidan till den andra. På den här marknaden är det sannolikt en förutsättning att den legitimerande parten inte behöver betala för att legitimera sig, medan förlitande part (myndigheter) har en betalningsvilja för att en E-legitimering sker. Ett ökat antal legitimerande parter bidrar till positiva nätverkseffekter och påskyndar det datum då e-förvaltning kan övergå från att vara kostnadsdrivande till att bli kostnadsreducerande. Därför är det motiverat med ett prissättningssystem som innebär att förlitande part betalar till utfärdarna och därmed subventionerar legitimerande parts användning av systemet. Observera dock att flertalet utfärdare själva också är förlitande parter, varför de renodlat förlitande parterna (myndigheterna) inte bör bära hela systemkostnaden.

Ett fyrpartssystem för E-legitimationer

Den svenska E-legitimationsmarknaden skulle sannolikt gynnas av att ett fyrpartssystem introduceras, om detta är tekniskt möjligt. Då skulle samtliga utfärdare och samtliga förlitande parter kunna avtala med en central plattform, en "legitimationsväxel" (i viss analogi med Cekab, ett företag som fyller en liknande funktion på betalkortsmarknaden). Situationen illustreras i figuren nedan.

Figur 2. Marknaden för E-legitimationer som ett fyrpartssystem



I ett fyrpartssystem skulle utfärdarna, liksom idag, åta sig att identifiera individer och i detta syfte sluta avtal med dessa. När en individ vill använda en tjänst som kräver E-legitimation skulle den förlitande parten skicka en fråga till den centrala plattformen ("växeln"), som i sin tur skulle skicka en förfrågan till den utfärdare med vilken förlitande part har ett avtal. Om utfärdaren accepterar E-legitimationen skulle en bekräftelse skickas tillbaka till förlitande part, via "växeln". Dvs. systemet skulle fungera ungefär som när en individ som är kund hos bank A använder sitt betalkort i en butik vars terminal är ansluten till bank B.

I figuren ovan har förlitande parter antagits ha en avtalsrelation direkt med växeln. Detta är bara en möjlighet; man kan också tänka sig att en typ av aktörer fungerar som länk mellan förlitande part och växeln. Detta skulle kunna vara de företag som utfärdar E-legitimationer eller företag som är specialiserade på att länka förlitande parter med växeln. I E-delegationens betänkande föreslås Skatteverket utföra de tjänster som i figuren ovan utförs av en "växel". Delegationen kallar modellen för en "federationslösning".

Ett fyrpartssystem har ett antal fördelar. Antalet avtalsrelationer minskar väsentligt när antalet aktörer är stort, vilket sänker transaktionskostnaderna. Framför allt behöver förlitande part bara sluta ett avtal, nämligen med den centrala plattformen ("växeln") eller, alternativt, med ett företag som länkar förlitande parter med "växeln". Eftersom endast växeln behöver sluta avtal med utfärdaren så finns inga starka skäl att utesluta utfärdare med ett litet

antal anslutna legitimerande parter. Därmed blir det möjligt att ansluta utfärdare som specialiserar sig på vissa kundgrupper, exempelvis individer med ovanliga operativsystem eller särskilda behov. Det blir också enklare för nya aktörer att ansluta sig till systemet, vilket är bra ur konkurrenssynpunkt.

Vidare gäller att en fyrpartersmodell går att förena med ändamålsenliga mekanismer för styrning och prissättning. Detta gäller även om olika företag agerar på de två sidorna av marknaden, t.ex. om vissa företag specialiserar sig på att agera utfärdare och andra på att utföra tjänster för förlitande part. En subvention från den ena sidan till den andra kan enkelt åstadkommas genom avgifter till respektive ersättning från "växeln" till de anslutna företagen. Hur en lämplig prisstruktur kan se ut mer i detalj diskuteras nedan.

Man kan tänka sig att den centrala funktionen ("växeln") ägs – och därmed styrs – av det offentliga eller gemensamt av marknadens aktörer. Den förra modellen föreslås av E-delegationen, medan den senare ofta används på finansiella marknader. En central funktion som ägs av marknadsaktörerna skulle sannolikt i stor utsträckning vara självreglerande. Dvs. marknadsaktörerna skulle ha incitament att se till att hög säkerhet mm. upprätthölls. En central funktion ägd av det offentliga innebär istället att samhället får kontroll över den strategiska styrningen och därmed ansvar för dessa frågor. Samtidigt kan mycket av den faktiska produktionen bedrivas i privat regi, vilket ofta innebär bättre kostnadskontroll. E-delegationen föreslår att den funktion jag här kallar växel drivs av Skatteverket och att ersättningen till utfärdarna ensidigt fastställs av växeln (Skatteverket). Det senare föreslås ske enligt samma princip som när kommuner med kundvals-system fastställer ersättningen för friskolor och privata äldreomsorgsföretag, i det senare fallet enligt lagen om valfrihetssystem (LOV).

Eftersom den offentliga sektorn är den enda egentliga användaren på den förlitande sidan av ett fyrpartssystem (bortsett från bankernas interna användning) så förefaller det rimligt att denna skall ha en ledande roll vad gäller ägande och styrning av en central plattform. Detta utesluter inte att stora utfärdare är delägare eller att de i varje fall på en tämligen operativ nivå medverkar i styrningen av plattformen.

Ett fyrpartssystem erbjuder en väg bort från den nuvarande ramavtalsmodellen, vilken har många nackdelar. (Se nedan.) Observera att inrättandet av ett fyrpartssystem inte hindrar att trepartssystem samtidigt finns kvar på marknaden. Det är måhända osannolikt att banker skulle acceptera inloggning genom ett system som drivs av en annan bank eller, exempelvis, av Skatteverket.

Tillsyn

Med tillsyn menas i detta avsnitt statlig övervakning och reglering av säkerhetsmässiga aspekter och liknande, men inte reglering av prissättning och prisstruktur.

Det är inte självklart att någon omfattande tillsyn behövs av marknaden, i synnerhet inte om ett fyrpartssystem utvecklas. Detta gäller självklart i ännu högre grad om den centrala funktionen ägs och drivs av den offentliga sektorn, enligt E-delegationens förslag. Dock framstår det som uppenbart att styrning via upphandlade leveransavtal inte är en ändamålsenlig metod. Mer rimligt vore statlig styrning antingen genom ett direkt statligt ägaransvar, enligt E-delegationens förslag, eller genom traditionell statlig myndighetstillsyn.

Bankerna erbjuder E-legitimationstjänster med till synes tillräcklig säkerhet utan någon egentlig tillsyn och myndigheterna (de förlitande parterna) är rimligen starka nog att inte sluta avtal med oseriösa aktörer eller aktörer med för låg säkerhetsnivå. Man kan också tänka sig grader av tillsyn. Om granskande myndighet aktivt skall godkänna varje utfärdare blir tillsynen relativt hård. En mildare form av tillsyn är att aktörer (kanske under vissa förutsättningar) får välja att agera som utfärdare och att den granskande myndigheten endast ingriper när den upptäcker missförhållanden. På den här marknaden förefaller den mildare formen av tillsyn motiverad, i varje fall för de aktörer som själva har ett uppenbart intresse av att upprätthålla en hög grad av säkerhet (banker mm).

Om ett utpekat tillsynsansvar skall finnas, dvs. i första hand om systemet drivs av privata företag, så förefaller det rimligt att samla ansvaret till en enda myndighet. Mest närliggande är i så fall PTS, som bl a har till uppgift att bevaka säkerheten på internet. Mindre naturliga alternativ är Finansinspektionen, FRA eller MSB. Det finns två skäl till detta. Dels har PTS närliggande uppgifter vad gäller säkerhet. Dels kan det (se nedan) finnas skäl att reglera ersättningen för legitimeringstjänster, och PTS har liknande uppgifter för marknader som principiellt liknar E-legitimationsmarknaden. PTS besitter därmed både de tekniska kunskaperna som behövs för att utöva tillsyn över säkerheten och de ekonomiska och juridiska kunskaper som behövs för en eventuell prisreglerande roll.

Ramavtalsupphandling och utvärderingskriterier

Ramavtal används ofta när flera olika köpare vill koordinera sina inköp och när inköpsvolymerna är okända. Ett syfte är att minska transaktionskostnaderna, genom att en enda upphandling kan genomföras för flera köpares räkning. Ett annat syfte är att pressa priset genom att samla flera köpares volym. (Se Fredrik Anderssons rapport för Konkurrensverket, 2006.)

Ramavtal kan också användas av en enda köpare och skall i princip användas i de fall inköpsvolymen är osäker, oavsett antal köpare. (I praktiken används dock ofta andra upphandlingsformer även då en relativt hög osäkerhet råder om inköpsvolymen, vilket sannolikt är i strid med lagstiftarens intentioner.)

En nackdel med ramavtalsupphandlingar är att den osäkerhet som råder om inköpsvolym riskerar att höja prisnivån. Säljaren ger ju köparen en option att köpa till ett fastställt pris och måste därmed hålla kapacitet i beredskap; kapacitet som kanske inte kommer att utnyttjas. Säljaren måste kompenseras för detta, vilket i allmänhet sker genom en högre prisnivå. Om denna effekt är stark nog att motverka de två besparingseffekterna enligt ovan beror självfallet på omständigheterna.

I det här fallet framstår det som sannolikt att vinsterna, i form av lägre transaktionskostnader, överstiger nackdelarna, i form av en prispremie för osäkerhet om inköpsvolymerna. Det är sannolikt inte möjligt att exakt förutse transaktionsvolymerna; därmed skulle även en upphandling som genomförs av en enskild myndighet egentligen också behöva utformas som ramavtal.⁹⁸ Transaktionskostnaderna är sannolikt relativt höga, med tanke på den relativt höga graden av teknisk komplexitet.

Inom ramen för detta uppdrag har det inte varit möjligt att ta ställning till om de tekniska krav och de kvalitetskrav som ställs är rimliga eller ändamålsenligt formulerade och värderade. Däremot finns det anledning att kommentera hur priserna värderas och vägs samman med kvalitén.

För det första är det viktigt att de ”representativa myndigheter” som används vid utvärderingen av priser faktiskt är representativa. Om de inte är det, så blir det möjligt för budgivarna att lämna ”skruvade” bud, dvs. bud som exploaterar det faktum att den vikt som läggs på en viss tjänst vid anbudsvärderingen avviker från den förväntade faktiska vikten. De tjänster som har relativt hög vikt vid utvärderingen (jämfört med förväntade faktiska volymer) kommer att prissättas (mycket) lågt, medan de tjänster som har relativt låg vikt vid utvärderingen kommer att prissättas (mycket) högt. Det har inte funnit utrymme för att värdera om detta är eller varit en reell risk vid upphandling av E-legitimationstjänster.

För det andra används en modell där priserna värderas i förhållande till lägsta avgivna bud. Det lägsta budet erhåller högsta poäng, högre bud erhåller linjärt avtagande poäng ända tills priset är dubbelt så högt som det lägsta. Vid en prisnivå motsvarande två gånger det lägsta priset eller högre erhålls noll poäng.

⁹⁸ Den underliggande osäkerheten om efterfrågan skulle med andra ord inte minska bara för att man valde att inte använda ramavtal.

En sådan relativ värderingsmodell har två påtagliga nackdelar. Dels kan rangordningen bli beroende av irrelevanta alternativ. Detta utvecklas utförligt i Lunander och Anderssons rapport för Konkurrensverket (2004). Dels, och väl så allvarligt, gör en sådan modell att värderingen av kvalitet i praktiken tenderar att bli godtycklig och frikopplad från rimliga bedömning av vad kvalitet är värd. Detta utvecklas av Bergman och Lundberg (2009, kommande) och av Lunander och Andersson.

Kvalitet och pris bör istället vägas samman genom att kvalitet värderas i kronor och genom att motsvarande (fiktiva, endast för anbudsvärderingen) avdrag görs från det erbjudna priset. Detta gäller oaktat att omräkning av pris till (kvalitets)poäng är den vanligaste modellen vid offentlig upphandling. Om det är svårt att värdera kvalitet, eller om värdet av högsta tänkbara kvalitet inte påtagligt överstiger värdet av lägsta acceptabla kvalitet, så bör istället en renodlad priskonkurrens med höga skall-krav övervägas.

Ramavtalsmodellen och prisnivån

Uppenbarligen är det kostnadseffektivt att använda de system som redan är i drift för E-legitimering. Dels är det kostsamt att bygga upp systemen som sådana. Än viktigare förefaller dock kostnaden för kundackvisation vara, med tanke på kundernas ovilja att ansluta sig till fler än ett legitimeringsystem.

En fördel med ramavtalsmodellen är att dessa kostnadsbesparingar kan utnyttjas, men modellen har också väsentliga nackdelar. Det är svårt för myndigheter att bara erbjuda e-tjänster till vissa bankers kunder och detta vet givetvis de banker som kan erbjuda E-legitimationstjänster. Om upphandlaren (staten) är pressad att köpa av alla, eller i stort sett alla, budgivare, så är incitamenten att konkurrera med priset små. Varje utfärdare har i det närmaste monopol på sina legitimerande parter (sina anslutna kunder) och kan därför begära ett högt pris. Om, å andra sidan, upphandlaren försöker skapa en verklig konkurrenssituation, så innebär detta att man måste vara villig att riskera att utestänga stora grupper av legitimerande parter – om den aktuella utfärdaren begär ett alltför högt pris. (Situationen liknar i viss mån det "termineringsmonopol" som varje teleoperatör anses ha, hur liten marknadsandel operatören än har. Monopolet innebär att endast den operatör, hos vilken en viss kund köper teletjänster, kan koppla samtal *till* just den kunden, dvs. "terminera" samtal till den aktuella kunden. På telemarknaden har detta motiverat att termineringstjänster är prisreglerade också för mycket små aktörer.)

Med andra ord är upphandling, i form av ramavtal eller på annat sätt, inte en lämplig modell när köparen avser att köpa av alla eller så gott som alla budgivare. (Detsamma gäller när köparen avser att köpa av de utfärdare

som står för alla eller så gott som alla ingångna avtal med legitimerande parter.) När budgivarna vet att alla kommer att få sälja, i det närmaste oavsett prisnivån och oavsett om deras bud är högst eller lägst, så försvinner incitamenten att konkurrera med priset. Marknader med dessa egenskaper brukar prisregleras – eller så sköts uppgifterna i regi av den offentliga sektorn själv, enligt diskussionen ovan. Alternativet är att strukturera om marknaden eller definiera om behovet så att en verklig konkurrens kan uppstå. En medelväg av dessa två alternativ är att E-legitimationssystemet som sådant ägs av den offentliga sektorn, medan driften av detta upphandlas. En sådan lösning förutsätter inte att privatkunder byter utfärdare. Fungerande konkurrens utan något inslag av offentligt ägande torde däremot kräva att stora kollektiv av privatkunder byter leverantör när en gammal leverantör förlorar en upphandling på grund av att det begärda priset är alltför högt.

Den faktiska tillämpningen av ramavtalsmodellen har gynnat leverantörer som har många kunder anslutna. Om en sådan modell alls skall väljas, så vore det bättre att gynna aktörer som kan ansluta många kunder per kostnad. Dvs. en utfärdare som kan ansluta 10 000 kunder och begär 1 krona per transaktion bör väljas före en utfärdare som kan ansluta 1 miljon kunder och begär 2 kronor per transaktion. Det hindrar inte att man ställer upp som mål att ett visst antal kunder (eller en viss andel av befolkningen) skall finnas bland vinnarna av upphandlingen. Detta löses enkelt genom att budgivarna rangordnas efter pris per transaktion (eller per kund, se nedan) och att så många vinnare utses, som behövs för att nå upp till det önskade antalet legitimerade parter. För att förhindra att prisnivån blir alltför hög kan man dessutom sätta ett maxpris per kund eller per transaktion. Om maxpriset nås innan det önskade antalet legitimerade parter så accepterar man att man inte når sitt mål. För att spara transaktionskostnader kan man förstås välja att prioritera ned utfärdare med ett mycket litet antal kunder.

Som alternativ till prissättning i konkurrens och genom offentlig upphandling, så kan man tänka sig att priset bestäms genom att det offentliga står som ägare till de centrala systemkomponenterna och helt enkelt fastställer vilken ersättning som skall utgå till de privata leverantörerna. Detta är den modell E-delegationen föreslagit. En annan metod är att använda traditionell prisreglering av de aktuella tjänsterna, motsvarande vad som gäller på vissa andra nätverksmarknader, t.ex. telemarknaden.

Ytterligare en nackdel med ramavtalsmodellen (och kanske också med andra upphandlingsmodeller) är att den är svår att förena med en optimal prisstruktur. I följande avsnitt redovisas överväganden om hur en sådan struktur skulle kunna se ut.

Prisstruktur

Utformningen av prisstrukturen och fastställandet av prisnivån är två i viss mån oberoende frågor. Prisnivå kan tolkas som medelpris eller, alternativt, totala intäkter för de reglerade företagen. I allmänhet kan man tänka sig många olika prisstrukturer som ger samma medelpris. Exempelvis kan man ha höga fasta priser och låga rörliga, eller tvärt om; man kan låta vissa kundgrupper betala mycket och andra litet, osv.

Av skäl som redogjorts för ovan är det rimligt att utforma prisstrukturen så att ersättning utgår till utfärdare från förlitande part. Ersättningen bör utformas så att den maximerar nyttan av systemet, vilket bl.a. innebär att utfärdare och förlitande parter ges incitament som stimulerar till kundackvisation respektive utveckling av e-tjänster i rimlig grad.

Det finns skäl att tro att den tillkommande kostnaden per transaktion för en befintlig kund är relativt låg, medan kostnaden för att övertala en ny kund att ansluta sig (kundackvisation) är relativt hög. På den förlitande sidan finns en variation mellan myndigheter som har blott någon enstaka transaktion per legitimerande part och år – och de som har åtskilliga transaktioner per legitimerande part och år.

Detta talar för att betalningen från förlitande part till utfärdare bör vara två- eller tredelad.⁹⁹ Prisstrukturen kan innehålla ett lågt pris per transaktion, som i stort sett motsvarar marginalkostnaden per transaktion, och ett pris per ansluten kund, som motiveras av kostnaden per nyansköffad kund. För att förtydliga redogörs nedan, i ett fiktivt exempel, hur en sådan prisstruktur skulle kunna utformas.

Exempel (fiktivt): Låt oss säga att Skattemyndigheten har 6 miljoner "kunder" som var och en gör en transaktion per år, och att 300 kommuner har i genomsnitt 20 000 "kunder" som gör 9 transaktioner per år. Inga andra förlitande parter finns. Totalt finns alltså 6 miljoner individer som använder E-legitimation. Alla är "kunder" hos Skattemyndigheten och var och en är "kund" hos en enda kommun. Totalt gör individerna 60 miljoner transaktioner per år. Antag att marginalkostnaden per transaktion är 0,1 kr, att marginalkostnaden för att ansluta en förlitande part är 20 000 och att marginalkostnaden för att skaffa en ny kund kan beräknas till motsvarande 2 kronor per person och år. Antag slutligen att de totala kostnaderna är 36 miljoner kronor.

⁹⁹ Här bortses från anslutningsavgift, även om en sådan i och för sig kan vara motiverad. Vidare bortses från distinktionen mellan aktiva och potentiella användare; en sådan kan också vara motiverad. Såväl anslutningsavgifter som distinktionen mellan aktiva och passiva användare återfinns i förfrågningsunderlaget. Enligt förfrågningsunderlaget skall budgivarna erbjuda en meny av prislister. Jag återkommer nedan till detta.

Marginalkostnadsprissättning innebär med detta exempel 0,1 krona per transaktion, 1 krona per kund (dvs 2 x 6 miljoner kronor i kostnad delat på 2 x 6 miljoner kundrelationer) och 20 000 kronor per förlitande, vilket ger totala intäkter på 6 plus 12 plus 6 miljoner kronor eller totalt 24 miljoner kronor. De återstående 12 miljoner kronorna, de genuint fasta (eller gemensamma) kostnaderna måste fördelas genom påslag på de rörliga kostnaderna. Utgångspunkten i exemplet är att alla kostnader skall betalas av de förlitande parterna, utifrån en bedömning att detta gynnar systemeffektiviteten bäst, dvs. bäst tillvaratar tvärsidiga nätverkseffekter.¹⁰⁰

Ett påslag på avgiften per förlitande part riskerar att avskräcka små myndigheter från att erbjuda e-tjänster, medan påslag på avgiften per transaktion riskerar att avskräcka myndigheter med många transaktioner från att utveckla attraktiva e-tjänster. Påslag på avgiften per ansluten kund riskerar å andra sidan att avskräcka myndigheter med få transaktioner per kund. I princip bör de 12 miljoner kronorna i fasta avgifter fördelas så att de negativa incitamentseffekterna blir så små som möjligt. Detta innebär, enligt principen för Ramseyprissättning, att höga påslag skall göras i de dimensioner där de förlitande parternas priskänslighet är relativt låg, och omvänt.

I exemplet har hänsyn till de tvärsidiga nätverkseffekterna tagits bara på ett begränsat sätt, genom utgångspunkten att hela systemkostnaden skall bäras av de förlitande parterna. En mer exakt beräkning av optimal avgiftsstruktur kan leda till att legitimerande parter får betala en viss andel av kostnaderna – eller omvänt att förlitande parter får betala avgifter som sammanlagt överstiger kostnaderna. Det senare skulle göra det mer lönsamt för utfärdarna att konkurrera om att ansluta fler legitimerande parter.

Att fastställa optimal prisstruktur förutsätter kunskap om förlitande parter efterfrågeelasticitet i de tre dimensionerna (årlig anslutningsavgift, avgift per transaktion och avgift per kund); den samlade nyttan hos förlitande parter av att ansluta ytterligare en legitimerande part; legitimerande parts efterfrågeelasticitet (eller kostnaden för att förmå ytterligare en kund att ansluta sig); nyttan hos legitimerande part av att ytterligare förlitande parter ansluts och av att ytterligare e-tjänster görs tillgängliga; samt konkurrenssituationen på marknadens två sidor. En helt igenom optimal prissättning är med andra ord svår att uppnå. Däremot bör en utveckling av ovanstående principer kunna ge viss vägledning för hur en förbättrad prisstruktur skulle kunna åstadkommas.

Ytterligare en komplexitetsdimension är att utfärdarna kan erbjuda olika menyer av priser, med olika kombinationer av fasta och rörliga avgifter, som är tänkta att användas av förlitande parter med olika behov. Exempelvis

¹⁰⁰ Implicit är en annan utgångspunkt självkostnadsprissättning, dvs att kostnaderna skall bäras av de myndigheter som erbjuder e-tjänster. Om det finns starka positiva nätverkseffekter kan man ju också tänka sig att staten går in och betalar hela eller delar av kostnaderna för systemet.

kommer en förlitande part med få transaktioner att föredra låga fasta avgifter även om detta medför relativt höga rörliga avgifter, medan en förlitande part med många transaktioner kommer att föredra låga rörliga avgifter även om detta medför relativt höga fasta avgifter. Detta brukar kallas andra gradens prisdiskriminering och syftar till att å ena sidan hålla uppe intäkterna och, å andra sidan, erbjuda kunderna priser som skapar så små distortioner som möjligt. Det är i allmänhet effektivt att tillåta andra gradens prisdiskriminering.

En effektiv prisstruktur är sannolikt svår att uppnå vid en upphandlingslösning, även om upphandlaren av E-legitimationstjänster uppenbarligen försökt styra prisstrukturen i den riktningen. Det är sannolikt lättare att uppnå en bra prisstruktur om antingen centrala delar av systemet är statligt ägt eller genom en traditionell prisreglering.

Sammanfattning och slutsatser

Det finns stora nackdelar med att upphandla E-legitimationstjänster, givet önskemålet att utfärdare med avtalsrelation med en mycket stor andel av befolkningen skall finnas bland dem som tilldelat avtal. Detta önskemål gör att priskonkurrens inte kommer att fungera väl.

En alternativ ansats är att utveckla en E-legitimation kontrollerad av staten och som helt enkelt fastställer ersättningen till utfärdarna, enligt E-delegationens förslag. Ansatsen kan kombineras med att man låter privata utförare konkurrera om att handha *driften* av det aktuella systemet. Ett annat alternativ är att utveckla marknaden i riktning mot ett fyrpartssystem som antingen är uttryckligen reglerat eller självreglerat. Prisreglering kräver att lagstiftning införs. Sannolikt skulle PTS vara den mest lämpliga regleraren; myndigheten har både teknisk kompetens och ekonomisk-juridisk regleringskompetens.

I båda fallen – offentligt ägande respektive privat ägande med reglering – är det lämpligt att utveckla systemet så att befintliga utfärdare och förlitande parter enbart behöver en avtalsrelation (med en central plattform), dvs. ett fyrpartssystem. Detta sänker transaktionskostnaderna.

I det fall upphandling trots dessa invändningar skulle användas även i framtiden, så förefaller ramavtal att vara den enda rimliga och möjliga ansatsen. Det har inte funnits möjlighet att inom ramen för detta uppdrag utvärdera metodiken för att värdera kvalitet. Däremot bör metodiken för att väga samman pris och kvalitet ändras, så att kvalitet värderas i (räknas om till) pengar, istället för att pris räknas om till (kvalitets)poäng. Den senare metoden innebär att rangordningen kan ändras av irrelevanta alternativ och, mer allvarligt, att det är svårt att på ett rimligt sätt värdera kvalitetsskillnader.

Vid en jämförelse mellan olika leverantörers (utfärdares) anbud bör rangordning ske efter pris per ansluten legitimerande part, snarare än efter antal legitimerande parter. (Möjligen kan en viss premiering ske av stora aktörer, i den mån detta innebär lägre kostnader för upprättande av avtalsrelationer mellan utfärdare och förlitande parter.)

Prisstrukturen bör utformas så att den gynnar tvåsidiga nätverkseffekter, genom att kostnaderna på ett lämpligt sätt allokeras i proportion till antal förlitande parter, antal (aktiva eller potentiella) legitimerande parter och antal transaktioner. Sannolikt är det rätt att lägga kostnaderna på förlitande parter och inte på legitimerande parter.

Tidigare utgivna rapporter från Riksrevisionen

2003	2003:1	Hur effektiv är djurskyddstillsynen?
2004	2004:1	Länsplanerna för regional infrastruktur – vad har styrts prioriteringarna?
	2004:2	Förändringar inom kommittéväsendet
	2004:3	Arbetslöshetsförsäkringens hantering på arbetsförmedlingen
	2004:4	Den statliga garantimodellen
	2004:5	Återfall i brott eller anpassning i samhället – uppföljning av kriminalvårdens klienter
	2004:6	Materiel för miljarder – en granskning av försvarets materiel- försörjning
	2004:7	Personlig assistans till funktionshindrade
	2004:8	Uppdrag statistik – Insyn i SCB:s avgiftsbelagda verksamhet
	2004:9	Riktlinjer för prioriteringar inom hälso- och sjukvård
	2004:10	Bistånd via ambassader – en granskning av UD och Sida i utvecklingssamarbetet
	2004:11	Betyg med lika värde? – en granskning av statens insatser
	2004:12	Höga tjänstemäns representation och förmåner
	2004:13	Riksrevisionens årliga rapport 2004
	2004:14	Arbetsmiljöverkets tillsyn
	2004:15	Offentlig förvaltning i privat regi – statsbidrag till idrottsrörelsen och folkbildningen
	2004:16	Premiepensionens första år
	2004:17	Rätt avgifter? – statens uttag av tvingande avgifter
	2004:18	Vattenfall AB – Uppdrag och statens styrning
	2004:19	Vem styr den elektroniska förvaltningen?
	2004:20	The Swedish National Audit Office Report 2004
	2004:21	Försäkringskassans köp av tjänster för rehabilitering
	2004:22	Arlandabanan – Insyn i ett samfinansierat järnvägsprojekt
	2004:23	Regelförenklningar för företag
	2004:24	Snabbare asylprövning
	2004:25	Sjukpenninganslaget – utgiftsutveckling under kontroll?
	2004:26	Utgift eller inkomstavgift? – Regeringens hantering av det tillfälliga sysselsättningsstödet
	2004: 27	Stödet till polisens brottsutredningar
	2004:28	Regeringens förvaltning och styrning av sex statliga bolag
	2004:29	Kontrollen av strukturfonderna
	2004:30	Barnkonventionen i praktiken

- 2005 2005:1 Miljömålsrapporteringen – för mycket och för lite
- 2005:2 Tillväxt genom samverkan? Högskolan och det omgivande samhället
- 2005:3 Arbetslöshetsförsäkringen – kontroll och effektivitet
- 2005:4 Miljögifter från avfallsförbränningen – hur fungerar tillsynen
- 2005:5 Från invandrapolitik till invandrapolitik
- 2005:6 Regionala stöd – styrs de mot ökad tillväxt?
- 2005:7 Ökad tillgänglighet i sjukvården? – regeringens styrning och uppföljning
- 2005:8 Representation och förmåner i statliga bolag och stiftelser
- 2005:9 Statens bidrag för att anställa mer personal i skolor och fritidshem
- 2005:10 Samordnade inköp
- 2005:11 Bolagiseringen av Statens järnvägar
- 2005:12 Uppsikt och tillsyn i samhällsplaneringen – intention och praktik
- 2005:13 Riksrevisionens årliga rapport 2005
- 2005:14 Förtidspension utan återvändo
- 2005:15 Marklösen – Finns förutsättningar för rätt ersättning?
- 2005:16 Statsbidrag till ungdomsorganisationer – hur kontrolleras de?
- 2005:17 Aktivitetsgarantin – Regeringen och AMS uppföljning och utvärdering
- 2005:18 Rikspolisstyrelsens styrning av polismyndigheterna
- 2005:19 Rätt utbildning för undervisningen – Statens insatser för lärarkompetens
- 2005:20 Statliga myndigheters bemyndiganderedovisning
- 2005:21 Lärares arbetstider vid universitet och högskolor – planering och uppföljning
- 2005:22 Kontrollfunktioner – två fallstudier
- 2005:23 Skydd mot mutor – Läkemedelsförmånsnämnden
- 2005:24 Skydd mot mutor – Apoteket AB
- 2005:25 Rekryteringsbidrag till vuxenstuderande – uppföljning och utbetalningskontroll
- 2005:26 Granskning av Statens pensionsverks interna styrning och kontroll av informationssäkerheten
- 2005:27 Granskning av Sjöfartsverkets interna styrning och kontroll av informationssäkerheten
- 2005:28 Fokus på hållbar tillväxt? Statens stöd till regional projektverksamhet
- 2005:29 Statliga bolags årsredovisningar
- 2005:30 Skydd mot mutor – Banverket
- 2005:31 När oljan når land – har staten säkerställt en god kommunal beredskap för oljekatastrofer?

- 2006 2006:1 Arbetsmarknadsverkets insatser för att minska deltidsarbetslösheten
- 2006:2 Regeringens styrning av Naturvårdsverket
- 2006:3 Kvalitén i elöverföringen – finns förutsättningar för en effektiv tillsyn?
- 2006:4 Mer kemikalier och bristande kontroll – tillsynen av tillverkare och importörer av kemiska produkter
- 2006:5 Länsstyrelsernas tillsyn av överförmyndare
- 2006:6 Redovisning av myndigheters betalningsflöden
- 2006:7 Begravningsverksamheten – förenlig med religionsfrihet och demokratisk styrning?
- 2006:8 Skydd mot korruption i statlig verksamhet
- 2006:9 Tandvårdsstöd för äldre
- 2006:10 Punktskattekontroll – mest reklam?
- 2006:11 Vad och vem styr de statliga bolagen?
- 2006:12 Konsumentskyddet inom det finansiella området – fungerar tillsynen?
- 2006:13 Kvalificerad yrkesutbildning – utbildning för marknadens behov?
- 2006:14 Arbetsförmedlingen och de kommunala ungdomsprogrammen
- 2006:15 Statliga bolag och offentlig upphandling
- 2006:16 Socialstyrelsen och de nationella kvalitetsregistren inom hälso- och sjukvården
- 2006:17 Förvaltningsutgifter på sakanslag
- 2006:18 Riksrevisionens årliga rapport
- 2006:19 Statliga insatser för nyanlända invandrare
- 2006:20 Styrning och kontroll av regeltillämpningen inom socialförsäkringen
- 2006:21 Finansförvaltningen i statliga fastighetsbolag
- 2006:22 Den offentliga arbetsförmedlingen
- 2006:23 Det makroekonomiska underlaget i budgetpropositionerna
- 2006:24 Granskning av Arbetsmarknadsverkets interna styrning och kontroll av informationssäkerheten
- 2006: 25 Granskning av Migrationsverkets interna styrning och kontroll av informationssäkerheten
- 2006:26 Granskning av Lantmäteriverkets interna styrning och kontroll av informationssäkerheten
- 2006:27 Regeringens uppföljning av överskottsmålet
- 2006:28 Anställningsstöd
- 2006:29 Reformen av Försvarets logistik – Blev det billigare och effektivare?
- 2006:30 Socialförsäkringsförmåner till gravida – Försäkringskassans agerande för en lagenlig och enhetlig tillämpning
- 2006:31 Genetiskt modifierade organismer – det möjliga och det rimliga
- 2006:32 Bidrag som regeringen och Regeringskansliet fördelar

- 2007 2007:1 Statlig tillsyn av bostad med särskild service enligt LSS
- 2007:2 The Swedish National Audit Office – Annual report 2006
- 2007:3 Regeringens beredning och redovisning av skatteutgifter
- 2007:4 Beredskapen för kärnkraftsolyckor
- 2007:5 Regeringens skatteprognoser
- 2007:6 Vägverkets körprov – lika för alla?
- 2007:7 Den största affären i livet – tillsyn över fastighetsmäklare och konsumenternas möjlighet till tvistelösning
- 2007:8 Regeringens beredning av förslag om försäljning av sex bolag
- 2007:9 Säkerheten vid vattenkraftdammar
- 2007:10 Regeringens styrning av informationssäkerhetsarbetet i den statliga förvaltningen
- 2007:11 Statens företagsbefrämjande insatser. När de kvinnor och personer med utländsk bakgrund?
- 2007:12 Hur förbereds arbetsmarknadspolitiken? En granskning av regeringens underlag
- 2007:13 Granskning av Årsredovisning för staten 2006
- 2007:14 Riksrevisionens årliga rapport
- 2007:15 Almi Företagspartner AB och samhällsupdraget
- 2007:16 Regeringens uppföljning av kommunernas ekonomi
- 2007:17 Statens insatser för att hantera omfattande elavbrott
- 2007:18 Bilprovningen och tillgängligheten – Granskning av ett samhällsuppdrag
- 2007:19 Tas sjukskrivnas arbetsförmåga till vara? Försäkringskassans kontakter med arbetsgivare
- 2007:20 Oegentligheter inom bistånd – Är Sidas kontroll av biståndsinsatser via enskilda organisationer tillräcklig?
- 2007:21 Regeringens analys av finanspolitikens långsiktiga hållbarhet
- 2007:22 Sambandet mellan utgiftstaket, överskottsålet och skattepolitiken – regeringens redovisning
- 2007:23 Statens insatser vid anmälningar av vårdskador – Kommer patienten till tals?
- 2007:24 Utanförskap på arbetsmarknaden – Funktionshindrade med nedsatt arbetsförmåga
- 2007:25 Styrelser med fullt ansvar
- 2007:26 Regeringens redovisning av budgeteffekter
- 2007:27 Statligt bildande stiftelsers årsredovisningar
- 2007:28 Krisberedskap i betalningssystemet – Tekniska hot och risker
- 2007:29 Vattenfall – med vind i ryggen?
- 2007:30 Så förvaltas förmögenheten – fem stiftelsers kapitalförvaltning och regeringens roll som stiftare
- 2007:31 Bistånd genom budgetstöd – regeringens och Sidas hantering av en central biståndsform
- 2007:32 Försäkringskassans hantering av arbetsskadeförsäkringen

- 2008 2008:1 Pandemier – hantering av hot mot människors hälsa
- 2008:2 Statens insatser för att bevara de kyrkliga kulturminnena
- 2008:3 Staten och pensionsinformationen
- 2008:4 Regeringens redovisning av arbetsmarknadspolitikens förväntade effekter
- 2008:5 Högskolelärares bisysslor
- 2008:6 Regler och rutiner för indirekt sponsring – tillräckligt för att säkerställa SVT:s oberoende?
- 2008:7 Statligt bildade stiftelser – regeringens insyn och uppföljning
- 2008:8 Dricksvattenförsörjning – beredskap för stora kriser
- 2008:9 Regeringen och krisen – regeringens krishantering och styrning av samhällets beredskap för allvarliga samhällskriser
- 2008:10 Riksrevisorernas årliga rapport 2008
- 2008:11 Tvärvillkorskontroller i EU:s jordbruksstöd
- 2008:12 Regeringens försäljning av åtta procent av aktierna i TeliaSonera
- 2008:13 Svenskundervisning för invandrare (sfi). En verksamhet med okända effekter
- 2008:14 Kulturbidrag – effektiv kontroll och goda förutsättningar för förnyelse?
- 2008:15 Tillämpningen av det finanspolitiska ramverket. Regeringens redovisning i 2008 års ekonomiska vårproposition
- 2008:16 Sänkta socialavgifter – för vem och till vilket pris?
- 2008:17 Regeringens hantering av tilläggsbudgeten
- 2008:18 Avveckling av myndigheter
- 2008:19 Hög kvalitet i högre utbildning?
- 2008:20 Granskning av Årsredovisning för staten 2007
- 2008:21 Statens styrning av kvalitet i privat äldreomsorg
- 2008:22 Rekryteringen av internationella studenter till svenska lärosäten
- 2008:23 Statens insatser för ett hållbart fiske
- 2008:24 Stöd till start av näringsverksamhet. Ett framgångsrikt program
- 2008:25 Kasernen Fastighetsaktiebolag
- 2008:26 Utanförskap och sysselsättningspolitik – regeringens redovisning
- 2008:27 Delpension för statligt anställda – tillämpning och effekter
- 2008:28 Skyddat arbete hos Samhall. Mer rehabilitering för pengarna
- 2008:29 Skyddet för farligt gods
- 2008:30 Tillämpningen av det finanspolitiska ramverket. Regeringens redovisning i budgetpropositionen för 2009
- 2008:31 Svenska trygghetssystem utomlands. Försäkringskassans och CSN:s utbetalningar och fordringshantering.

- 2009 2009:1 Omställningskrav i sjukförsäkringen – att pröva sjukas förmåga i annat arbete
- 2009:2 Försäkringskassans inköp av IT-lösningar
- 2009:3 Skatteuppskov. Regeringens redovisning av bostadsuppskov och pensionsavdrag
- 2009:4 Swedfund International AB och samhällsuppdraget
- 2009:5 En effektiv och transparent plan- och byggprocess? Exemplet buller
- 2009:6 Energideklarationer – få råd för pengarna
- 2009:7 Beslut om sjukpenning – har försäkringskassan tillräckliga underlag?
- 2009:8 Riksrevisorernas årliga rapport 2009
- 2009:9 Regeringens försäljning av V&S Vin & Sprit AB
- 2009:10 Psykiatrin och effektiviteten i det statliga stödet
- 2009:11 Försvarsmaktens personalförsörjning – med fokus på officersförsörjningen
- 2009:12 Hanteringen av unga lagöverträdare – en utdragen process
- 2009:13 Omställningskraven i arbetslöshetsförsäkringen
- 2009:14 Tillämpningen av den finanspolitiska ramverket. Regeringens redovisning i 2009 års ekonomiska vårproposition
- 2009:15 Sidas stöd till utveckling av kapacitet i mottagarländernas statsförvaltning
- 2009:16 Underhåll av belagda vägar
- 2009:17 Tillämpningen av det finanspolitiska ramverket. Regeringens redovisning i budgetpropositionen för 2010.
- 2009:18 IT-investeringar över gränserna

Beställning: publikationsservice@riksrevisionen.se