E-legitimationsnämnden och Svensk e-legitimation

Betänkande av Utredningen om bildande av en e-legitimationsnämnd

Stockholm 2010

STATENS OFFENTLIGA UTREDNINGAR
SOU 2010:104

SOU och Ds kan köpas från Fritzes kundtjänst. För remissutsändningar
av SOU och Ds svarar Fritzes Offentliga Publikationer på uppdrag av
Regeringskansliets förvaltningsavdelning.

Beställningsadress:
Fritzes kundtjänst
106 47 Stockholm
Orderfax: 08-598 191 91
Ordertel: 08-598 191 90
E-post: order.fritzes@nj.se
Internet: www.fritzes.se

Svara på remiss. Hur och varför. Statsrådsberedningen (SB PM 2003:2, reviderad 2009-05-02)
– En liten broschyr som underlättar arbetet för den som ska svara på remiss.
Broschyren är gratis och kan laddas ner eller beställas på
http://www.regeringen.se/remiss

Textbearbetning och layout har utförts av Regeringskansliet, FA/kommittéservice.

Tryckt av Elanders Sverige AB
Stockholm 2010

ISBN 978-91-38-23507-2
ISSN 0375-250X

Till statsrådet Anna-Karin Hatt

Regeringen beslutade den 17 juni 2010 (dir. 2010:69) att tillkalla en särskild utredare för att förbereda och genomföra bildandet av en nämndmyndighet för samordning av statens och kommunernas hantering av metoder och tjänster för elektronisk identifiering och signering (e-legitimationer).

Generaldirektören Stig Jönsson förordnades att vara särskild utredare från den 17 juni 2010. Dano Costouvsqi anställdes som utredningssekreterare från samma dag.

Utredningen har antagit namnet Utredningen om bildande av en e-legitimationsnämnd.

Utredningen överlämnade den 6 september 2010 promemorian *Instruktion för E-legitimationsnämnden – delredovisning I* och den 19 november 2010 promemorian *Verksamhetsplan för E-legitimationsnämnden – delredovisning II.*

Utredningen överlämnar härmed betänkandet *E-legitimationsnämnden och Svensk e-legitimation* (SOU 2010:104).

Uppdraget är härmed slutfört.

Stockholm i december 2010

Stig Jönsson

Innehåll

Bilagor

Sammanfattning

Dagens lösning för e-legitimationer fungerar relativt väl och i en internationell jämförelse är det förhållandevis många medborgare i Sverige som kan utföra legitimering och underskrift i en elektronisk miljö. Myndigheter, landsting och kommuner har också, i samverkan med utfärdarna av e-legitimationer, infört dialoger och användargränssnitt för e-legitimering som fungerar och en samsyn har vuxit fram kring bl.a. rätts- och administrativa frågor.

Dagens system har dock brister. Det finns ingen sammanhållen och enhetlig infrastruktur för identifiering vilket försvårar och förmodligen hämmar utvecklingen av e-tjänster. En samordnad infrastruktur för användning av e-legitimationer underlättar och förenklar för den offentliga sektorn och bör främja en utveckling av e-tjänster. Dagens modell är ett system som inte öppnar upp för möjliga nya aktörer att komma in på marknaden och därigenom bidra till en mångfald. Vidare bygger dagens modell för e-legitimationer på en upphandling som går ut per halvårsskiftet 2012 och som inte kan förlängas.

Den i utredningen föreslagna modellen för Svensk e-legitimation med en federation skapar en sådan sammanhållen och förenklad infrastruktur och bidrar till en fortsatt utveckling av e-legitimationer i Sverige på ett antal områden. Inom infrastrukturen för Svensk e-legitimation ska alla e-legitimationer som uppfyller uppställda krav kunna användas av medborgare och anställda i organisationer för åtkomst till förvaltningens e-tjänster. Utredningen beskriver i rapporten hur en sådan infrastruktur kan skapas och regleras. Syftet med infrastrukturen är inte att förhindra några idag existerande identitetslösningar utan att skapa förutsättningar, regelverk, m.m. för användning av existerande och tillkommande lösningar för identifiering. Vidare föreslås tjänster

för signering utanför området för den aktuella identitetslösningen. Detta möjliggörs genom ett enhetligt gränssnitt mot infrastrukturen för Svensk e-legitimation.

Regeringen har beslutat om inrättande av en E-legitimationsnämnd från årsskiftet. Den övergripande målsättningen med bildandet av en E-legitimationsnämnd är att skapa förutsättningar för en väl fungerande Svensk e-legitimation som kan skapa stark tillit till verksamheten såväl i Sverige som internationellt. Svensk e-legitimation ska möjliggöra för såväl användare som offentlig sektor att på ett effektivt sätt etablera och nyttja e-tjänster vilka kräver e-legitimationer och eller signering.

I förverkligandet av målbilden ingår att skapa en affärsmodell för Svensk e-legitimation som bygger på ett antal aktörer i samverkan – E-legitimationsnämnden, användare i form av privatpersoner och anställda i organisationer, identitetsutfärdare, e-tjänsteleverantörer samt attributsutfärdare.

Förvaltningens e-tjänsteleverantörer kommer i infrastrukturen att på ett förenklat sätt få tillgång till e-legitimationstjänster genom – E-legitimationsnämnden - vilket bland annat kommer att underlätta integration och hantering av tjänster.

Genom utredningens förslag skapas en infrastruktur för den offentliga sektorn. En viktig uppgift för E-legitimationsnämnden blir att verka för att en motsvarande och samverkande infrastruktur etableras även för den privata sektorn. Det är först då en sådan samverkande infrastruktur etablerats som Svensk E-legitimation kan användas för både offentliga och privata e-tjänster.

Attributsutfärdarna kommer som medlemmar i modellen spela en viktig roll som källa till kompletterande information.

Enligt förslaget ska infrastrukturen byggas med hjälp av flera samverkande regelverk, delvis inrättade genom författning, delvis skapade genom civilrättsliga avtal efter upphandling.

Med anledning av den bedömning som gjordes i *Instruktion för E-legitimationsnämnden – delredovisning I* (Fi 2010:05), att de av regeringen uppställda målen inte kan realiseras genom de upphandlingsförfaranden som anges i lagen (2007:1091) om offentlig upphandling, föreslås i utredningen att det inrättas en ny lag enligt vilken E-legitimationsnämnden får inrätta valfrihetssystem för Svensk e-legitimation. E-legitimationsnämnden ska fastställa reglerna för infrastrukturen men det är olika aktörer på

marknaden som ska ta fram och erbjuda identifieringstjänster och andra tjänster, t ex E-legitimationer. Det kan antas att det inom ramen för Svensk e-legitimation kommer att erbjudas olika alternativ av e-legitimationer och det är väsentligt att användarna får en valmöjlighet mellan olika alternativ. Utredningen föreslår därför att det inrättas ett valfrihetssystem baserat på reglerna i lagen (2008:962) om valfrihetssystem. Utredningen gör bedömningen att inrättandet av valfrihetssystemet ska anses vara en tilldelning av avtal genom tjänstekoncession.

I utredningen redovisas även ett förslag till regelverk för den föreslagna infrastrukturen. Regelverket avses styra parternas civilrättsliga mellanhavanden genom att föras in i de avtal som E-legitimationsnämnden ingår med dem som ansluts till infrastrukturen för Svensk e-legitimation. Regelverket specificerar villkoren för de olika tjänster som kommer att tillhandahållas.

Utredningen föreslår att en förordning om infrastrukturen för Svensk e-legitimation skapas. Förordningen syftar till att etablera infrastrukturen för svensk e-legitimation inom den offentliga förvaltningen och att samordna och förenkla e-tjänsteleverantörernas användning av funktioner för elektronisk legitimering och elektronisk underskrift. Förordningen ska bland annat definiera de centrala begrepp som används inom infrastrukturen.

En infrastruktur för identifiering bör ta sin utgångspunkt i ett tillitsramverk byggt på internationell standard och medge den flexibilitet som den föreslagna infrastrukturen för Svensk e-legitimation och internationell samverkan kräver. E-legitimationsnämnden bör vidare verka för att standardiseringsarbetet inom ISO/IEC leder till resultat som är förenliga med behoven inom den föreslagna infrastrukturen för identifiering. Om dessa resultat nås bör Sverige följa denna internationella standard. Vid en tillämpning av dessa internationella normer har det, såvitt hittills framkommit, visat sig ändamålsenligt att för Svensk e-legitimation kräva en tillitsnivå som motsvarar nivå 3 (AL3) eller högre, vilket också är den nivå som ligger närmast de av ramavtalsleverantörerna idag utgivna e-legitimationerna.

Som ett led i att skapa en långsiktig, hållbar och teknikneutral grund för identifiering har utredningen valt att inte reglera hur bärare skall utformas eller på annat sätt peka på någon särskild teknik för själva e-legitimationshandlingen, utan tar fasta på att

säkerställa att identifieringen sker på ett betryggande sätt. Abstraktionslagret med identitetsintyg gör det möjligt för e-legitimationsutfärdare att helt fritt utforma och utveckla lösningarna så länge de uppfyller säkerhetskraven i tillitsramverket.

E-legitimationsnämnden ska genom sin verksamhet skapa och utveckla modellen för Svensk e-legitimation baserat på följande utgångspunkter:

- att en affärs- och prismodell skapas som är enkel, transparent och långsiktig. Den ska leda till mer förutsägbara och om möjligt lägre kostnader än i dagens ramavtalsmodell
- att det ska vara enkelt för statlig myndighet, landsting eller kommun att få tillgång till tjänster för elektronisk identifiering och signering. En statlig myndighet, landsting eller kommun ska genom en part – E-legitimationsnämnden – få tillgång till alla tjänster som omfattas av modellen
- att en statlig myndighet, landsting eller kommun i så liten utsträckning som möjligt själv ska behöva ha kompetens och funktioner för att kunna använda tjänster för elektronisk identifiering och signering i verksamheten
- att modellen bör, om det med hänsyn till övriga förutsättningar är möjligt, stödja teknikneutralitet samt bygga på lösningar som utvecklas av marknaden. Befintliga e-legitimationer bör, eventuellt med viss anpassning för att klara vald tillitsnivå, fungera i den nya modellen
- att alla aktörer på marknaden som uppfyller relevanta krav ska kunna bli leverantörer i den nya modellen

Inom Svensk e-legitimation finns ett antal grundläggande tjänster, där vissa handlas upp och tillhandahålls via E-legitimationsnämnden och andra tillhandahålls från godkända medlemmar i modellen. Dessa tjänster kan indelas i följande grupper: registertjänster, e-legitimationer, anvisningstjänst, attributsintygstjänst och signeringstjänst. Det är fortfarande under utredning hur vissa av dessa tjänster ska utformas, val av teknisk lösning samt ifall de ingår i prismodellen som en bastjänst eller ifall en extra avgift kommer att utgå.

Verksamhetsplanen för E-legitimationsnämnden omfattar perioden 2011 till 2013 vilket motsvarar den period då nämndens

verksamhet samt infrastrukturen för Svensk e-legitimation ska byggas upp. Målsättningen är att under våren 2012, och senast per utgången av juni 2012 ha infrastrukturen för Svensk e-legitimation i drift. För att nå dit innefattar genomförandeplanen en lång rad aktiviteter där några av de mer väsentliga är författningsförändringar, inrättande av ett valfrihetssystem, framtagande av avtal, utveckling av teknisk infrastruktur och tjänster, uppdatering av affärsmodellen, inrättande av ett säkerhets- och tillitsramverk, genomförande av säkerhets- och andra kontroller samt detaljering av övergångsplan. Övergångsplanen är kritisk för att få en smidig övergång från nuvarande modell till den framtida modellen.

En annan viktig del i nämndens arbete är att genomföra ett stort antal samverkans- och förankringsaktiviteter med såväl offentliga som privata e-tjänsteleverantörer, identitetsutfärdare, attributsutfärdare samt andra viktiga intressenter för att på bästa sätt vidareutveckla och bygga önskad modell för e-legitimationer i Sverige.

Affärsmodellen för Svensk e-legitimation syftar till att skapa en modell som fungerar effektivt med nyttor och incitament för aktörerna. Det är vidare viktigt att modellen är utvecklingsbar och kan anpassas efter nya förutsättningar.

Den prismodell som tagits fram som en del av affärsmodellen har utgått ifrån att den totala ersättningen till identitetsutfärdarna bör motsvara nuvarande marknadsstorlek i initialskedet. Tillväxten i marknaden förväntas ske genom att ytterligare myndigheter, landsting och kommuner ansluter sig till systemet. E-tjänsteleverantörernas avgifter ska vara förutsebara, överskådliga och därmed enkla att budgetera. De kostnader som nämnden har som är direkt relaterade till drift av Svensk e-legitimation bör på sikt finansieras via avgifter. Den viktigaste källan till finansiering i modellen utgörs av fasta årsavgifter som betalas av e-tjänsteleverantörerna till E-legitimationsnämnden. Huvuddelen av dessa avgifter betalas därefter ut till identitetsutfärdarna utifrån prestation mätt som respektive aktörs marknadsandel i modellen, beräknat som antal utfärdade identitetsintyg per unik användare och tidsenhet, jämfört med totala antalet utfärdare intyg. Därtill kommer såväl identitetsutfärdare som attributsutfärdare att betala en årlig avgift för att täcka administrativa kostnader och tillsyn. Identitetsutfärdarna fastställer själva inom ramen för regelverket villkoren för utfärdandet av e-legitimationer och dessa villkor kan innefatta en anskaffningsavgift för användaren.

Svensk e-legitimation ska kunna utfärdas såväl till en medborgare – s.k. *privat e-legitimation* – som till anställda eller uppdragstagare – s.k. *e-tjänstelegitimation*. Medan användaren själv får anskaffa privat e-legitimation är det arbets- eller uppdragsgivaren som ansöker om och tilldelar den anställde en e-tjänstelegitimation. E-tjänstelegitimationerna ligger inom regelverket men utanför valfrihetssystemet och är inte ersättningsgrundande i affärsmodellen.

E-legitimationsnämnden föreslås i utredningen initialt bemannas med fyra årsarbetskrafter. Under de första åren då Svensk e-legitimation ska etableras och infrastrukturen utvecklas kommer visst projektarbete krävas, vilket bör kunna hanteras med hjälp av externa resurser. Drift och förvaltning av infrastrukturen för Svensk e-legitimation föreslås upphandlas på marknaden.

E-legitimationsnämnden kommer under en inledande uppbyggnadsperiod behöva anslagsstöd för att finansiera verksamheten. Hur lång denna period blir är beroende av i vilken takt nuvarande e-tjänsteleverantörer väljer att anslutas till Svensk e-legitimation. Vid 100% anslutning av nuvarande aktörer i samband med lanseringen 2011 beräknas täckning för nämndens kostnader direkt relaterade till drift av Svensk e-legitimation kunna uppnås 2014. Även om detta scenario ej kan uppnås bör det på sikt när verksamheten nått ett normaltillstånd vara möjligt att finansiera den operativa delen av verksamheten via avgifter. Visst utvecklingsarbete, omvärldsbevakning, internationella relationer och liknande bedöms även fortsatt behöva finansieras via anslag.

Som framgår av betänkandet har utredningen valt att ta ställning till flera svåra frågor och med relativt hög detaljeringsgrad för att tydliggöra områdets komplexitet och bredd och för att få igång en aktiv dialog kring frågeställningarna.

Nämnden tar nu vid där utredningen slutar. Det ligger i sakens natur att fortsatt dialog och djupare analys kommer att kunna resultera i modifieringar av olika slag.

Författningsförslag

1.1 Förslag till lag om valfrihet för Svensk e-legitimation

Härigenom föreskrivs följande.

1 § E-legitimationsnämnden får besluta att tillhandahålla valfrihetssystem för tjänster som upphandlas för elektronisk identifiering.

Med valfrihetssystem menas ett förfarande där användaren har rätt att välja den leverantör som ska utföra tjänsten och som E-legitimationsnämnden godkänt och tecknat kontrakt med.

2 § När E-legitimationsnämnden tillhandahåller valfrihetssystem enligt denna lag ska myndigheten tillämpa lagen (2008:962) om valfrihetssystem. I stället för det som sägs i 2 kap. 3 § första meningen, 6 och 7 §§ lagen om valfrihetssystem ska med

1. leverantör menas den som på marknaden tillhandahåller tjänster som nämns i 1 §,
2. tjänst menas sådan tjänst som nämns i 1 §, och
3. upphandlande myndighet menas E-legitimationsnämnden.

E-legitimationsnämnden ska dock inte tillämpa 9 kap. 2 § lagen om valfrihetssystem när nämnden tillhandahåller valfrihetssystem enligt denna lag.

3 § En kommun eller ett landsting får uppdra åt E-legitimationsnämnden att på kommunens eller landstingets vägnar besluta om godkännande av sökande och ingående av kontrakt enligt denna lag eller på annat sätt genomföra och avsluta ett inrättande eller en förändring av ett valfrihetssystem enligt denna lag.

Denna lag träder i kraft den [ ] 2011

1 Utredningens uppdrag och arbete

1.1 Utredningens uppdrag

Regeringen beslutade den 17 juni 2010 att tillkalla en särskild utredare för att förbereda och genomföra bildandet av en nämndmyndighet för samordning av statens och kommunernas hantering av metoder och tjänster för elektronisk identifiering och signering (e-legitimationer). Utredningens uppdrag framgår av kommittédirektivet (dir. 2010:69), se *bilaga 1*.

Utredningen har antagit namnet Utredningen om bildande av en e-legitimationsnämnd.

Utredningen har enligt direktivet i sin första delredovisning den 6 september 2010 lämnat förslag till en instruktion för E-legitimationsnämnden. Den 19 november 2010 har utredningen lämnat förslag till E-legitimationsnämndens verksamhetsmål och verksamhetsplan för 2011-2013 jämte en beskrivning av en ny nationell e-legitimationsmodell benämnd *Svensk e-legitimation*.

Regeringen har beslutat om förordning med instruktion för E-legitimationsnämnden, se *bilaga 2*, och förordnade av nämndens ledamöter, se *bilaga 3*.

I detta betänkande, *E-legitimationsnämnden och Svensk e-legitimation*, finns utredningens författningsförslag om ett nytt valfrihetssystem samt uppdaterade förslag och beskrivningar av verksamhetsplan för E-legitimationsnämnden och Svensk e-legitimation.

Uppdraget är härigenom avslutat.

1.2 Utredningens arbete

Utredningen inledde sitt arbete i mitten av juni 2010. Utredningen har i olika omfattning haft samråd med Sveriges Kommuner och Landsting och de myndigheter som ingår i E-delegationen – inklusive dess arbetsgrupp och Roland Höglund – samt med Datainspektionen, Post- och telestyrelsen, Datainspektionen och Domstolsveket. Därtill har utredningen haft samråd med Apotekens Service AB, Kommunförbundet Stockholms län, CEHIS och .SE.

Utredningen har haft tre samrådsmöten med de leverantörer som omfattas av ramavtal Elektronisk identifiering (eID) 2008 och två möten med s.k. infratjänstleverantörer. Vidare har utredningen tillsammans med Ingenjörsvetenskapsakademien, IVA, anordnat ett näringslivsseminarium med ett åttiotal deltagare. Utredningen har medverkat i två informationsmöten som Dataföreningen har anordnat samt som föredragshållare på BankID-dagen. Utredningen har varit på studiebesök hos Difi (Direktoratet for forvaltning og IKT) i Norge och utredningssekreteraren har deltagit i internationella konferenser om e-legitimationer i Tallinn och Aten.

Utredningen har gett Setterwalls Advokatbyrå och Capgemini Sverige AB (som i sin tur anlitat underkonsulterna 3xA Security AB, Certezza AB och Kirei AB) i uppdrag att bistå utredningen med att ta fram förslag till en ny nationell modell för elektronisk identifiering och signering (e-legitimationer). Leif Johansson, Sunet, har bistått konsultgruppen i deras arbete. I uppdraget har ingått att ta fram förslag till den nya E-legitimationsnämndens verksamhetsplan, finansieringsform (affärs- och prismodell) och mål för verksamheten samt kravspecifikationer, föreskrifter, avtal och annat underlag som behövs för att den nya e-legitimationsmodellen ska kunna genomföras i sin helhet av den nybildade nämnden.

Utredningen har tagit fram begrepp och definitioner avseende Svensk e-legitimation, se *bilaga 4.*

2 E-legitimationer i Sverige – bakgrund

2.1 Dagens modell

I takt med att medborgarna blivit allt mer kunniga användare av Internet har utvecklingen i Sverige tagit ett nytt steg mot tydliga och standardiserade förutsättningar för e-tjänster. Verksamhetsutvecklingen bygger i dag på samlad kunskap hos individer, organisationer, företag och den offentliga förvaltningen som kan komplettera varandra. Målet för verksamhetsutvecklingen är inte längre att bara öka den interna nyttan eller nyttan för användare av e-tjänsterna utan att skapa största möjliga totala nytta för samhället i samverkan med andra aktörer.[1]

Ett stort antal myndigheter, landsting och kommuner tillhandahåller i dag e-tjänster som kräver en säker elektronisk identifiering. Utöver identifiering behövs också metoder för att säkert signera handlingar elektroniskt inom vissa områden för att kunna vidareutveckla e-tjänster i förvaltning och infrastruktur. Dagens användande varierar stort mellan olika organisationer varför det fortsatt förväntas finnas potential för tillväxt i marknaden.

2.2 Begränsningar i nuvarande modell

Dagens modell för e-legitimation anses relativt framgångsrik och svensk e-förvaltning har betraktats som en av de främsta i världen. Många medborgare i Sverige om kan utföra legitimering och underskrift i en elektronisk miljö. Myndigheter, landsting och kommuner har också, i samverkan med utfärdarna av e-legitimationer, infört dialoger och användargränssnitt för e-legitimering

[1] Strategi för myndigheternas arbete med e-förvaltning, 2009.

som fungerar och en samsyn har vuxit fram kring bl.a. rätts- och administrativa frågor.

Samtidigt finns brister i dagens system. Det finns ingen sammanhållen och enhetlig infrastruktur för identifiering vilket försvårar och förmodligen hämmar utvecklingen av e-tjänster inom den offentliga sektorn. En samordnad infrastruktur för användning av e-legitimationer skulle underlätta och förenkla för den offentliga sektorn och främja utvecklingen av e-tjänster. Dagens modell är inte öppen för möjliga nya aktörer att komma in på marknaden och därigenom bidra till en mångfald. Vidare bygger dagens modell för e-legitimationer på en upphandling som går ut per halvårsskiftet 1012 och som inte kan förlängas.

Dagens användning av metoder för identifiering och signering bygger på ramavtalsupphandlingar, genomförda av Kammarkollegiet, från vilka statliga myndigheter och kommuner kan göra avrop. Nuvarande avtal för elektronisk identifiering har blivit förlängt till juni 2012 och avrop kan gälla under fyra år. Som längst kan ett avrop från gällande avtal därför gälla till 30 juni 2016. Myndigheter, landsting och kommuner har hittills även kunnat avropa förmedling av spärrkontrollfråga till rätt utfärdare via Infratjänsten, vilket nu upphört och ersatts av ramavtalet för E-förvaltningsstödjande tjänster.[2] En viktig drivkraft till en översyn av den svenska modellen för e-legitimationer är att förutsättningarna förändrats så att den form för upphandling som tidigare använts inte kan användas på nytt för att få flera leverantörer av dessa tjänster. En ny lösning behöver därför tas fram.

[2] <www.avropa.se>.

3 En ny nationell modell för e-legitimationer

I detta avsnitt beskrivs utgångspunkterna för en ny nationell modell för e-legitimationer. Denna modell kan beskrivas som en infrastruktur som består av de e-legitimationer som godtas, en standardiserad lösning för identifiering, signering samt de aktörer som utför dessa uppgifter. E-legitimationsnämndens föreslagna framtida uppgifter beskrivs, en genomgång görs även av övriga aktörer i modellen identitetsutfärdare, e-tjänsteleverantörer och attributsutfärdare. I tillägg beskrivs de huvudsakliga tjänsterna dvs. anvisningstjänst, signeringstjänst samt attributstjänst.

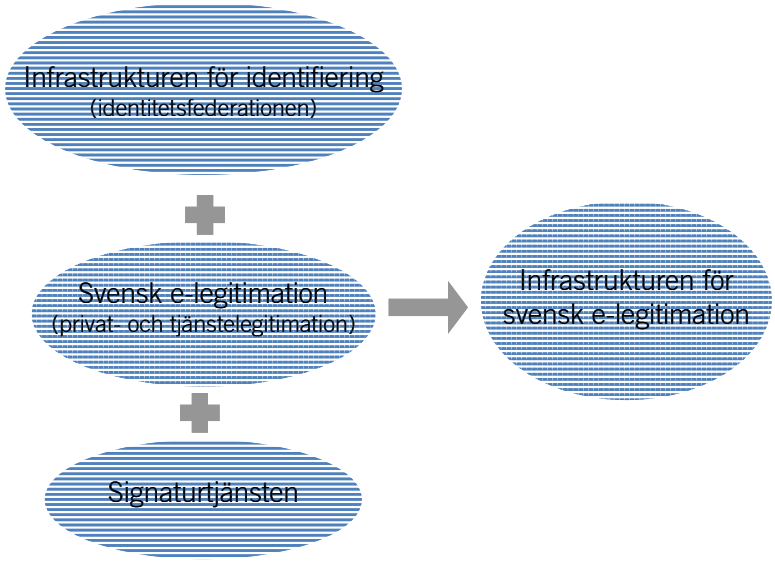
3.1 Utgångspunkter

Frågan om hur elektronisk identifiering och elektroniska underskrifter kan utvecklas och anpassas till framtida behov har varit föremål för utredning i flera olika sammanhang.[1] Frågan berördes senast i utredningens promemoria den 6 september 2010, med en delredovisning till regeringen, där en förordning med instruktion för E-legitimationsnämnden har föreslagits. E-legitimationsnämnden ska enligt förslaget samordna statens arbete med och användning av metoder och tjänster för elektronisk identifiering och signering samt säkerställa att nödvändiga tjänster och funktioner för e-legitimationer finns tillgängliga för den offentliga förvaltningen.

[1] Se bl.a. E-delegationen som i sitt delbetänkande *Strategi för myndigheternas arbete med e-förvaltning* (SOU 2009:86) lämnat förslag till hur förvaltningens framtida arbete med e-legitimationer kan organiseras. Delegationens förslag har sin utgångspunkt i förslag som redovisats i en rapport från dåvarande Verket för förvaltningsutveckling, Verva, *Slutrapport om säkert elektroniskt informationsutbyte och säker hantering av elektroniska handlingar* (Rapport 2008:12).

Utredningen har utarbetat ett förslag till en ny nationell modell för att använda e-legitimationer. Denna modell kan beskrivas som en infrastruktur (”Infrastrukturen för Svensk e-legitimation”), som består av de e-legitimationer som godtas (”Svensk e-legitimation”), en standardiserad lösning för identifiering, i tekniska sammanhang kallad identitetsfederation (”Infrastrukturen för identifiering”), en tjänst för att underlätta för den som tillhandahåller en e-tjänst att införa funktioner för elektroniska underskrifter (”Signaturtjänsten”) och ett regelverk för denna infrastruktur; se figuren nedan.

Figur 3.1 Infrastrukturen för Svensk e-legitimation



Denna modell behöver fungera från upphandlings- och konkurrensrättsliga utgångspunkter samtidigt som andra frågor – såväl juridiska som tekniska och affärsmässiga – måste lösas och formas till en helhet.

Dessa komplexa samband mellan teknik, juridik och affärsmodell gör det till en utmaning att beskriva Infrastrukturen för Svensk e-legitimation så att alla berörda yrkeskategorier får en rättvisande bild av lösningen som helhet. Ett mål är emellertid att förenkla genom att komplexiteten hanteras dels av E-legi-

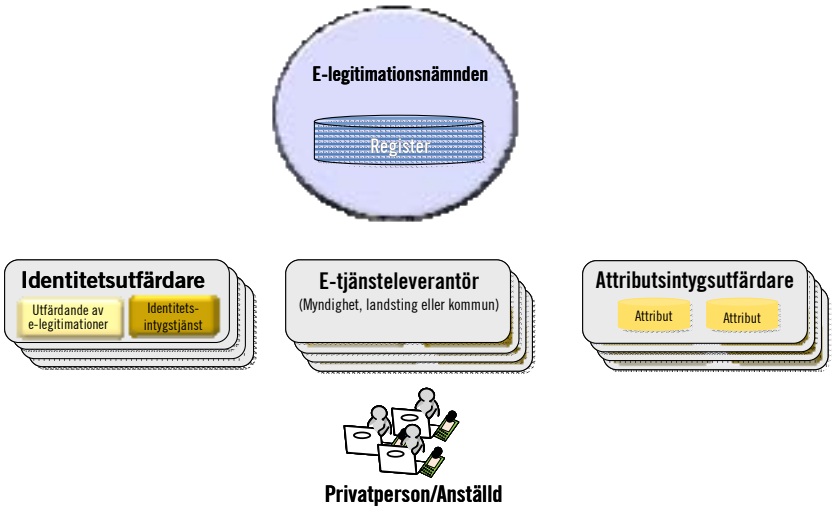
timationsnämnden, som utarbetar och inför lösningar såväl tekniskt som juridiskt, dels av s.k. Identitetsutfärdare, så att myndigheter och företag som tillhandahåller e-tjänster endast behöver hantera intyg om redan utförd identifiering eller äkthetskontroll.

Utredningen har tagit fram tekniska specifikationer för infrastrukturen för Svensk e-legitimation som redovisas i utredningens bilagor (*bilagorna 11–17*). I det följande ska den föreslagna lösningen beskrivas närmare.

3.2 Aktörer inom Infrastrukturen för Svensk e-legitimation

De aktörer som ingår i Infrastrukturen för Svensk e-legitimation redovisas något förenklat i följande figur.

Figur 3.2 Aktörer i Svensk e-legitimation



E-legitimationsnämnden ska enligt föreskrifter i förordning, som framgått, samordna statens arbete med och användning av metoder och tjänster för elektronisk identifiering och signering samt säkerställa att nödvändiga tjänster och funktioner för e-legitimationer finns tillgängliga för den offentliga förvaltningen. Denna *Infrastruktur för Svensk e-legitimation* bärs upp av privaträttsliga

aktörer som utfärdar e-legitimationer och tillhandahåller tjänster över tiden, däribland identitetsintyg, så att de utfärdade e-legitimationerna smidigt kan nyttjas. Dessa s.k. *identitetsutfärdare* utfärdar intyg när en innehavare av en e-legitimation, *användaren*, legitimerat sig med stöd av sin e-legitimation. Intygen utfärdas åt myndigheter och vissa därmed jämställda organ inom offentlig sektor, s.k. *e-tjänsteleverantörer*, efter att identitetsutfärdaren utfört vissa kontroller. Identitetsintygen ska härvid ses som en del i användningen av e-legitimationer och inte som en självständig tjänst.

Tanken är att de e-legitimationer (kallade Svensk e-legitimation) som uppfyller kraven och har anslutits till Infrastrukturen för Svensk e-legitimation ska få användas inte bara i myndigheters e-tjänster utan även ska kunna brukas hos aktörer utanför offentlig sektor. E-legitimationsnämnden ska verka för och stödja en sådan utveckling. Det är emellertid inte en uppgift för nämnden att anskaffa tjänster för kontroll av e-legitimationer åt företag eller andra privaträttsliga subjekt som tillhandahåller en e-tjänst. Detta ska emellertid inte hindra att en användare brukar samma e-legitimation hos privaträttsliga e-tjänsteleverantörer, som i myndigheters e-tjänster.

Svensk e-legitimation ska vidare kunna utfärdas till såväl en medborgare eller någon annan i egenskap av privatperson – s.k. *privat e-legitimation* – som till anställda eller uppdragstagare – s.k. *e-tjänstelegitimation*. Medan användaren själv får anskaffa privat e-legitimation är det arbets- eller uppdragsgivaren som ansöker om och tilldelar den anställde en e-tjänstelegitimation.

Det ska dessutom finnas en typ av intyg – s.k. *attributsintyg* – som utfärdas av en *attribututfärdare* som även kan vara en identitetsintygsutfärdare. Det kan vara fråga om sådana attribut som t.ex. *juridisk behörighet* att agera för en juridisk persons räkning i egenskap av ställföreträdare eller fullmäktig, en roll av juridisk betydelse såsom lärare, läkare eller sjuksköterska eller någon annan uppgift av betydelse om en individ, t.ex. uppgift om anställning inom visst företag eller visst uppdrag för en angiven huvudman.

På ett övergripande plan kan den planerade Infrastrukturen för Svensk e-legitimation sägas innefatta att

1. utfärda, använda, verifiera och spärra Svenska e-legitimationer,

2. tillhandahålla en Infrastruktur för identifiering där
    a) e-tjänsteleverantörer kan erhålla identitets- och attributsintyg för att granska om uppgifter som lämnats om identitet eller juridisk behörighet eller andra attribut är riktiga,
    b) ett centralt register över aktörer förmedlar uppgifter om aktörernas tjänster och funktioner för tillit och säkert informationsutbyte,
    c) en anvisningstjänst som kan ge användaren av en e-tjänst hjälp att välja e-legitimation att bruka i e-tjänsten,
3. tillhandahålla en signeringstjänst som gör det möjligt för användaren att skriva under handlingar elektroniskt.

Denna infrastruktur syftar till att etablera funktioner för e-legitimationer, elektroniska underskrifter och identitets- och attributsintyg, som ska vara enkla att förstå och bruka för användare av e-legitimationer och e-tjänsteleverantörer, samtidigt som infrastrukturen på ett balanserat sätt ska kunna tillgodose skyddet för rättssäkerheten, informationssäkerheten och enskildas personliga integritet.

3.3 E-legitimationsnämndens uppgifter

E-legitimationsnämnden ska styra, utveckla och svara för verksamheten inom infrastrukturen för Svensk e-legitimation, bl.a. utarbeta *föreskrifter* för Svensk e-legitimation och *avtal och allmänna villkor* i de delar som ska regleras genom civilrättsliga överenskommelser. Nämnden ska också utarbeta *riktlinjer och vägledningar* för Svensk e-legitimation och dokumentation av tekniska krav för den gemensamma infrastrukturen. Hit hör bl.a. specifikationer av tillitsnivå och tekniska lösningar för Svensk e-legitimation.

E-legitimationsnämnden ska också *upphandla en leverantör av tekniska tjänster* för bl.a. drift och underhåll av *utfärdar- och e-tjänsteregister* – i tekniska sammanhang kallade metadata – och *inrätta* ett *valfrihetssystem* för Svensk e-legitimation.

Utfärdar- och e-tjänsteregistren skapar tillit mellan de identitetsutfärdare, attributsutfärdare och e-tjänsteleverantörer som ska ingå i Infrastrukturen för identifiering; i tekniska samman-

hang kallad identitetsfederationen. Där publiceras vissa uppgifter om varje aktör – identitetsutfärdare, attributsutfärdare och e-tjänsteleverantör – så att de kan kommunicera på ett säkert sätt och kan kontrollera att identitets- och attributsintyg är äkta.[2] I utfärdar- och e-tjänsteregistren finns också uppgifter om Internet-adresser till samtliga tjänster och e-tjänsteleverantörer, vilka attribut som kan tillhandahållas samt vilka attribut respektive e-tjänsteleverantör behöver för sina kontroller. Alla aktörer får därmed veta vilken information som ska tillhandahållas och vart den ska sändas.

I dessa register, som i tekniska sammanhang kallas metadata och något förenklat kan beskrivas genom en jämförelse med domännamnssystemet och det domännamnsregister som .SE tillhandahåller, är det inte meningen att personuppgifter ska registreras utan endast uppgifter om identitetsutfärdare, attributsutfärdare och e-tjänsteleverantörer (dvs. juridiska personer).[3]

Attributsutfärdare av allmänt intresse kan registreras i E-legitimationsnämndens utfärdarregister, t.ex. Bolagsverket. Beträffande övriga attributsutfärdare får berörda e-tjänsteleverantörer emellertid se till att skapa en egen tillit eftersom denna attributshantering inte sker inom den av E-legitimationsnämnden samordnade infrastrukturen för Svensk e-legitimation. Denna attributshantering kräver alltså särskilda affärsmässiga och juridiska anpassningar utanför Infrastrukturen för identifiering.

Uppgifterna i *utfärdarregistret* ska vara offentligt tillgängliga; jfr hur uppgifterna i aktiebolagsregistret och domännamnsregistret är tillgängliga för var och en via Internet. För uppgifter om e-tjänsteleverantörer behövs två typer av e-tjänsteregister, en där leverantörer inom offentlig sektor registreras och en där e-tjänsteleverantörer som är företag kan registreras. De senare behövs emellertid inte för att offentlig sektor ska kunna tillhandahålla e-tjänster inom Infrastrukturen för Svensk e-legitimation. Näringslivets e-tjänsteleverantörer behöver emellertid ha tillgång till samma register över utfärdare. E-legitimationsnämnden ska därför svara för de två första registren men inte för det där näringslivets e-tjänsteleverantörer registreras. E-legitimationsnämnden ska se till att utfärdarregistret blir tillgängligt även för näringslivet och

[2] Alternativet – att alla aktörer skapar tillit sinsemellan – är inte realistiskt. I så fall kan en identitetsfederation endast skapas för en handfull parter och därmed inte uppfylla direktivets krav på utvecklingsmöjligheter.
[3] Jfr lagen (2006:24) om nationella toppdomäner för Sverige på Internet.

att ett tillförlitligt kompletterande register för näringslivets e-tjänsteleverantörer regleras på lämpligt sätt.

E-legitimationsnämnden avser dessutom att verka för att en modell som kan hantera svenskt näringslivs behov etableras, vidare beskrivet i avsnitt 10.

Till E-legitimationsnämndens uppgifter hör att

1. *utarbeta* underlag till föreskrifter för Infrastrukturen för Svensk e-legitimation, avtal och allmänna villkor i de delar Infrastrukturen för Svensk e-legitimation regleras genom civilrättsliga överenskommelser samt riktlinjer, vägledningar, dokumentation och tekniska krav för Infrastrukturen för Svensk e-legitimation,
2. *meddela föreskrifter* inom ramen för den normgivningskompetens som delegeras till nämnden,
3. *upphandla leverantörer* av tekniska tjänster för Infrastrukturen för Svensk e-legitimation,
4. *sluta avtal* med aktörer inom Infrastrukturen för Svensk e-legitimation,
5. *inrätta en Infrastruktur för identifiering* inom ramen för Infrastrukturen för Svensk e-legitimation, och för denna infrastruktur
   a) inrätta ett valfrihetssystem för Svensk e-legitimation,
   b) ange de tekniska och andra krav som ställs på de e-legitimationer som ska få anslutas, bl.a. beträffande tillitsnivåer, och utöva tillsyn.

3.4 Identitetsutfärdare

De identitetsutfärdare som ansluts till Infrastrukturen för Svensk e-legitimation ska utfärda dels e-legitimationer till medborgare, anställda och uppdragstagare, dels identitetsintyg till e-tjänsteleverantörer inom offentlig sektor. Som framgått är avsikten att alla utfärdare som når upp till de krav som ställs för deltagande i Infrastrukturen Svensk e-legitimation ska ha rätt att bli anslutna. Den som ansluts ska tillhandahålla identitetsintyg, i egen regi eller genom någon annan aktör som uppfyller de krav som nämnden ställer. I juridisk mening ska emellertid en ansluten utfärdare

ansvara för både de e-legitimationer och de identitetsintyg som denne tillhandahåller. I praktiken kan inte uteslutas att en myndighet eller ett offentligt ägt bolag blir utfärdare av e-tjänstelegitimationer och identitetsintyg, vilket behöver utredas vidare.

Tanken är alltså att utfärdaren av den e-legitimation som brukas och utfärdaren av ett identitetsintyg till följd av brukandet ska vara samma part. En utfärdare kan visserligen anlita en underleverantör för att ställa ut och hantera e-legitimationer, identitetsintyg eller anknytande funktioner men utfärdaren ska – såvitt är av betydelse för ett lämnat intyg – svara för dessa funktioner som om Identitetsutfärdaren själv hade ställt ut e-legitimation och identitetsintyg och hanterat anknytande funktioner. En sådan stark koppling är naturlig eftersom utfärdandet av identitetsintyg ska ses som en del i nyttjandet av e-legitimationer och inte som en självständig fristående tjänst.

Om en identitetsutfärdare inte kan leverera alla de uppgifter som en e-tjänsteleverantör behöver ska kompletterande uppgifter kunna begäras från och lämnas av en attributsutfärdare i form av ett attributsintyg.

Identitetsutfärdarens relation till användaren

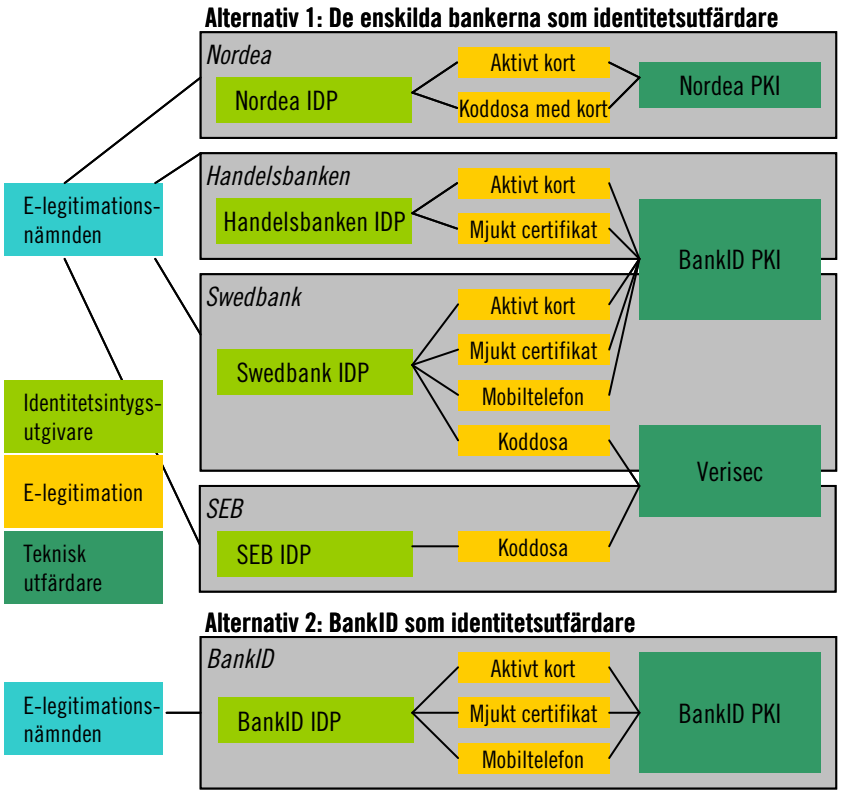
En användare som ska identifiera sig väljer via anvisningstjänsten vilken identitetsutfärdare som ska brukas. Identifiering sker sedan direkt mellan användaren och den valda identitetsutfärdaren. Detta är därför viktigt att identitetsutfärdaren är en part som användaren känner igen och har en direkt relation till, t.ex. som kund, medlem eller anställd. Detta är särskilt viktigt att beakta i de fall där själva bäraren av e-legitimationen utfärdas av någon annan, t ex en underleverantör till identitetsutfärdaren, en part som inte nödvändigtvis användaren har en relation till.

Bankerna som identitetsutfärdare

De banker som i dag utfärdar e-legitimationer inom ramen för BankID-samarbetet kan, förutsatt att kraven för Svensk e-legitimation uppfylls, anslutas som identitetsutfärdare var för sig eller gemensamt. Vilken av dessa anslutningsformer som är lämplig beror på de affärsmässiga och juridiska bedömningar som aktörerna

gör. Bland de exempel som varit föremål för diskussion finns de som översiktligt återges i följande figur.

Figur 3.3 Bankerna som identitetsutfärdare, exempel



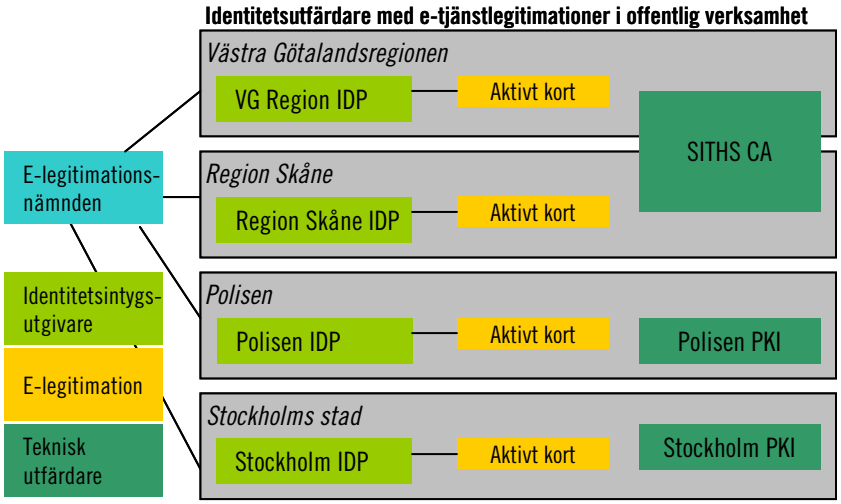
Utfärdare av e-tjänstelegitimationer i offentlig verksamhet

För anställda inom ett landsting bör landstinget själv vara identitetsutfärdare, förutsatt att de uppfyller kraven för Svensk E-legitimation, då det är landstingen som av den anställde uppfattas som utfärdare av tjänstekortet (SITHS[4].). Att det rent tekniskt är en underleverantör (TeliaSonera AB) till ett av landstingen

[4] SITHS är ett smart kort för elektronisk identifiering. Alla medarbetare i till exempel kommuner, landsting och eller privata vårdgivare kan använda den här elektroniska tjänstelegitimationen.

gemensamt ägt bolag (Inera AB) som utfärdat e-legitimationen bör alltså ses som sekundärt. Motsvarande synsätt bör tillämpas även för annan offentlig verksamhet. Se vidare bilden nedan.

Figur 3.4 Utfärdare av e-tjänstelegitimation i offentlig verksamhet, exempel



3.5 E-tjänsteleverantörer inom offentlig sektor

E-tjänsteleverantörerna behöver inte – jämfört med dagens lösningar – införa funktioner för att kontrollera om en legitimering är riktig eller om en underskrift är äkta. Detta blir av stor betydelse eftersom sådana kontroller i dag utförs av e-tjänsteleverantörerna – ofta genom underleverantör – enligt flera olika tekniska lösningar och förutsätter att varje myndighet, som tillhandahåller e-tjänster som kräver e-legitimation, för sig sluter avtal med flera olika leverantörer.

I en identitetsfederation gör det ingen skillnad för e-tjänsteleverantören om det är en, två eller hundra identitetsutfärdare. E-tjänsteleverantörens e-tjänst blir inte längre en del av processen för att kontrollera den använda e-legitimationen och resultatet av de tekniska procedurerna för elektronisk legitimering och underskrift. E-tjänsteleverantören behöver i praktiken endast lämna fullmakt till E-legitimationsnämnden, som hanterar erforderliga avtalsslut, och ha förmågan att tolka intyg i enlighet med den standardiserade

lösningen för att hantera identitetsintyg vilken här betecknas Infrastrukturen för identifiering (federationen).

Merparten av dagens e-tjänsteleverantörer har redan i dag förmågan att tolka identitets- och attributsintyg och behöver endast till E-legitimationsnämnden ange sina behov av identitetsinformation och attribut.

3.6 En anvisningstjänst

En anvisningstjänst ska införas för att, i samband med användarens utnyttjande av e-tjänster, underlätta användarens val av e-legitimation.

En viktig funktion i en anvisningstjänst är att hantera information om användarens tidigare val av e-legitimation så att användaren vid nästa tillfälle får upp sina tidigare val som förval. Uppgifter om tidigare val lagras i användarens webbläsare som en s.k. ”cookie” som returneras av användarens webbläsare till anvisningstjänsten vid återkommande besök.

Även anvisningstjänsten föreslås som två alternativa tjänster. Det första alternativet medger en enklare integration för e-tjänsteleverantörerna i deras e-tjänster medan det andra utförandet möjliggör mera avancerade och användarvänliga gränssnitt för e-tjänsternas användare.

Inför e-tjänsteleverantören det första alternativet överförs användaren till anvisningstjänsten som tillhandahåller gränssnitt för användarens val av e-legitimation. Anvisningstjänsten anpassar gränssnittet med stöd av tillgänglig information om användarens tidigare val av e-legitimation. När användaren gjort sitt val av e-legitimation överförs användaren, tillbaka till e-tjänsten, med information om vilken identitetsutfärdare användaren vill använda för att legitimera sig.

Om e-tjänsteleverantören inför det andra alternativet kan denne föra in ett eget gränssnitt gentemot användaren som innehåller instruktioner till dennes webbläsare om att hämta hem relevant anvisningsinformation från anvisningstjänsten. De uppgifter som returneras från anvisningstjänsten anpassas utifrån den information som finns tillgänglig om användarens tidigare val av e-legitimation och om vilka behov av legitimering som föreligger i e-tjänsten. Användaren upplever sig – vid den dialog som sker för att välja e-legitimation – aldrig lämna e-tjänsten och genom det dynamiskt an-

passade gränssnittet lämnas information till e-tjänsten om vilken identitetsutfärdare som kan identifiera användaren.

Det senare alternativet kräver instruktioner i e-tjänstens webbgränssnitt mot användare, som utformats så att de på ett korrekt sätt hämtar och använder information från anvisningstjänsten. Samtidigt ger det senare alternativet emellertid användaren en upplevelse av att hela tiden kommunicera endast med e-tjänsten. Införs det första alternativet blir det däremot påtagligt för användaren att han eller hon överförs till en separat tjänst för valet av e-legitimation. De tekniska lösningarna specificeras närmare i *bilaga 16*.

Vi återkommer till anvisningstjänsten i avsnittet om regelverk för den föreslagna infrastrukturen.

3.7 En signeringstjänst

För att den beskrivna infrastrukturen ska bli fullständig behövs även en central tjänst för elektroniska underskrifter (signeringstjänst). Denna bör om möjligt utformas dels så att kvalificerade certifikat utfärdas momentant, dels så att en säker anordning för signaturframställning tillhandahålls så att de elektroniska underskrifterna kan anses vara kvalificerade.

Tanken är att Infrastrukturen för Svensk e-legitimation ska kunna innefatta nya typer av e-legitimationer såsom koddosor och liknande, vilka inte faller inom ramen för en sådan publik nyckelstruktur som dagens användning av e-legitimationer förutsätter. Sådana nya typer av e-legitimationer kan inte i sig användas för att förse en handling med en avancerad elektronisk signatur enligt 2 § lagen (2000:832) om kvalificerade elektroniska signaturer (signaturlagen) och sådana e-legitimationer kan inte heller brukas för underskrifter med vanligt förekommande och allmänt accepterade format. I vissa länder, exempelvis Norge, har därför en signeringsfunktion införts som en central tjänst där elektroniskt undertecknande inte gjorts beroende av hur användarens e-legitimation är utformad. Till sådana tillämpningar har dessutom knutits anordningar för signaturframställning som utfärdaren betecknat som säker i signaturdirektivets mening.

Det är centralt för en svensk lösning att signaturlagens krav uppfylls. Den elektroniska underskriften ska ha skapats med medel som endast användaren kontrollerar, dvs. som användaren

kontrollerar så att den inte kan kopieras eller annars missbrukas av en obehörig utan att detta upptäcks. För att tillgodose detta krav får användaren legitimera sig med sin e-legitimation varje gång som han eller hon ska skriva under elektroniskt med stöd av signeringstjänsten. Denna tjänst måste dessutom ha sådana skydd mot förfalskningar och andra manipulationer att tjänsten åtnjuter såväl allmänhetens som myndigheternas förtroende.

Den föreslagna Infrastrukturen för identifiering – där nya typer av e-legitimationer kan ingå – bör därmed förenas med en signaturtjänst så att Infrastrukturen för Svensk e-legitimation innefattar motsvarande möjligheter till elektronisk underskrift som i dagens system. Här föreslås emellertid två alternativa tjänster och tanken är att de ska kunna tillhandahållas var för sig eller i kombination, utifrån e-tjänsteleverantörens behov och riskbedömning.

Det första alternativet har utformats så att en e-tjänsteleverantör med minsta möjliga integrationsarbete ska kunna införa funktioner för elektroniska underskrifter i en e-tjänst. I detta alternativ lämnas åt signeringstjänsten att hantera hela processen för underskrift, vilket innefattar

- presentation av det utkast som ska undertecknas av användaren,
- mottagande av användarens aktivering av underskriftsfunktionen (dvs. klicket på knappen ”Jag skriver under”),
- legitimering av användare när underskriftsfunktionen aktiveras,
- skapande av signeringsnycklar och utfärdande av signeringscertifikat för den aktuella underskriften,
- skapandet av underskriften med användarens nya nyckel,
- tidsstämpling av underskriften (när det krävs), och
- sammanfogande av text, underskrift, certifikat och eventuell stämpel till ett paket i enlighet med vedertagen standard för signaturformat.

En fördel från informationssäkerhetssynpunkt med detta alternativ är att den centrala signeringstjänsten oberoende av e-tjänsten hanterar att användaren får ta del av den text som ska granskas för underskrift. Detta förutsätter emellertid att signeringstjänsten får tillgång till hela den text som ska skrivas under och att texten getts ett format som tillåter signeringstjänsten att presentera innehållet på ett för undertecknaren begripligt och meningsfullt sätt.

Detta första alternativ ökar riskerna för enskildas personliga integritet, genom att all text som ska skrivas under förs till en viss central tjänst. Alternativet minskar emellertid samtidigt riskerna för undertecknarens rättssäkerhet genom att texten som ska granskas för underskrift kan presenteras med sådana rutiner att e-tjänsteleverantören eller annan får mera begränsade möjligheter att förvanska det som visas för granskning, så att användaren skriver under något annat än det han eller hon fått se.

Det andra alternativet utformas så att e-tjänsteleverantörer kan få utkast till elektroniska handlingar underskrivna av användare utan att utkastet behöver lämnas till den centrala tjänsten. Detta alternativ möjliggör också för e-tjänsteleverantörer att få tillgång till en central signaturtjänst när de inte kan leverera utkast till en central tjänst i sådan form så att undertecknaren kan läsa handlingen, för att handlingens sammansättning, format eller egenskaper i övrigt eller e-tjänsteleverantörens e-tjänst har sådana egenskaper att den centrala lösningen inte fungerar. Det kan dessutom vara så att en e-tjänsteleverantör inte vill, bör eller får lämna utkastet till en central signeringstjänst.

Det andra alternativet förutsätter att e-tjänsteleverantören i större omfattning deltar i processen för underskrift genom att själv ombesörja presentation av texten i utkastet samt själv foga samman materialet till ett paket, efter att underskrift skett, så att underskrift, certifikat och text ges en utformning som följer ett standardiserat signaturformat eller annars kan hanteras.

De tekniska lösningarna specificeras närmare i *bilaga 17*. Förenklat kan dessa alternativ redovisas i enlighet med sammanställningen i följande figur.

Tabell 3.1 Tekniska lösningar – alternativ

	Tjänst som hanterar förfarandet	
Uppgift	***Alternativ 1***	***Alternativ 2***
Presentation av utkast	I signeringstjänsten	I e-tjänsten
Skapande av fingeravtryck av text för elektronisk underskrift	I signeringstjänsten	I e-tjänsten
Motta svar att användaren vill skriva under granskad text	I signeringstjänsten	I e-tjänsten
Identifiering av användaren	I signeringstjänsten	I signeringstjänsten
Skapa nycklar och utfärda certifikat	I signeringstjänsten	I signeringstjänsten
Tidsstämpla en färdig handling (om så begärs)	I signeringstjänsten	I signeringstjänsten
Underskrift av text (fingeravtrycket)	I signeringstjänsten	I signeringstjänsten
Foga samman till ett paket	I signeringstjänsten	I e-tjänsten

Det återstår att bedöma dessa alternativ från rättsliga utgångspunkter. Som framgår av avsnitt 5.5.3 har även ett tredje alternativ med begränsad funktionalitet diskuterats för det fall en sådan rättslig prövning visar att en signeringstjänst enligt ovan inte är realiserbar.

3.8 Attributstjänster

3.8.1 Bakgrund

En traditionell legitimationshandling kan innehålla uppgift om roll, t.ex. att innehavaren är läkare eller anställd vid ett företag. Uppgifter av sådant slag lämnas dock vanligtvis i andra handlingar. Vid personliga möten används visitkort. Mottagaren brukar lita på sådana handlingar utan några kontroller. Ska en persons juridiska behörighet att företräda annan kontrolleras krävs ofta registreringsbevis utfärdade av en myndighet, t.ex. Bolagsverket, och i vissa fall traditionella undertecknade fullmakter. Vid kontroller för att motverka penningtvätt och i registreringsärenden hos Bolagsverket förekommer kopior av pass eller ID-handlingar. Sådana handlingar brukar lämnas i kopia och t.ex. registreringsbevis är ofta inte bestyrkta.[5] När förfarandet är skriftligt finns det inte

[5] En skriftlig fullmakt återkallas genom att den återtas eller rivs sönder. Det är därför betydelsefullt att originalhandlingen visas upp. Trots detta nöjer sig förlitande parter ofta med en kopia.

heller möjlighet att granska underskrifter genom att jämföra dem med det som återges i undertecknarens legitimationshandling.

Behövs en individs personnummer kan uppgiften samlas in och kontrolleras genom att granska dennes legitimationshandling. Ofta får individen dock själv fylla i personnummer, utan kontroll av legitimation.[6]

När en viss roll är av betydelse – t.ex. för läkare i tjänsten – förekommer att den anges i en traditionell legitimation. I IT-system förs register över personer som hör till aktuell kategori. I fysisk miljö är det oftast känt vilka som har en viss roll och det finns en social kontroll.

3.8.2 Attributsintyg och innehåll

Intygen

Som framgått ska elektroniska intyg, s.k. *attributsintyg,* införas för att lämna motsvarande uppgifter om behörighet, uppdrag, roll eller andra egenskaper, som i traditionell miljö lämnas genom att visa upp en legitimation eller ge in registreringsbevis, fullmakter eller liknande handlingar. Härigenom ska myndigheters och företags e-tjänster smidigt kunna förses med ytterligare information om användare som legitimerar sig. Attribut kan vara ett eller flera och kan innehålla vilken information som helst – inom rimliga gränser – och de ”paketeras” på samma sätt som i ett identitetsintyg, dvs. i ett standardiserat format kallat SAML 2.0.

Det finns inga tekniska hinder mot att förse ett enda intyg med såväl identitetsinformation som attribut. Denna tekniska flexibilitet aktualiserar dock ett antal verksamhetsfrågor och rättsfrågor; vilka bör utfärda attributsintyg, hur bör de tekniska möjligheterna i praktiken tas tillvara och kan attributsintyg ersätta traditionella pappersbaserade handlingar så att kontroller kan utföras automatiserat?

[6] Ett exempel är butiksbiträden som – utan att granska någon legitimationshandling – ber kunden att fylla i sitt personnummer på ”slipen” för kontokortsbetalning i samband med undertecknandet.

Valmöjligheter

Från juridiska utgångspunkter och sett från ett dokument-perspektiv blir valmöjligheterna många. Ska det intyg som utfärdas vid identifieringen (identitetsintyget), som ställs ut av identitets-utfärdaren, kompletteras med ett eller flera attributintyg? Intyg som innehåller attribut tar sin utgångspunkt i den identifierade personen, t.ex. genom att ange i vilken form denne är behörig att företräda ett visst företag eller har någon annan egenskap. E-tjänsteleverantören (förlitande part) får själv utvärdera informationen för att kunna bedöma frågan om behörighet.

Om utgångspunkten för förfrågan i stället behöver vara företaget, för att inte bara utröna om en viss individ är behörig etc., utan inhämta fullständiga uppgifter om vilka individer som registrerats som behöriga eller har viss annan roll eller egenskap, måste detta göras som en kompletterande sökning, (utanför Infrastrukturen för identifiering) t.ex. genom Bolagsverkets XML-tjänst för registreringsbevis.

När E-tjänsteleverantören är en myndighet har denne ofta behov av en uppgift om användarens personnummer. Detta kan tillgodoses genom att personnummer knutet till e-legitimation tas in direkt i identitetsintyget. Olika lösningar kan komma att väljas utifrån olika praktiska situationer (vilka regler som gäller för persondataskydd etc.). Dessa lösningar bör i praktiken begränsas till vissa typfall som lämpligen kan beskrivas utifrån den praktiska situationen.

Exemplet med behörighetskontroll hos Skatteverket

Flera e-tjänster hos Skatteverket kan förbättras och förfinas om verket, när en användare loggar in, får information om vilken behörighet användaren har att företräda annan. Användaren legitimerar sig först med sin e-legitimation och Skatteverket kontrollerar användarens identitet med hjälp av ett identitetsintyg från en utfärdare inom Infrastrukturen för Svensk e-legitimation. Skatteverkets e-tjänst blir inte en del av autentiseringsprocessen. Skatteverket ställer därefter med vetskap om användarens identitet en attributsintygsfråga till Bolagsverket, när t.ex. ett aktiebolag ska företrädas. Verket besvarar förfrågan med ett attributsintyg med

dessa uppgifter. Denna process kan genomföras synligt eller osynligt för brukaren.

Exemplet med e-tjänstelegitimation och personnummer

Många myndigheter har relationer med företrädare för organisationer, såväl inom näringsliv som offentlig sektor, där företrädare önskar använda en e-tjänstelegitimation. Sådana legitimationer innehåller inte personnummer utan kan innehålla allt från en sedvanlig användaridentitet till en pseudonym. I flera e-tjänster krävs emellertid personnummer för att tjänsten ska kunna användas.

I dessa fall kan personnumret lämnas till e-tjänsteleverantören som ett attribut, i ett identitetsintyg eller ett särskilt attributsintyg. Uppgiften finns hos e-legitimationsutfärdaren. En fråga är om uppgiften om personnummer ska lämnas ut av identitetsutfärdaren, en annan om det ska krävas att individen har samtyckt i varje enskilt fall till att personnumret lämnas ut.

Exemplet med behörighetstilldelning inom vård och omsorg

Ett attributsintyg kan som framgått användas för att visa behörighet i en e-tjänst. Inom vård och omsorg har det blivit allt vanligare att uppgifter om behörighet finns lagrade och tas in i ett identitetsintyg som attribut i samband med att intyget skapas. En person kan ha flera olika uppdrag och behörigheter. Det är därför viktigt att rätt behörighet anges i det enskilda fallet när ett identitetsintyg utfärdas.

Särskilt om registreringsbevis m.m. från Bolagsverket

En central fråga är hur de beskrivna nya lösningarna bör tas tillvara när en e-tjänsteleverantör ska kontrollera om en användare som vill logga in i en e-tjänst, enligt det av Bolagsverket förda aktiebolagsregistret är företrädare enligt 8 kap. ABL för ett aktiebolag. Ska utfärdaren av identitetsintyget (som är annan än Bolagsverket) hämta uppgifter ur aktiebolagsregistret och lämna dem i sitt intyg eller ska det, utöver identitetsintyget, lämnas kompletterande uppgifter från Bolagsverket i ett attributsintyg?

En annan mera komplicerad fråga är hur inloggning ska kunna ske när en företrädare inte ensam är behörig utan endast i förening med annan (jfr 8 kap. 39 § ABL) eller när behörigheten grundas endast på fullmakt? Bör ”elektronisk fullmakt” krävas – hur ska detta i så fall lösas (genom t.ex. kungörelsefullmakter eller särskilda register)? Bör nya funktioner införas i e-tjänster där den som är behörig i förening med annan först går in i e-tjänsten och legitimerar sig, för att ange att en annan som är behörig i förening med denne ska släppas in (ensam) när den andre senare loggar in i samma e-tjänst (krav på samtidig inloggning är knappast realistisk) eller bör nya register eller liknande införas där särskilda behörigheter registreras och administreras? Hur ska uppgifter om sådan roll som t.ex. läkare tillhandahållas (i identitetsintyg eller i särskilt attributsintyg) och varifrån ska uppgifterna hämtas?

Vid elektronisk identifiering för tillträde till en e-tjänst uppkommer dessutom följdfrågor när företrädare ska *skriva under elektroniskt.* Kan det räcka att behörigheten kontrollerats vid inloggningen i e-tjänsten – i förening med att denna kontroll och resultatet av den noterats – eller ska uppgiften lämnas i ett nytt intyg? Om underskrift krävs av flera – ska särskilda funktioner finnas för multipla e-underskrifter eller ska en enda underskrift i förening med fullmakt för den andre eftersträvas?

Dessa komplexa frågor har blivit av praktisk betydelse i myndigheternas arbete med mera avancerade e-tjänster. E-legitimationsnämnden kan därför behöva ta höjd för dessa behov vid utvecklingen av Infrastrukturen för Svensk e-legitimation.

3.8.3 Behov av reglering

Den tekniska standard och de programvaror och rutiner som numera finns att tillgå på området för identitets- och attributsintyg gör det *praktiskt möjligt* att i elektronisk miljö införa fungerande lösningar inte bara för att identifiera användare utan också för att få tillgång till och kontrollera uppgifter om juridisk behörighet liksom vissa roller eller personnummer. Samtidigt behöver emellertid juridiska bedömningar göras utifrån lag och rättspraxis och dessa regler kan inte ändras över en natt.

Det föreslås därför att hanteringen av attribut som rör juridisk behörighet vid användning av Svensk e-legitimation ska ta sin utgångspunkt i gällande rätt och utformas i nära anknytning till

vedertagna rutiner för sådana behörighetskontroller. Med aktiebolag och dess företrädare samt aktiebolagsregistret som exempel föreslås att särskilda attributsintyg ska utfärdas av Bolagsverket, inom ramen för den infrastruktur e-legitimationsnämnden inför för Svensk e-legitimation.

Bolagsverket bör ansöka hos E-legitimationsnämnden om anslutning till Svensk e-legitimation, närmare bestämt om att införas som utfärdare av attributsintyg i det utfärdarregister som E-legitimationsnämnden ska föra. På så sätt kan verkets deltagande i en infrastruktur för Svensk e-legitimation göra det möjligt för anslutna myndigheter att enkelt och kostnadseffektivt fråga efter attributsintyg samt elektroniskt få svar som kan tolkas i enlighet med en standardiserad lösning där intygens äkthet skyddas genom elektroniska stämplar.

Bolagsverket bör lämna attributsintyg så att mottagaren automatiserat eller manuellt kan tolka uppgifterna. Myndigheter som behöver göra många sådana kontroller, t.ex. Skatteverket, bör kunna införa sina ”tolkningsparametrar” i program för automatiserade kontroller. På så sätt blir ansvarsfördelningen densamma som i dag. Bolagsverket lämnar utdrag ur aktiebolagsregistret och förlitande part tolkar dem, t.ex. bedömer om det är tillräckligt för den aktuella inloggningen eller underskriften om personen är verkställande direktör (jfr 8 kap. 36 § ABL).

Det behöver därmed finnas gränssnitt för både maskiner (tekniska gränssnitt) och för människor (användargränssnitt) som gör det enkelt att läsa attributsintygen såväl automatiserat som manuellt på bildskärm.

Denna lösning bör emellertid kompletteras med ett förenklat förfarande för mindre myndigheter som inte har förutsättningar att införa egna lösningar för automatiserade behörighetskontroller med stöd av attributsintyg. Bolagsverket överväger i denna del att skapa ett ”förenklat registreringsbevis” utifrån en klassificering för maskinell behandling. Genom en sådan tjänst skulle uppgifter sållas bort så att endast en kod anges i intyg till e-tjänsteleverantören (förlitande part). För att ansvarsfördelningen mellan registerföraren (Bolagsverket) och förlitande part (e-tjänsteleverantören) inte ska rubbas skulle dessa koder kunna grundas på en specifikation som Bolagsverket publicerar, efter samråd med berörda aktörer, och utifrån vilken förlitande part själv får göra en juridisk behörighetsbedömning. Tekniskt skulle en sådan hantering kunna bli enkel.

Den första lösningen synes inte kräva någon författningsreglering eftersom Bolagsverket alltjämt endast skulle lämna utdrag ur aktiebolagsregistret. Den förenklade lösningen kan däremot behöva författningsregleras. För att ett författningsförslag ska kunna läggas fram krävs emellertid närmare klarlägganden av hur lösningen ska utformas.

3.8.4 Bedömning

Myndigheter hämtar redan i dag uppgifter om juridisk behörighet från Bolagsverket och det finns överenskommelser och regler om vad detta kostar och hur betalning ska ske. Dessa överenskommelser och regler bör i princip kunna gälla även för tillhandahållande och betalning av elektroniska registreringsbevis och föreslagna förenklade förfaranden. Det bör därmed vara tillräckligt att Bolagsverket genom ett ansökningsförfarande ansluts av E-legitimationsnämnden till Infrastrukturen för Svensk e-legitimation, närmare bestämt till det utfärdarregister – i tekniska sammanhang kallat federationsregister – som E-legitimationsnämnden avses inrätta och föra.

Utöver de ansöknings- och anslutningsavgifter som nämnden kan komma att ta ut av Bolagsverket och anslutna e-tjänsteleverantörer inom offentlig sektor avses ingen ersättning utgå inom Infrastrukturen för identifiering för att fråga ska få ställa om attributsintyg från Bolagsverket och att verket ska få leverera intyget via den kanalen. Någon upphandling torde därmed inte behövas i denna del.

Motsvarande synsätt bör tillämpas för andra myndigheter som med stöd av författning för register över juridiska personer och deras företrädare.

Attributsintyg beträffande annat än juridisk behörighet – t.ex. om viss roll eller om personnummer eller anställning hos viss juridisk person – kräver såvitt framkommit inte någon särskild författningsreglering. Det avgörande är att mottagande organ inom offentlig sektor kan lita på uppgifterna i attributsintygen. Sådant fog för tillit byggs upp inom Infrastrukturen för Svensk e-legitimation; jfr principen om fri bevisprövning. Infrastrukturens kvalitet och de funktioner som erbjuds synes därmed bli mera styrande än regler i lag eller förordning.

Det får antas att det finns ett betydande behov av uppgifter om behörighet i egenskap av firmatecknare eller fullmäktig. En marknad för att administrera och tillhandahålla tillförlitliga sådana uppgifter kan därmed förväntas växa fram. En fråga blir härvid vilka utfärdare av attributsintyg som ska få ingå i det utfärdarregister som ska föras av E-legitimationsnämnden. Myndigheter som med stöd av författning för register över juridiska personer och deras företrädare – t.ex. Bolagsverket – bör få registreras i det utfärdarregister som E-legitimationsnämnden avses föra. Detta bör i vart fall gälla när särskilda rättsverkningar är knutna till registreringen i det aktuella registret och regler finns i författning om bl.a. ansvar för uppgifternas innehåll. Det får i övrigt genomlysas vilka regler som bör gälla för att bedöma vilka aktörer som är av sådan betydelse för berörda myndigheter och uppfyller sådana krav på tillit och juridisk betydelse att de bör få ingå i den föreslagna Infrastrukturen för identifiering. E-legitimationsnämnden bör utifrån ett regelverk ha att pröva vilka attributsutfärdare som ska få anslutas till utfärdarregistret.

Attributsutfärdare som anslutits till Infrastrukturen för identifiering ska således tillhandahålla uppgifter åt e-tjänsteleverantörer om juridisk behörighet, roll, personnummer eller annat av betydelse för en e-tjänsteleverantör som ska kontrollera uppgifter om användare. Attributsutfärdare bör få anslutas till Infrastrukturen för identifiering om utfärdaren enligt lag eller författning ska registrera och tillhandahålla de uppgifter som avses lämnas i attributsintygen och uppgifterna är av generell betydelse från kontrollsynpunkt eller omdet annars finns särskilda skäl för att ett visst slag av attribut från en viss utfärdare ska få lämnas inom Infrastrukturen för identifiering.

E-legitimationsnämnden bör samtidigt ges i uppgift att verka för att en parallell infrastruktur växer fram för andra attributsutfärdare och för e-tjänsteleverantörer utanför offentlig sektor, där motsvarande tillgång till uppgifter bör ges. Hur en sådan på privaträttsliga regler grundad infrastruktur närmare ska utformas bör emellertid inte behandlas här.

3.9 Behörighetshantering med stöd av attribut

Identitetsintyg och hur de används kan beskrivas relativt enkelt, i vart fall på ett övergripande plan. För hanteringen av attribut och

Attributsintyg är situationen en annan. Skilda regler och krav gäller inom olika delar av offentlig förvaltning, exempelvis för kontroller av juridisk behörighet med stöd av registerutdrag från Bolagsverket respektive kontroller inom hälso- och sjukvården för att få tillgång till uppgifter i patientjournaler. En närmare genomgång utifrån dessa exempel har visat att det behöver klargöras vad som ska ingå i den Infrastruktur för identifiering som E-legitimationsnämnden enligt sin instruktion har att etablera och vad som bör utvecklas och användas som särlösningar för vissa områden; se vidare *bilaga 8*.

4 Ett nytt valfrihetssystem för offentlig sektor

I detta kapitel lämnas ett förslag om ett valfrihetssystem på området för e-legitimationer.

4.1 Bakgrund

4.1.1 Valfrihetssystem

Lagen om valfrihetssystem

Lagen (2008:962) om valfrihetssystem (LOV) trädde i kraft den 1 januari 2009. Där regleras vad som ska gälla när en upphandlande myndighet beslutat att tillämpa valfrihetssystem beträffande vissa tjänster inom hälsovård och socialtjänster. Med valfrihetssystem menas ett förfarande där den enskilde har rätt att välja den leverantör som ska utföra tjänsten och som en upphandlande myndighet har godkänt och tecknat kontrakt med.

Inom ramen för ett valfrihetssystem konkurrensutsätts en tjänst genom att brukarna av tjänsten ges möjlighet att välja mellan olika leverantörer som den upphandlande myndigheten tecknat avtal med. De ekonomiska villkoren för utförandet av tjänsten bestäms i avtal mellan den upphandlande myndigheten och leverantörerna.

En upphandlande myndighet som beslutat att tillämpa valfrihetssystem ska annonsera detta på en nationell webbplats som upprättats för ändamålet.[1] På webbplatsen ska ett förfrågningsunderlag finnas tillgängligt. Förfrågningsunderlaget ska ange grunderna för den ekonomiska ersättningen till leverantörerna. Den upphandlande myndigheten får dessutom, genom angivande i annonsen eller förfrågningsunderlaget, ställa särskilda sociala och

[1] Sådan webbplats tillhandahålls av Kammarkollegiet.

miljömässiga villkor eller andra villkor för hur ett kontrakt ska fullgöras.

Utgångspunkten vid inrättandet av ett valfrihetssystem är att alla de fysiska och juridiska personer som lämnat in en ansökan och uppfyller villkoren i förfrågningsunderlaget ska godkännas av den upphandlande myndigheten. Den upphandlande myndigheten får dock under vissa förutsättningar utesluta sökanden, t.ex. på grund av att en sökande har ekonomiska problem eller tidigare gjort sig skyldig till brott med avseende på yrkesutövningen.

Efter att den upphandlande myndigheten har godkänt en leverantör ska kontrakt tecknas med denne. En leverantör som anser att den upphandlande myndigheten brutit mot en bestämmelse i LOV får ansöka om rättelse hos allmän förvaltningsdomstol.

Tillämpningsområdet för LOV är begränsat till valfrihetssystem som inrättas av kommunala myndigheter och vissa därmed likställda organ. Vidare är lagen begränsad till valfrihetssystem som avser tjänster inom hälsovård och socialtjänster, som är upptagna som B-tjänster i kategori 25 i bilaga 3 till lagen (2007:1091) om offentlig upphandling (LOU).

För kommunala myndigheter är tillämpning av valfrihetssystem enligt LOV ett frivilligt alternativ till upphandling enligt LOU. Kommunerna väljer alltså om upphandling ska ske genom att tillämpa valfrihetssystem eller om upphandling enligt LOU ska användas. Regeringen anförde i propositionen 2008/09:29 *Lag om valfrihetssystem* att det är kommunen som inom sitt område bäst kan avgöra om valfrihetssystem är möjliga och lämpliga att införa och vilka delar av verksamheten som ska ingå i valfrihetssystemet (s. 54).

En avgörande skillnad i förhållande till en upphandling enligt LOU är att alla leverantörer som godkänns får teckna kontrakt med den upphandlande myndigheten. Om en upphandling i stället genomförs enligt LOU ska den upphandlande myndigheten utse en vinnare bland leverantörerna.

När LOV infördes angavs att syftet var att sätta brukaren i fokus och att åstadkomma en maktförskjutning från politiker och tjänstemän till medborgare. Dessutom eftersträvades ökad valfrihet och ökat inflytande, fler utförare och större mångfald. Ett brukarinflytande förutsattes vidare öka kvalitén på tjänsterna.

De tjänster som LOV omfattar (vissa s.k. B-tjänster) omfattas endast i begränsad omfattning av Europaparlamentets och rådets direktiv 2004/18 om offentlig upphandling av byggentreprenader,

varor och tjänster (upphandlingsdirektivet). Det fanns därför vissa möjligheter till nationell särlösning.

Regeringen har vidare konstaterat att kontrakt inom ett valfrihetssystem kan vara att bedöma som tjänstekoncessioner (prop. 2008/09:29 s. 55 ff.). Avgörande ansågs vara om utföraren bär risken för att etablera och driva verksamheten. Regeringen fann att utföraren i sådana tillämpningar där LOV avses gälla fick anses stå den ekonomiska risken inom ramen för valfrihetssystemet.

Tjänstekoncessioner omfattas inte av upphandlingsdirektivet och inte heller av lagen om offentlig upphandling. Tilldelning av en tjänstekoncession liksom själva tjänstekoncessionsavtalet måste emellertid överensstämma med EU-rättens grundläggande principer om icke-diskriminering, likabehandling, öppenhet, ömsesidigt erkännande och proportionalitet.

Eftersom kontrakt om valfrihetssystem enligt LOV bedömdes utgöra tjänstekoncessioner kunde LOV utformas utan hänsyn till vissa av de bestämmelser som finns i upphandlings- och rättsmedelsdirektiven.

Valfrihetssystem hos statliga myndigheter

LOV gäller som nämnts endast för valfrihetssystem inrättade av kommunala myndigheter och vissa med dem likställda organ. Frågan om statliga myndigheters inrättande av valfrihetssystem har behandlats i regeringens propositioner 2009/10:146 *Valfrihet hos Arbetsförmedlingen* och 2009/10:60 *Nyanlända invandrares arbetsmarknadsetablering – egenansvar med professionellt stöd*.

Föreskrifter om valfrihetssystem hos Arbetsförmedlingen finns numera i lagen (2010:536) om valfrihet hos Arbetsförmedlingen. Ambitionen var att den offentliga arbetsförmedlingens kompetens och tjänsteutbud skulle kompletteras med flera olika aktörer i syfte att göra utbudet större och mer varierat. Regeringen fann att motiven bakom LOV fick anses giltiga också inom Arbetsförmedlingens verksamhetsområde, i den mån verksamheten inte skulle innefatta myndighetsutövning (prop. 2009/10:146 s. 15 ff.)

Lagen om valfrihet hos Arbetsförmedlingen är, till skillnad från LOV, inte begränsad till s.k. B-tjänster. Mot bakgrund av bedömningen att kontrakt som sluts efter upphandling enligt lagen om valfrihetssystem är tjänstekoncessioner som inte omfattas av

EU:s upphandlingsdirektiv, anförde regeringen att A-tjänster inte behövde undantas (prop. 2009/10:146 s. 20).

I lagen (2010:197) om etableringsinsatser för vissa nyanlända invandrare, har införts bestämmelser om att Arbetsförmedlingen ska tillhandahålla ett eller flera valfrihetssystem som ger nyanlända rätt att välja en av Arbetsförmedlingen godkänd och kontrakterad etableringslots.

4.1.2 Behov av valfrihetssystem för Svensk e-legitimation

Behovet av mångfald gör sig särskilt starkt gällande på området för Svensk e-legitimation. Medborgare, företag och myndigheter har redan i betydande omfattning valt utfärdare av e-legitimation, lärt sig att använda tillhandahållna e-legitimationer och tjänster samt skapat rutiner för användningen, memorerat lösenord och infört erforderligt stöd.

Även inom ramen för den framtida lösningen för Svensk e-legitimation bör användaren kunna välja leverantör utifrån behov av bl.a. tillit, service, funktionalitet och kvalitet. Redan gjorda investeringar i infrastruktur och anskaffningar av e-legitimationer bör tas tillvara så att den synnerligen utbredda användningen i Sverige av e-legitimationer inte stannar upp utan ytterligare tar fart inom en framtida infrastruktur. Dagens e-legitimationer uppfyller redan i allt väsentligt den säkerhetsnivå som för närvarande anses erforderlig för Svensk e-legitimation och de kan – liksom nya lösningar – anpassas till ändrade förutsättningar, t.ex. om en viss teknisk lösning skulle bli genombruten till följd av matematiska genombrott, snabbt ökad processorkraft eller andra liknande händelser.

Eftersträvad flexibilitet och anpassning till användares behov kan uppnås om Svensk e-legitimation inrättas inom ramen för ett valfrihetssystem. Skulle i stället en upphandling enligt LOU krävas och en enda vinnare behöva utses för myndigheternas användning av Identitetsintyg kommer endast den som har en e-legitimation utfärdad av den vinnande utfärdaren att kunna legitimera sig i e-tjänster hos myndigheter som kräver identifiering med Svensk e-legitimation.

I arbetet med Infrastrukturen för Svensk e-legitimation har därför konstaterats att ett valfrihetssystem bör införas för elektronisk identifiering inom offentlig sektor. Tanken är att alla

utfärdare som uppfyller valfrihetssystemets krav ska anslutas genom kontrakt med den myndighet – E-legitimationsnämnden – som inrättats för att styra, utveckla och svara för verksamhet på området för Svensk e-legitimation. De myndigheter som tillhandahåller e-tjänster där elektronisk legitimering krävs för tillträde (E-tjänsteleverantörer) ska anslutas så att de med hjälp av identitetsintygstjänster kan kontrollera att den som vill bereda sig tillträde till en e-tjänst verkligen är den han eller hon utger sig för att vara.

Det har vidare visat sig att de e-tjänster som tillhandahålls eller planeras inom offentlig sektor i allt högre grad används inte bara av privatpersoner utan också av anställda eller uppdragstagare som agerar i tjänsten, antingen för ett privaträttsligt subjekts – vanligtvis ett företags – räkning eller för ett offentligrättsligt organs räkning (en myndighet kan använda en annan myndighets e-tjänst). Det är därför viktigt att regleringen för att bruka e-legitimationer omfattar inte bara privata e-legitimationer utan även e-tjänstelegitimationer som företag eller myndigheter anskaffar åt sina anställda. Att detta regelverk ska gälla även för en sådan användning innebär emellertid inte att anskaffning genom ett valfrihetssystem för Svensk e-legitimation även ska innefatta myndigheters och företags anskaffning av e-tjänstelegitimationer. Det innebär inte heller att den ersättningsmodell som föreslås för en Infrastruktur för identifiering ska omfatta e-tjänstelegitimationer.

4.2 Valfrihetssystem för identitetsintygstjänster

4.2.1 En lag om valfrihet för Svensk e-legitimation

Förslag: En ny lag ska ge E-legitimationsnämnden möjlighet att tillhandahålla valfrihetssystem. E-legitimationsnämnden ska efter erforderliga anpassningar tillämpa lagen (2008:962) om valfrihetssystem. E-legitimationsnämnden får tillhandahålla valfrihetssystem vid upphandling av tjänster för elektronisk identifiering.

Befintliga upphandlingsmöjligheter tillgodoser inte behoven

En utgångspunkt vid inrättandet av en Infrastruktur för Svensk e-legitimation är att mångfald och konkurrens ska eftersträvas på marknaden för elektronisk identifiering. Den lösning för samordning av hanteringen av elektronisk identifiering som E-delegationen föreslagit skulle innebära att samtliga leverantörer som uppfyller de uppställda kraven ska kunna få tillträde till marknaden. I utredningens direktiv har regeringen konstaterat att en sådan lösning kan förväntas förbättra förutsättningarna för en fungerande konkurrens på marknaden för elektronisk identifiering och skapa en frihet för användaren att välja den e-legitimation som användaren tycker svarar mot dennes krav och önskemål.

En förutsättning för att de mål som ställts upp av regeringen ska kunna tillgodoses är att E-legitimationsnämndens upphandling av e legitimationstjänster kan leda till att samtliga e-legitimationer som uppfyller uppställda krav kan brukas av medborgare och företag när de använder förvaltningens e-tjänster.

Under utredningens arbete har emellertid den bedömningen gjorts att varken upphandling enligt LOU eller tilldelning av avtal genom en tjänstekoncession, utan särskild lagstiftning om valfrihetssystem för området, uppfyller kraven för att åstadkomma en Infrastruktur för Svensk e-legitimation.

Upphandling av ramavtal enligt LOU innebär att upphandlande myndigheter antar en eller flera leverantörer för att i ett senare skede kunna avropa tjänster från dessa. När ramavtal ingås med flera leverantörer ska – om alla villkoren är fastställda i ramavtalet – kontrakt tilldelas den leverantör som rangordnats högst på grundval av de villkor som angetts i ramavtalet. Avsteg från rangordningen får inte göras. Om alla villkor inte är fastställda i ramavtalet ska i stället en förnyad konkurrensutsättning ske, där leverantörerna ska inbjudas att på nytt lämna anbud i enlighet med de villkor som anges i ramavtalet. Kontrakt ska tilldelas den leverantör som lämnat bästa anbudet på grundval av de tilldelningskriterier som angetts i förfrågningsunderlaget till ramavtalet.

Eftersom LOU, enligt ovan, anger uttömmande på vilka sätt en upphandlande myndighet kan genomföra en upphandling är det inte möjligt att på LOU grunda ett förfarande där samtliga leverantörer som uppfyller ställda kvalifikationskriterier antas, och där val av leverantör överlämnas till den som ska använda e-legitimation.

Upphandling av tjänstekoncession framstår följaktligen som ett lämpligare alternativ för att tillgodose de mål som ställts upp av regeringen. Den svenska upphandlingslagstiftningen är som framgått inte tillämplig på tjänstekoncessioner, vilket innebär att det är möjligt att, inom ramen för upphandling av tjänstekoncessioner, använda andra förfaranden än de som LOU tillhandahåller, bl.a. förfaranden där samtliga leverantörer som uppfyller ställda kvalifikationskriterier antas.

I utredningens arbete har emellertid den bedömningen gjorts att möjligheterna till rättsprövning av ett beslut om tilldelning genom tjänstekoncession är oklara och att författningsreglering därför behövs, såvitt avser möjligheten till rättsprövning, om alternativet tjänstekoncession ska väljas.

En författningsreglering krävs därför för att tillgodose de mål som regeringen ställt upp. Utredningen har härvid övervägt om E-legitimationsnämnden, efter författningsändringar, kan genomföra sina anskaffningar genom tjänstekoncessioner, i enlighet med det förfarande som anges i LOV.

Motiven bakom lagen om valfrihetssystem är giltiga för e-legitimationer

När LOV infördes angavs att syftet var att sätta brukaren i fokus och att åstadkomma en maktförskjutning från politiker och tjänstemän till medborgare. Dessutom eftersträvades ökad valfrihet och ökat inflytande, fler utförare och större mångfald. Ett brukarinflytande förutsattes vidare öka kvalitén på tjänsterna; se regeringens proposition 2008/09:29 *Lag om valfrihetssystem*.

Samma intressen gör sig gällande på området för Svensk e-legitimation. Målen med en samordningsfunktion har angetts vara att E-legitimationer ska vara lätt tillgängliga för medborgare och företag, att en och samma e-legitimation ska kunna användas för alla e-tjänster hos kommuner och andra myndigheter, att konkurrensen och förutsättningarna för att utveckla nya tjänster för elektronisk identifiering ska förbättras och att myndigheters kostnader ska minska.

Ett valfrihetssystem i enlighet med det som genomförts genom LOV skulle ge E-legitimationsnämnden möjlighet att etablera en standard för e-legitimationstjänster inom ramen för en nationell modell, samtidigt som det skulle uppstå en kvalitetskonkurrens i

brukarledet genom att brukarna ges möjlighet att välja leverantör. Tjänster för Svensk e-legitimation bör på detta sätt kunna göras mera lättillgängliga samtidigt som konkurrensen kan förväntas öka.

Ett valfrihetssystem enligt LOV kan följaktligen utgöra en lämplig struktur för att inrätta en Infrastruktur för Svensk e-legitimation.

Genomförande i en ny lag

Lagen om valfrihetssystem gäller, som tidigare nämnts, endast för valfrihetssystem inrättade av kommunala myndigheter och vissa organ som är likställda med dem. Författningsreglering är alltså en förutsättning för att E-legitimationsnämnden ska kunna inrätta Infrastrukturen för Svensk e-legitimation i enlighet med det förfarande som anges i LOV.

Inrättandet av valfrihetssystem för Svensk e-legitimation bör därför ske genom att E-legitimationsnämnden i en ny lag ges rätt att tillhandahålla valfrihetssystem för elektronisk identifiering. När nämnden inrättar valfrihetssystem ska nämnden enligt den föreslagna lagen tillämpa LOV.

Valfrihetssystem får inrättas för elektronisk identifiering

Valfrihetssystem som inrättas av E-legitimationsnämnden med stöd av den nya lagen avses omfatta de tjänster som behövs för att bygga upp en Infrastruktur för Svensk e-legitimation. Den exakta omfattningen av tjänster som behöver upphandlas inom valfrihetssystemet bestäms bäst av E-legitimationsnämnden i dess fortsatta arbete. I den nya lagen förslås därför att det område inom vilket E-legitimationsnämnden får inrätta valfrihetssystem anges som elektronisk identifiering. En mer detaljerad avgränsning i lag har inte bedömts vara lämplig på detta tidiga stadium i utvecklingsarbetet; jfr den vida avgränsning som gjorts i lagen (2010:536) om valfrihet hos Arbetsförmedlingen.

4.2.2 Kontrakt inom valfrihetssystemet är tjänstekoncessioner

Bedömning: Valfrihetssystem som E-legitimationsnämnden inrättar enligt den föreslagna lagen innebär att avtal tilldelas genom tjänstekoncession. Denna tilldelning omfattas därför inte av LOU.

En förutsättning för att en infrastruktur ska kunna inrättas enligt LOV:s förfaranderegler är att de offentliga kontrakt som E-legitimationsnämnden tecknar med Identitetsutfärdare anses vara tjänstekoncessioner. Om så inte är fallet blir LOU tillämplig vid upphandlingen. Där anges uttömmande på vilka sätt en upphandlande myndighet kan genomföra en upphandling. Det blir därmed avgörande om inrättandet av ett valfrihetssystem för Svensk e-legitimation kan anses utgöra tilldelning av tjänstekoncessioner. Med tjänstekoncession menas enligt 2 kap. 17 § LOU ett kontrakt av samma slag som ett tjänstekontrakt, men där ersättningen för tjänsterna helt eller delvis utgörs av en rätt att utnyttja tjänsten. Tjänstekoncession kan därmed beskrivas som ett kontrakt enligt vilket ett företag åtar sig att ansvara för en verksamhet och där ersättning för detta utgår i form av rätten att ta betalt av allmänheten för att utnyttja tjänsterna som produceras i denna verksamhet eller en sådan rätt i kombination med betalningar från den upphandlande myndigheten (prop. 2006/07:128 s. 181). I propositionen med förslag till LOV gjorde regeringen bedömningen att kontrakt kan anses utgöra tjänstekoncession även om betalningen inte kommer direkt från tredje man, förutsatt att det är leverantören som bär risken (prop. 2008/09:29 s. 56 f.). Att kommissionen gjort samma bedömning framgår av ett tolkningsmeddelande (kommissionens tolkningsmeddelande om koncessioner enligt EG-rätten, EGT C 121, 29.04.2000, not 13).

Ett avgörande kriterium vid bedömningen av om ett avtal utgör en tjänstekoncession är om koncessionsinnehavaren ges rätt att utnyttja sina egna tjänster kommersiellt och därigenom tar en betydande ekonomisk risk (se t.ex. NOU:s yttrande i RK 2006:797). Kommissionen har uttalat följande i ovan nämnda tolkningsmeddelande:

> Nyttjanderättskriteriet är avgörande när det gäller att fastställa om ett avtal är en tjänstekoncession eller inte. Enligt detta kriterium rör det

> sig om en koncession, om tjänsteleverantören tar riskerna i samband med den tillhandahållna tjänsten (etablering och nyttjande) och tar ut ersättning av användaren, t.ex. via avgifter i vilken form det än vara må. Sättet på vilket tjänsteleverantören får ersättning är, liksom för byggkoncessioner, en faktor som gör det möjligt att fastställa vem som tar på sig risken i samband med nyttjandet. Tjänstekoncessioner kännetecknas, liksom byggkoncessioner, av att ansvaret för nyttjandet överförs på koncessionshavaren.[2]

Ett avtal kan alltså utgöra en tjänstekoncession om leverantören tar en risk i samband med den tillhandahållna tjänsten och leverantören tar ut ersättning av användaren, t.ex. i form av avgifter. Det sätt på vilket ersättning till tjänsteleverantören utgår är således en faktor som gör det möjligt att fastställa vem som står risken i sambandet med nyttjandet. Ersättningen kan dock utgå från den upphandlande myndigheten förutsatt att det är leverantören som bär risken för nyttjandet (se prop. 2009/10:60 s. 86 f.). Så blir fallet om det är användarna som styr till vem ersättning ska utgå.

Regeringen anförde i propositionen 2008/09:29, *Lag om valfrihetssystem* att ett kontrakt inom ramen för ett valfrihetssystem kan vara att bedöma som en tjänstekoncession (s. 55 ff.). Avgörande ansågs vara om utföraren bär risken för att etablera och driva verksamheten. Regeringen fann att utföraren i sådana tillämpningar där LOV avses gälla fick anses stå den ekonomiska risken inom ramen för valfrihetssystemet.

Motsvarande gäller för det valfrihetssystem som E-legitimationsnämnden föreslås få inrätta enligt en lag om valfrihet för Svensk e-legitimation. De identitetsutfärdare som ansluts till valfrihetssystemet är beroende av användarnas val för att verksamheten ska kunna generera inkomster. Ett kontrakt med en upphandlande myndighet innebär alltså inte någon inkomstgaranti. Att de tjänster som upphandlas blir till nytta för myndigheterna hindrar inte att kontrakten ses som tjänstekoncessioner. Avgörande blir om den nytta som kan uppkomma för en myndighet kan anses påverka nyttjanderättskriteriet, dvs. riskövergången med avseende på nyttjandet.

Ett införande av föreslagen Infrastruktur för Svensk e-legitimation medför att de upphandlande myndigheterna förbinds att ta emot Identitetsintyg från de Identitetsutfärdare som användarna väljer. Myndigheterna kan därför inte styra vilken Identitetsutfärdare som ska få ersättning. Vidare är all ersättning

[2] Kommissionens tolkningsmeddelande om koncessioner enligt EG-rätten (2000/C 121/02).

som Identitetsutfärdarna kan få enligt berörda upphandlingskontrakt beroende av utfärdarnas förmåga att locka kunder. Identitetsutfärdarna får således, enligt denna modell, stå hela risken för nyttjandet av de upphandlade tjänsterna.

Det måste också beaktas att tjänsten för Identitetsintyg ska ses som en del i själva nyttjandet av e-legitimationen. Till nyttjandet hör olika tjänster som t.ex. att Identitetsutfärdaren kontrollerar att e-legitimationen inte är spärrad. Av tekniska skäl ”levereras” Identitetsintyget till E-tjänsteleverantören men detta förhållande gör inte att utfärdandet av Identitetsintyget kan ses som en fristående och självständig tjänst utan utfärdandet av Identitetsintyg ska ses som en del i det knippe av tjänster som Identitetsutfärdaren tillhandahåller för att e-legitimationer ska kunna användas inom Infrastrukturen för Svensk e-legitimation.

Till detta kommer att konkurrensen på marknaden kraftigt skulle begränsas om nyttjanderättskriteriet inte anses uppfyllt och LOU därför anses tillämplig, eftersom myndigheterna då skulle ha behövt välja en enda leverantör av Identitetsintyg. Dagens infrastruktur torde dessutom vid en sådan utveckling bli delvis avvecklad utan någon allmänt spridd ersättare eftersom trögheten hos användarna är betydande när det gäller att anskaffa en ny e-legitimation hos annan utfärdare.

Valfrihetssystem som E-legitimationsnämnden inrättar enligt den förslagna lagen bör alltså anses innebära att avtal tilldelas genom tjänstekoncession och ett valfrihetssystem bör därmed kunna inrättas enligt de förfaranderegler som LOV anger.

Till skillnad från vad som gäller för tjänstekoncession enligt LOV kommer Svensk e-legitimation kunna omfatta ett brukande för en juridisk persons räkning. Avgörande för om LOV:s förfaranderegler kan användas är om inrättandet av valfrihetssystemet anses vara en tjänstekoncession och det avgörande kriteriet vid denna bedömning är inte vilka brukarna är utan om det är tjänsteleverantören som står den ekonomiska risken i samband med den tillhandahållna tjänsten.

4.2.3 Samordnat inrättande av valfrihetssystemet

Förslag: En kommun eller ett landsting ska få uppdra åt E-legitimationsnämnden att på kommunens eller landstingets vägnar besluta om godkännande av sökande och ingående av kontrakt eller på annat sätt genomföra och avsluta ett inrättande eller en förändring av ett valfrihetssystem enligt den nya lagen.
Bedömning: Ett ramavtal för inrättande av valfrihetssystem bör anses uppfylla krav på ramavtal eller andra gemensamma avtal enligt förordningen (1998:796) om statlig inköpssamordning.

Samordnat inrättande genom gemensamma avtal

Inom ramen för den föreslagna infrastrukturen ska ett stort antal myndigheter sluta avtal med Identitetsleverantörer om tillhandahållande av tjänster. Utgångspunkten för utredningens förslag är att E-legitimationsnämnden ska ges möjlighet att samordna inrättandet av valfrihetssystemet för Svensk e-legitimation så att myndigheterna kan sluta gemensamma avtal med Identitetsutfärdarna.

Enligt den föreslagna lagen ges E-legitimationsnämnden möjlighet att fatta beslut om att tillhandahålla valfrihetssystem för Svensk e-legitimation. E-legitimationsnämnden anges också vara upphandlande myndighet enligt LOV, vilket innebär att LOV:s förfaranderegler och rättsmedel endast gäller E-legitimationsnämnden och dess beslut.

Detta hindrar emellertid inte att E-legitimationsnämnden inrättar valfrihetssymetet genom att teckna gemensamma avtal med identitetsutfärdarna, där alla E-tjänsteleverantörer som lämnat uppdrag åt E-legitimationsnämnden är parter. Eftersom avtal inom valfrihetssystem för Svensk e-legitimation har bedömts utgöra tjänstekoncessioner kan detta ske utan hänsyn till LOU:s regler om förfarande och rättsmedel.

Enligt befintliga regler får kommuner och landsting emellertid inte överlåta till extern part att fatta beslutet om vilken leverantör som ska tilldelas ett kontrakt; se vidare departementspromemorian Samordnad upphandling (Ds 2004:37). Vid en samordnad upphandling måste tilldelningsbeslut därför fattas av varje kommun

och landsting.[3] Ett uppdrag att utreda frågan om utökade delegationsmöjligheter för kommuner och landsting vid samordnad upphandling har kort tid innan avlämnandet av detta betänkande lämnats till Utredningen om offentliga företag – upphandling, kontroll, insyn (dir. 2010:115). Det ska enligt detta direktiv utredas om det är lämpligt att införa en generell delegationsbestämmelse.

Inom ramen för vårt uppdrag har endast en begränsad delegationsbestämmelse övervägts, motsvarande vad som återfinns i 6 kap. 3 § lagen (2009:47) om vissa kommunala befogenheter. En sådan begränsad bestämmelse kan inte antas ha någon sådan inverkan på det kommunala självstyret eller upphandlingsmarknaden att ett kommande förslag från Utredningen om offentliga företag – upphandling, kontroll behöver avvaktas; jfr Ds 2004:37 för en närmare diskussion rörande konsekvenserna av att tillåta extern delegation.

För att säkerställa att anslutningen till valfrihetssystemet inte blir mer omständlig och kostsam för kommuner och landsting än för statliga myndigheter, föreslår vi att även kommuner och landsting ska ges möjlighet att uppdra åt E-legitimationsnämnden att på kommunens eller landstingets vägnar besluta om godkännande av sökande och ingående av kontrakt eller på annat sätt genomföra och avsluta ett inrättande eller en förändring av ett valfrihetssystem enligt den nya lagen.

Statlig inköpssamordning

I förordningen (1998:796) om statlig inköpssamordning anges att ramavtal eller andra gemensamma avtal ska finnas för varor och tjänster som myndigheterna upphandlar ofta, i stor omfattning eller som uppgår till stora värden. De tjänster som E-legitimationsnämnden ska upphandla torde omfattas av detta krav. Enligt förordningen ska således ett ramavtal eller annat gemensamt avtal finnas.

Frågan är om gemensamma avtal för inrättande av valfrihetssystem kan anses uppfylla krav på ramavtal eller annat gemensamt avtal. Begreppet ramavtal åsyftar, i upphandlingsrättsliga sammanhang, vanligen sådana ramavtal som avses i 2 kap. 15 § LOU. Vad

[3] Se t.ex. departementspromemorian *Samordnad upphandling* (Ds 2004:37) s. 32, prop. 2009/10:180, *Nya rättsmedel på upphandlingsområdet*, s. 266 f., Statskontorets rapport *Offentliga inköpscentraler i Sverige* (2008/163-5) s. 10.

som avses med ”annat gemensamt avtal” är emellertid inte helt klart. Ekonomistyrningsverket nämner, i en kommentar till förordningen, att det t.ex. kan vara samordnade inköpsavtal med preciserade kvantiteter enligt bindande avtal mellan parterna.[4] I samma kommentar anger Ekonomistyrningsverket att de gemensamma avtal som förordningen nämner ska upphandlas enligt LOU, vilket inte blir fallet för valfrihetssystem enligt den nya lagen.

Det är uppenbart att syftet med förordningen om statlig inköpssamordning är att kostnadseffektivisera myndigheters inköpsverksamhet, inte att ställa upp upphandlingsrättsliga förfaranderegler (se 1 §).[5] Det kan därför anses rimligt att innefatta gemensamma avtal för inrättande av valfrihetssystem i förordningens uppställda krav på ramavtal eller annat gemensamt avtal.

Gemensamma avtal för inrättande av valfrihetssystem bör därför anses uppfylla krav på ramavtal eller andra gemensamma avtal enligt förordningen om statlig inköpssamordning. Några författningsändringar behövs därmed inte i denna del. Detta innebär vidare att myndigheter under regeringen ska använda sig av sådant gemensamt avtal om myndigheten inte finner att en annan form av avtal sammantaget är bättre.

[4] Se <http://www.avropa.se/templates/Page2760.aspx>.
[5] Se även prop. 1997/98:136, *Statlig förvaltning i medborgarnas tjänst*, s. 41, Statskontorets rapport *En effektivare statlig inköpssamordning* (2009:12), Ekonomistyrningsverkets information på <http://www.avropa.se/templates/Page32.aspx.>.

5 Ett regelverk för infrastrukturen för Svensk e-legitimation

I detta avsnitt beskrivs hur den Infrastruktur för Svensk e-legitimation som föreslås ska kunna realiseras genom författningsreglering och civilrättslig reglering.

5.1 Flera samverkande regleringar

För att den föreslagna modellen till en ny Infrastruktur för Svensk e-legitimation ska kunna bli verklighet behövs som framgått både *författningsreglering* och *civilrättslig reglering*.

Två grundläggande komponenter i en författningsreglering av området har redan berörts, nämligen

1. Förslag till lag om valfrihet för Svensk e-legitimation, och
2. Beslutad förordning med instruktion för E-legitimationsnämnden.

Ytterligare reglering genom förordning kan dock visa sig behövas genom dels kompletteringar i E-legitimationsnämndens instruktion, när uppdraget utkristalliserats närmare (jfr avsnitt 3.4), dels en särskild förordning om Infrastrukturen för Svensk E-legitimation. I den särskilda förordningen kan närmare regler ges för bl.a. statliga myndigheters mellanhavanden vid införande och användning av den nya infrastrukturen. Eftersom myndigheter under regeringen är en del av samma juridiska person regleras deras mellanhavanden normalt i författning. De utgör ett och samma rättssubjekt och kan därför inte sluta bindande civilrättsliga avtal med varandra eller få en tvist om en överenskommelse prövad i domstol.

Det planeras vidare att E-legitimationsnämnden ska ta ut en avgift för handläggningen av ärenden rörande Infrastrukturen för Svensk e-legitimation – dels en ansökningsavgift vid anslutning, dels en årlig avgift för administration och tillsyn. Dessa avgifter kan behöva regleras i förordning. Vissa förfaranderegler och regler om infrastrukturen kan också behöva ges i förordning. Det blir dessutom viktigt, med hänsyn till utvecklingstakten på området, att normgivningskompetens delegeras till E-legitimationsnämnden. Tekniskt och administrativt komplicerade frågor rörande elektronisk identifiering och elektroniska underskrifter bör så långt det är möjligt inte regleras i lag eller förordning, bl.a. för att nya tekniska landvinningar och förbättrade produkter ska kunna tas i bruk utan hinder av teknikrelaterade regler i lag eller förordning.

Till detta kommer de civilrättsliga regler som behövs inom Infrastrukturen för Svensk e-legitimation. Dessa regler kan införas som en del i parternas mellanhavanden genom att tas in i de avtal som E-legitimationsnämnden ingår med dem som ansluts till Infrastrukturen för Svensk e-legitimation. Denna infrastruktur byggs därmed genom flera samverkande regelverk. Frågan är emellertid hur dessa närmare bör utformas. Utredningens arbete har hittills fokuserat på att finna och utvärdera alternativ till en ny modell, vilket gör att regelarbetet ägnats mindre tid. I det följande kan därför endast en övergripande bild ges av dessa frågor och av hur en rättslig reglering av en Infrastruktur för Svensk e-legitimation skulle kunna fördelas mellan lag, förordning, myndighetsföreskrifter, civilrättsliga regler i avtal mellan aktörerna samt icke bindande allmänna råd, riktlinjer och tekniska specifikationer.

Det bör samtidigt noteras att det inte finns några vedertagna författningstekniska eller avtalstekniska lösningar för hur en infrastruktur av aktuell omfattning och betydelse bör regleras. Erfarenheter från området för e-legitimationer har dessutom visat att många och omfattande dokument lätt växer fram där det delvis framstår som oklart vad som utgör bindande regler till skillnad från rekommendationer, vägledningar eller tekniska beskrivningar av använda IT-lösningar. En central del i arbetet med regelverk för den föreslagna infrastrukturen bör därmed vara att införa en regelhierarki och utforma samverkande regler i lag, förordning och myndighetsföreskrifter som är tydliga, lättillgängliga och förenliga med reglerna om normgivningskompetensens fördelning, i den mån regleringen inte ska ske civilrättsligt i avtal mellan berörda parter.

5.2 Utkast till förordning om Infrastrukturen för Svensk e-legitimation

E-legitimationsnämnden ska som framgått inte bara utveckla en Infrastruktur för Svensk e-legitimation som myndigheter och vissa därmed jämställda organ avses använda. Nämnden ska också svara för centrala delar av infrastrukturen.

Den reglering av det planerade valfrihetssystemet som föreslås i lag och motiven till denna reglering kommer visserligen att ge en övergripande beskrivning av den Infrastruktur för Svensk e-legitimation som ett valfrihetssystem är tänkt att betjäna. Där kan emellertid inte mer än en övergripande bild ges och det föreslås inte heller några regler i lag om t.ex.

1. *vilka aktörer* som ska ingå i denna infrastruktur – att bara myndigheter och vissa jämställda organ inom offentlig sektor ska få anslutas i egenskap av e-tjänsteleverantörer,
2. *vilka register* som ska ingå i Infrastrukturen för identifiering, vilka som ska få registreras i dessa register och vem som ska svara för dem – att utfärdar- och e-tjänsteregister ska inrättas och föras för offentlig sektor, att E-legitimationsnämnden ska svara för registren, att endast utfärdare av Svensk e-legitimation och vissa attributsutfärdare ska få registreras där,
3. *hur infrastrukturen ska användas* – att bl.a. legitimering, elektronisk underskrift samt autentisering och äkthetskontroll ska kunna ske, och
4. *vilka regler* som ska gälla för bl.a. anslutningsförfarandet, avgifter, användning och ansvar.

Utvecklingen på området är snabb. En närmare beskrivning i lag skulle därmed, som framgått, snabbt kunna komma i konflikt med och kanske rent av hindra att kommande tekniska landvinningar tas tillvara. Vissa funktioner inom den planerade infrastrukturen blir dessutom av sådan betydelse att en författningsreglering kan ses som en naturlig del av en reglering. En särskild förordning om Infrastrukturen för Svensk e-legitimation kan härvid visa sig lämplig.

Vidare bör normgivningskompetens delegeras så att detaljerade och tekniskt relaterade regler för en Infrastruktur för Svensk e-legitimation kan ges genom myndighetsföreskrifter, antingen som

verkställighetsföreskrifter eller med stöd av den s.k. restkompetensen; 8 kap. 13 § regeringsformen (RF).

En sådan förordning om Infrastrukturen för Svensk e-legitimation bör syfta till att etablera infrastrukturen för svensk e-legitimation inom den offentliga förvaltningen och att samordna och förenkla e-tjänsteleverantörernas användning av funktioner för elektronisk legitimering och elektronisk underskrift. Förordningen bör kunna tillämpas för såväl statliga som kommunala myndigheter.

Som en första del i en sådan förordning bör definitioner ges av centrala begrepp, *se bilaga 4*.

Här kan inte nog betonas vikten av att den föreslagna, delvis komplexa infrastrukturen beskrivs och betecknas på ett enhetligt sätt, inte bara i författning utan även i det civilrättsliga regelverk som ska införs genom avtal vid anslutning till valfrihetssystemet.

Regler bör vidare ges, i en förordning om Infrastrukturen för Svensk e-legitimation, *se bilaga 5*, om de register som behövs inom infrastrukturen för identifiering. Där krävs dels ett utfärdarregister över de identitets- och attributsutfärdare som ansluts, dels ett e-tjänsteregister över e-tjänsteleverantörer som ansluts.

I denna del behövs föreskrifter för att tillgodose behovet av persondataskydd, genom att – så långt det är möjligt – förbjuda att personuppgifter behandlas. Det bör dessutom i tydlighetens intresse särskilt anges att uppgifter om vilken kommunikation som ägt rum med eller mellan användare och e-tjänsteleverantörer inte får registreras där och naturligtvis inte heller innehållet i identitets- eller attributintyg eller handlingar som ska eller har skrivits under elektroniskt. Det behöver vidare säkerställas att identitets- eller attributsintyg inte kan finnas loggade eller annars bevarade inom ramen för Infrastrukturen för Svensk e-legitimation. För signaturtjänsten krävs dessutom regler så att elektroniska meddelanden som ska skrivas under eller har undertecknats inte får finnas bevarade eller loggade – inte ens i säkerhetskopior, brandväggar, intrångsdetekteringssystem eller liknande.

Det bör dessutom – med hänsyn till infrastrukturens karaktär – föreskrivas att de tekniska och administrativa lösningarna ska utformas så att så få personuppgifter som möjligt samlas in, lämnas ut eller annars behandlas och att inte fler uppgifter än nödvändigt samlas in och bevaras så att de blir direkt tillgängliga. Samtidigt kan bestämmelser behövas för att säkra sådan *åtkomst i elektronisk form*

till de uppgifter i registren som krävs för att infrastrukturen ska kunna användas på ett fungerande sätt.

Anslutning till registret torde ske genom beslut av E-legitimationsnämnden i förvaltningsärenden. Detta gäller för både identitetsutfärdare och e-tjänsteleverantörer. Vissa regler om förfarandet och om avgifter m.m. behöver ges i en förordning om Infrastrukturen för Svensk e-legitimation. Vidare kan där erforderliga bemyndiganden ges för E-legitimationsnämnden att meddela föreskrifter rörande Infrastrukturen för Svensk e-legitimation.

Det behöver också övervägas i vilken mån bestämmelserna i 2 kap. 10 och 11 §§ tryckfrihetsförordningen (TF) kan bli tillämpliga på detta material. Möjligen kan vissa föreskrifter behöva ges om uppgiftshanteringen.

5.3 Valfrihetslag och civilrättslig reglering

5.3.1 En lösning genom avtal

Med det valfrihetssystem som föreslagits (kapitel 4) följer att civilrättsliga avtal sluts med alla identitetsutfärdare. Dessa avtalsslut avses leda till ett kontraktuellt förhållande mellan bl.a. varje identitetsutfärdare och varje e-tjänsteleverantör. Avtalssluten ska ske genom E-legitimationsnämnden, efter att e-tjänsteleverantörerna gett nämnden i uppdrag att ingå dessa avtal för deras räkning. Genom att avtal sluts mellan de involverade parterna uppkommer kontraktuella förhållanden direkt mellan dessa och lösningen innebär att sådana konstruktioner som tredjemansavtal kan undgås och därmed den rättsliga osäkerhet som avtal av det slaget lätt för med sig, t.ex. om villkor rörande ansvar eller begränsning av ansvar behöver knytas till en viss rättslig relation. Förenas de avtal som E-legitimationsnämnden enligt uppdrag tecknar med allmänna villkor som inkorporeras i samtliga avtal kan denna reglering – rätt utformad – delvis bära upp Infrastrukturen för Svensk e-legitimation. Genom att E-legitimationsnämnden ges en central roll i avtalstecknandet och i hanteringen av avtalen med Identitetsutfärdare kan en smidig och praktisk hantering skapas för e-tjänsteleverantörerna.

Om en lösning med avtal inte valts hade det dessutom krävts lagstiftning. Med den föreslagna inriktningen får marknaden delvis utforma affärsmodeller och lösningar. Eftersom det till stora delar

är osäkert hur denna marknad kommer att utvecklas saknas underlag för att utforma en reglering som har den stabilitet och förankring i vedertagna synsätt som brukar krävas i ett lagstiftningsärende. Valfrihetssystemet ger dessutom utrymme för anpassningar över tiden, vilket är en viktig del i utvecklingen av en Infrastruktur för Svensk e-legitimation. Genom denna flexibilitet kan t.ex. nya lösningar införas genom tillägg till träffade avtal. Stor hänsyn måste dock tas till identitetsutfärdarna vid förändringar.

Olika kontraktuella förhållanden uppstår således direkt genom valfrihetssystemet. I det följande redogörs översiktligt för dessa och hur regler för denna infrastruktur kan införas genom avtal.

5.3.2 E-legitimationsnämnden och identitetsutfärdaren

E-legitimationsnämnden tecknar, i egenskap av mellanman, avtal med de identitetsutfärdare som uppfyller kraven och ska anslutas till Infrastrukturen för identifiering. Nämnden företräder därvid ett stort antal aktörer inom den offentliga sektorn; andra myndigheter, kommuner m fl. Detta medför att det uppkommer ett civilrättsligt avtal mellan varje sådant rättssubjekt och varje identitetsutfärdare. Även E-legitimationsnämnden blir part i dessa avtal. Denna reglering omfattar inte bara ersättningsfrågor utan även mera övergripande regler som rapporteringsskyldighet, bestämmelser om tillsyn och inspektioner men också bestämmelser om rätt för E-legitimationsnämnden att frånträda avtalet vid grövre avtalsbrott från en identitetsutfärdares sida.

Avtalsregleringen mellan identitetsutfärdare och respektive e-tjänsteleverantörer ska omfatta t.ex. identitetsutfärdarens ansvar för de leveranser som sker. Samtidigt införs genom referens i de avtal som tecknas ett generellt regelverk för infrastrukturen – regelverket för Infrastrukturen för Svensk e-legitimation. På detta sätt införs genom civilrättsliga avtal regler om exempelvis hur e-legitimationer utfärdas och används, anslutning av utfärdare och e-tjänsteleverantörer till infrastrukturen, utformningen av tekniska hjälpmedel, bevarande av vissa handlingar, skydd för e-legitimationer och anmälan om spärr, e-tjänsteleverantörernas kontroller, legitimering och underskrift, persondataskydd, säkerhet och tillsyn eller annan granskning.

Genom att avtal sluts med alla aktörer inom Infrastrukturen för Svensk e-legitimation och att aktörerna i tillämpliga delar som

avtalsinnehåll får åta sig att följa regelverket kan mellanhavandena i allt väsentligt hanteras genom civilrättslig reglering. Denna lösning är enligt vår mening den lämpligaste formen för att etablera Infrastrukturen för Svensk e-legitimation. I ett senare skede kan det när förutsättningarna klarnat, genom bl.a. marknadens krav har stabiliserats och kan tydliggöras visa sig lämpligt att införa en reglering i lag.

5.3.3 Identitetsutfärdare och användare

Innehållet i de avtal som sluts mellan identitetsutfärdare och användare bestäms i allt väsentligt av utfärdaren och användaren. Mot bakgrund av den typ av standardiserade tjänster som det blir frågan om får det dock i praktiken antas att identitetsutfärdaren använder sig av standardavtal för e-legitimationstjänster och att utrymmet för individuellt förhandlade villkor är synnerligen begränsat. Priset för att tillhandahålla e-legitimationer bestäms vidare av utfärdaren utan inblandning av E-legitimationsnämnden. Valfrihetssystemet innebär att dessa priser och villkoren i övrigt måste vara konkurrenskraftiga eftersom användaren ska kunna välja mellan e-legitimationer från flera identitetsutfärdare.

I de avtal som E-legitimationsnämnden ingår med identitetsutfärdare åtar sig emellertid utfärdaren att tillhandahålla e-legitimationer som uppfyller kraven för Svensk E-legitimation. Identitetsutfärdaren måste se till att dessa krav i tillämpliga delar återförs i identitetsutfärdarens avtal med användaren. I denna del bör beaktas hur bl.a. finansiella institut, infört friskrivningar som föranlett lagstiftaren att i flera fall agera.[1] Regleringen av Infrastrukturen för

[1] I 2 kap. 21 § bankrörelselagen (1987:617), som numera ersatts av 9 kap. 4 § lagen (2004:297) om bank- och finansieringsrörelse infördes begränsningar i lag så att motbok eller annat bevis, som en bank utfärdar om tillgodohavande på räkning, ska ställas till viss man och innehålla att överlåtelse får ske endast till viss man samt att överlåtelsen bör anmälas hos banken, som inte får träffa förbehåll om rätt att åberopa betalning till annan än rätt innehavare av motbok. Bakgrunden var den att enskilda, efter stöld av bankbok blivit av med hela sitt sparkapital genom att det tagits ut och banken kunde åberopa att innehavaren ansågs behörig. På motsvarande sätt har det – till följd av alltför långtgående friskrivningar – i 34 § konsumentkreditlagen (1992:830) föreskrivits att avtalsvillkor som innebär att en kontohavare ska vara betalningsskyldig för ett belopp som har påförts kontot genom att ett kontokort har använts av någon obehörig person får göras gällande endast om kontohavaren eller någon annan som enligt kontoavtalet är behörig att använda kontokortet har (1.) lämnat ifrån sig kortet till någon annan, (2.) genom grov oaktsamhet förlorat kortet eller (3.) på något annat sätt förlorat besittningen av kortet och inte snarast efter upptäckten anmält förlusten hos kreditgivaren. Denna bestämmelse, som upphävts den 1 augusti 2010, har ersatts med lagen (2010:738) om obehöriga transaktioner med betalningsinstrument.

Svensk e-legitimation bör, så långt det kan ske, ges en balanserad utformning, bl.a. så att korrigeringar genom lag för att motverka mindre lämpliga friskrivningar kan undgås. Även i övriga delar kan tydlighet och balans behöva säkerställas.

De allmänna villkor som införs för Infrastrukturen för Svensk e-legitimation bör kunna spela en roll även i denna del genom att det där ställs krav även på avtalen mellan identitetsutfärdare och användare. Juridisk samordning och anpassning till vad som är en rimlig riskfördelning kan därmed uppnås även i denna del.

Det kvarstår emellertid att E-tjänsteleverantören, såvitt avser utfärdande och nyttande av e-legitimationen, inte kommer att ha någon avtalsrelation med användaren. En annan sak är att avtalsvillkor eller författningsreglering kan bli tillämplig för själva den e-tjänst där användaren brukar sin e-legitimation. Något förenklat kan hävdas att regleringen av själva e-tjänsten inte ska omfattas av det regelverk som införs för Infrastrukturen för Svensk e-legitimation.

Även i denna del finns paralleller mellan regleringen i avtal av Infrastrukturen för Svenska E-legitimation och den avtalsreglering som gäller för betal- och kreditkort. De finansiella instituten sluter avtal med användare om tillhandahållande och nyttjande av kort för betalningar (jämförbart med avtalet mellan identitetsutfärdaren och användaren), institutet träffar avtal med inköpsställen om att acceptera korten för betalning av de varor eller tjänster som inköpsstället tillhandahåller (jämförbart med avtal mellan e-tjänsteleverantörer och identitetsutfärdare). Något avtal mellan användaren och inköpsstället (eller e-tjänsteleverantören) avseende själva användningen av betal- eller kreditkortet (eller Svensk e-legitimation) träffas emellertid inte. För att infrastrukturen med ett stort antal finansiella aktörer ska hålla samman och ansvaret fördelas på ett balanserat sätt finns dessutom ett bakomliggande regelverk för anslutna institut (i någon mån jämförbart med de allmänna villkoren för Infrastrukturen för Svensk e-legitimation).

Inom ramen för det arbete som ledde fram till dagens e-legitimationslösning genomfördes en analys av användarvillkor, i samverkan mellan ett projekt som myndigheterna bedrev inom ramen för ett regeringsuppdrag (det s.k. SAMSET-projektet) och berörda utfärdare av e-legitimationer, i syfte att bereda väg för samordnade enkla och balanserade regler för användare.

Motsvarande samordning bör ske inför ett införande av en ny infrastruktur. Härvid bör emellertid regler införas också i allmänna

villkor som ska gälla för Infrastrukturen för Svensk e-legitimation. Dessa regler bör göras till avtalsinnehåll genom hänvisning i de avtal som sluts till följd av ett införande av det planerade valfrihetssystemet.

5.3.4 Nämnden, e-tjänsteleverantörerna och regelverket

Genom att E-legitimationsnämnden ingår avtal med identitetsutfärdare för e-tjänsteleverantörernas räkning blir det civilrättsliga regelverket – dvs. de allmänna villkoren för Infrastrukturen för Svensk e-legitimation – bindande inte bara för e-tjänsteleverantörerna. E-legitimationsnämnden blir också part i dessa avtal och binds därmed till de allmänna villkoren. Detta regelverk avses innehålla även mera övergripande regler om bl.a. rapporteringsskyldighet, inspektioner och rätt för nämnden och e-tjänsteleverantörer att frånträda avtalet vid grövre avtalsbrott från en identitetsutfärdares sida, se vidare *bilaga 6*.

Därmed skapas, på liknande sätt som på det finansiella området, en infrastruktur utifrån civilrättsliga överenskommelser där vissa centrala funktioner ingår såväl tekniskt som administrativt och i huvudsak regleras genom avtal. I den mån marknadens utveckling skulle medföra att avtal inte längre kan utgöra enda styrmedlet kan regler i lag eller förordning övervägas, t.ex. till följd av att särskilt skydd behövs för svagare part eller för persondata.

Den planerade infrastrukturen kan också visa sig få sådan betydelse att författningsreglering krävs, t.ex. vid utredningar av brott där elektronisk kommunikation har använts eller där samhällets säkerhet kräver det. På detta stadium har emellertid förutsättningarna inte klarnat tillräckligt för att dessa frågor ska kunna bedömas och det har i tidigare lagstiftningssammanhang visat sig svårt att förutse utvecklingen och införa tydliga regler; jfr t.ex. de komplikationer som särskilda s.k. registerlagar fört med sig.

I de delar där E-legitimationsnämnden ska handlägga och besluta i förvaltningsärenden behövs dock viss författningsreglering. När en identitetsutfärdare eller en e-tjänsteleverantör ska inleda sin verksamhet behöver denne registreras i något av de register som förs av E-legitimationsnämnden för dem som ingår i Infrastrukturen för Svensk e-legitimation. Denna offentligrättsliga hantering bör delvis regleras i den föreslagna förordningen om Infrastrukturen för Svensk e-legitimation.

5.4 Anvisningstjänsten respektive infrastrukturcertifikat

Anvisningstjänsten fungerar, som framgått av avsnitt 3.6, som ett stöd för användarens val av e-legitimation när han eller hon ska legitimera sig för att få tillträde till en e-tjänst. I vissa fall kan användaren se att en särskild tjänst för anvisning används, i andra fall inte.

Så som denna tjänst fungerar blir det naturligt att se E-legitimationsnämnden som underleverantör av den till respektive tillhandahållare av e-tjänster. E-tjänsteleverantören får därmed anses tillhandahålla anvisningstjänsten åt användaren. Denna tjänst bör ses endast som en liten kugge i Infrastrukturen för identifiering.

På liknande sätt finns certifikat för varje aktör i utfärdar- och e-tjänsteregistren. Vid förfrågningar och svar genom intyg inom Infrastrukturen för identifiering används dessa infrastrukturcertifikat automatiserat, för att motverka förfalskningar eller andra liknande manipulationer. Här involveras emellertid inte användaren. Detta skydd bör därmed i juridisk mening uppfattas som en av de funktioner som E-legitimationsnämnden tillhandahåller åt identitetsutfärdare och e-tjänsteleverantörer som är anslutna till Infrastrukturen för identifiering.

5.5 Signaturtjänsten

5.5.1 Behov av överväganden

Enligt avsnitt 3.7 bör de där beskrivna tjänsterna för elektroniska underskrifter (signeringstjänsten) om möjligt utformas dels så att *kvalificerade certifikat* utfärdas momentant, dels så att en *säker anordning för signaturframställning* tillhandahålls, så att de elektroniska underskrifterna kan anses vara kvalificerade. Förenklat kan detta beskrivas så att användaren – efter att ha granskat den aktuella texten inför underskrift – vidtar en aktiv handling (att klicka på knappen ”Jag skriver under”). Användaren får därvid legitimera sig för signeringstjänsten med sin ordinarie e-legitimation. Efter legitimeringen skapas omedelbart i signaturtjänsten ett nytt certifikat och kryptografiskt nyckelpar (tekniskt motsvarande dem i dagens e-legitimationer). Användarens privata nyckel i nyckelparet för underskrift aktiveras genast och destrueras när

underskrift skett. På så sätt kan den privata nyckeln inte därefter missbrukas av någon för ytterligare underskrifter. Det använda engångscertifikatet och den publika nyckeln bevaras emellertid under den tid detta krävs.

Från juridiska utgångspunkter aktualiseras i huvudsak två frågor. För det första behöver det bedömas om engångscertifikatet och de tekniska hjälpmedel som i övrigt tillhandahålls åt undertecknaren i signaturtjänsten kan användas så att en elektronisk underskrift blir att anse som en kvalificerad elektronisk signatur enligt lagen (2000:832) om kvalificerade elektroniska signaturer (signaturlagen); dvs. för att underteckna med en avancerad elektronisk signatur, baserad på ett kvalificerat certifikat och skapad av en säker anordning för signaturframställning.

Det behöver för det andra bedömas vem som i juridisk mening ska anses som utfärdare av engångscertifikaten och tillhandahållare av den säkra anordningen samt vad som i övrigt kan ingå i signaturtjänsten.

5.5.2 Signaturlagen och signaturtjänsten

Frågan om den planerade signaturtjänsten kan användas för kvalificerade elektroniska signaturer behöver bedömas i två led. Det första ledet rör huruvida definitioner och rekvisit i signaturlagen och bakomliggande direktiv kan förenas med en signaturtjänst. Om så är fallet behöver det, som ett andra led, bedömas om de *säkerhetslösningar* som krävs inom Infrastrukturen för Svensk e-legitimation kan nå upp till signaturlagens och direktivets krav.

De definitioner som främst berörs är ”avancerad elektronisk signatur”, ”kvalificerat certifikat”, och ”säker anordning för signaturframställning” (hit hör även definitionen av ”anordning för signaturframställning). Kvalificerad elektronisk signatur definieras nämligen som en avancerad elektronisk signatur som är baserad på ett kvalificerat certifikat och som är skapad av en säker anordning för signaturframställning.

I signaturlagen ges uppräkningar av krav för att sådana signaturer, certifikat och anordningar ska anses föreligga. En översiktlig granskning har visat att dessa krav är utformade så att hinder i princip inte synes föreligga mot att använda en signeringstjänst för att skriva under med en kvalificerad elektronisk signatur.

Det finns emellertid skäl att närmare överväga vad som enligt lagen och direktivet menas med att

1. en avancerad elektronisk signatur måste vara skapad med hjälpmedel som endast undertecknaren kontrollerar (2 §), och
2. den som tillhandahåller certifikattjänster inte ska lagra eller kopiera uppgifter för skapande av signaturer (direktivet Bilaga II j).

Kravet på att signaturerna ska vara skapade med hjälpmedel som endast undertecknaren kontrollerar kan tolkas antingen så att undertecknaren ensam måste ha *fysisk kontroll* över hjälpmedlet (den privata nyckeln) eller så att det räcker att undertecknaren ensam har *logisk kontroll* över detta hjälpmedel. Vår preliminära bedömning är att varken den svenska lagstiftningen eller direktivet utesluter en lösning som bygger på att undertecknaren, till följd av logiska lösningar, ensam får anses ha kontrollen över den privata nyckeln.[2] På detta stadium i utredningsarbetet torde emellertid underlag saknas för att bedöma om de säkerhetslösningar som väljs kan antas uppfylla signaturlagens krav.

Kravet i signaturdirektivet på att den som tillhandahåller certifikattjänster inte ska lagra eller kopiera uppgifter för skapande av signaturer har enligt lagmotiven införts genom såväl 9 § som 11 § signaturlagen. Av 9 § följer bl.a. att en certifikatutfärdare som utfärdar kvalificerade certifikat, *se bilaga 10*, till allmänheten ska bedriva verksamheten tillförlitligt och i förekommande fall se till att framställandet av signaturframställningsdata sker konfidentiellt (dessa data måste genereras på ett sådant sätt att de inte röjs för obehöriga, prop. 1999/2000:117 s. 73). I 11 § andra stycket föreskrivs vidare att certifikatutfärdaren inte får lagra eller kopiera signaturframställningsdata. Det är nämligen väsentligt för tilltron till elektroniska signaturer att det verkligen bara är undertecknaren som har tillgång till signaturframställningsdata (prop. 1999/2000:117 s. 74).

Rättsläget får anses oklart. Vår preliminära bedömning är emellertid att varken den svenska lagstiftningen eller direktivet bör anses utesluta en lösning där de privata nycklarna finns på en central server, förutsatt att det tekniska och administrativa skyddet

[2] Jfr även professor Henrik Udsen, Köpenhamns Universitet, *Notat om anvendelsen af serverbaserede losninger for kvalificerede elektroniske signaturer* <https://danid.dk/export/sites/dk.danid.oc/da/dokumenter/henrik_udsen_notat.pdf>.

utformats så att utfärdaren inte kan kopiera eller annars missbruka de privata nycklarna utan att detta upptäcks.[3]

Vi får i det fortsatta arbetet återkomma till den rättsliga bedömningen av dessa fysiska respektive logiska skydd.

5.5.3 Alternativa metoder

Användare måste ges möjlighet till elektronisk underskrift inom ramen för en infrastruktur för Svensk e-legitimation enligt utredningens förslag. Om resultatet av en utvärdering av signeringstjänsten visar att underskrift i en central tjänst inte är en lämplig lösning, så kan även infrastrukturen för identifiering samverka med en lösning där användare skriver under elektroniskt i sin lokala datormiljö. En närmare beskrivning av en sådan lösning samt dess för- och nackdelar presenteras närmare i *bilaga 17* (Central signeringstjänst).

5.6 Utfärdarens ansvar för intyg

Den föreslagna Infrastrukturen för identifiering innebär som framgått att Identitets- och At-tributsutfärdare – efter erforderliga kontroller – ska gå E-tjänsteleverantörer till handa med att i intyg bestyrka identitet eller elektronisk underskrift eller bekräfta att en person är behörig att vidta vissa tjänsteåtgärder, har en viss tjänsteställning eller kompetens eller är behörig att företräda någon annan. Dessa formuleringar, som delvis är hämtade ur lagen (1981:1363) om notarius publicus, tydliggör den roll vi föreslår för Identitetsutfärdare. De avses alltså fylla motsvarande funktion som den notarius publicus har tilldelats enligt författning, nämligen att gå allmänheten tillhanda med officiella bevis om vissa faktiska förhållanden. [4]

En skillnad är visserligen att en juridisk person inte kan förordnas till notarius publicus – rollen som utfärdare är tänkt att fullgöras av juridiska personer – en annan att det i allt väsentligt

[3] Jfr i föregående not anfört arbete, med hänvisningar.

[4] Genom förordningen (1982:327) om notarius publicus säkerställs dessutom att det finns tillgång till sådana befattningshavare (de förordnas av länsstyrelsen) och att de som förordnas har tillräcklig kompetens och är lämpliga för uppdraget. Det föreskrivs också att Notarius publicus skall fullgöra sitt uppdrag med redlighet, noggrannhet och opartiskhet och inte får befatta sig med ett ärende, om det angår honom själv eller om någon annan särskild omständighet föreligger som är ägnad att rubba förtroendet till hans opartiskhet.

blir fråga om helt automatiserade kontroller där intyg förses med en elektronisk stämpel. Den juridiska modellen bör emellertid kunna bli densamma. Det kan inte heller uteslutas att en Identitetsutfärdare i undantagsfall, när en funktion fallerat eller ifrågasatts, kan behöva utföra manuella åtgärder och upprätta elektroniskt underskrivna intyg eller intyg på papper.

Införandet av den nya infrastrukturen bör därmed kunna förenklas genom att beskriva Identitetsutfärdare som en slags motsvarigheter till notarius publicus och knyta an till de rättsregler som gäller för notarius publicus verksamhet. Att affärsmodellen för denna infrastruktur kan påverkas av valet mellan öppna respektive slutna system för e-legitimationer behöver inte bli ett hinder. Dagens affärsmodell för de e-legitimationer som myndigheter godtar förutsätter förlitandeavtal, medan ett införande av kvalificerade certifikat enligt signaturlagen måste ske inom ett öppet system; dvs. ett system där förlitande parter inte har avtal med utfärdaren. Vårt förslag om att införa ett valfrihetssystem och tillhörande hantering av Identitetsintyg leder emellertid till avtal mellan alla berörda aktörer, även för de fall där kvalificerat certifikat använts vid legitimering eller för underskrift. Ansvaret för Identitetsintygen bör härvid regleras i avtal så att utfärdare får bära samma risk som inom dagens system. Hur detta närmare ska utformas får genomlysas i det fortsatta arbetet med att upphandla ett valfrihetssystem.

Beträffande Attributsintygen är situationen delvis en annan. För utfärdare som redan idag ställer ut intyg i enlighet med regler i författning – t.ex. registreringsutdrag utfärdade av Bolagsverket – finns en vedertagen syn på ansvarets gränser och fördelningen av risker. Dessa förutsättningar bör inte ändras bara för att elektroniska rutiner införs. För andra som ska börja utfärda intyg kan frågan om ansvarsfördelning inte bedömas utifrån redan införda rutiner. Dessa olika bedömningar av hur risker ska fördelas torde inte kunna göras generellt. Frågan bör i stället bedömas från tillämpning till tillämpning.

6 Tillitsramverk

I detta avsnitt presenteras utredningens förslag till tillitsramverk för Svensk e-legitimation. Ett väl fungerande tillitsramverk som är i samklang med den internationella utvecklingen och standardiseringen är centralt för att bygga nödvändigt förtroende för Svensk e-legitimation. Praktiskt utgör det vidare en central del för att definiera vilka aktörer som kan bli leverantörer i Svensk e-legitimation.

6.1 Utgångspunkter

En Infrastruktur för identifiering bör ta sin utgångspunkt i ett tillitsramverk byggt på internationell standard och medge den flexibilitet som den föreslagna Infrastrukturen för Svensk e-legitimation och internationell samverkan kräver.

De flesta av de internationella ansträngningar som gjorts för att definiera nivåer av tillit vid användning av e-legitimationer har sin grund i en publikation (SP 800-63) från det amerikanska National Institute of Standards and Technology (NIST). De riktlinjer som beskrivs där är emellertid relativt allmänt hållna. Fördjupande arbeten har därför bedrivits inom bl.a. Europeiska unionen, där det storskaliga s.k. STORK-projektet utgjort en viktig del[1]

Ett betydelsefullt arbete för att utarbeta ett internationellt tillitsramverk bedrivs nu också inom International Organization for Standardization och International Electrotechnical Commission (ISO/IEC). Det kommande resultatet av detta arbete, ISO/IEC 29115, som förväntas bli internationell norm på området,

[1] EU-kommissionen har tagit fram en handlingsplan som ska underlätta för medlemsstaterna att införa ömsesidigt godkända och kompatibla system för e-signaturer och e-legitimationer i syfte att göra det lättare att tillhandahålla elektroniska offentliga tjänster över gränserna [KOM(2008) 798]. Arbetet för ömsesidigt erkännande av elektronisk identifiering inom EU genomförs inom STORK-projektet.

bygger på dokument som publicerats inom det s.k. Kantara Initiative Identity Assurance Framework (Kantara IAF).

Utredningens förslag

Under förutsättning att det fortsatta arbetet inom ISO/IEC leder till resultat som är förenliga med behoven inom den föreslagna Infrastrukturen för identifiering bör Sverige följa denna internationella standard. E-legitimationsnämnden bör därför, liksom E-delegationen, verka för att resultatet av standardiseringsarbetet blir förenligt med svenska intressen på området.

I avvaktan på detta resultat bör ett tillitsramverk införas som har sin förankring i de tidigare nämnda publikationerna. De har alla gemensamt att de definierar fyra tillitsnivåer (AL)[2] för e-legitimering, i syfte att möta olika nivåer av risk och olika krav på användbarhet. Dessa tillitsnivåer svarar mot olika grader av teknisk och operationell säkerhet hos utfärdaren och olika grader av kontroll av att en person som tilldelas en elektronisk identitet verkligen är den han eller hon utger sig för att vara.

Något förenklat kan tillitsnivåerna beskrivas som en måttstock, där en lägre indikering på skalan motsvarar enklare användning och utgivning, lägre kostnader, men också en lägre skyddsnivå. Högre klassificering medför högre kostnader för såväl utgivande som användande, men leder till att en högre grad av tillit kan fästas vid identifieringen.

Vid en tillämpning av dessa internationella normer har det, såvitt hittills framkommit, visat sig ändamålsenligt att för Svensk e-legitimation kräva en tillitsnivå som motsvarar nivå 3 (AL3) eller högre. Detta innebär att utgivare av Svensk e-legitimation ska ha dokumenterade och fungerande ledningssystem för informationssäkerhet i enlighet med erkända standarder, att innehavares identiteter verifieras på ett ändamålsenligt sätt, att metoden för legitimering baseras på starka kryptografiska mekanismer och utgivaren ska kunna påvisa att de når upp till och efterlever kraven enligt AL3.

Tillitsnivå 3 är också den nivå som ligger närmast de av ramavtalsleverantörerna idag utgivna e-legitimationerna. Den öppnar emellertid även nya typer av e-legitimationer som inte är

[2] AL är en förkortning av den internationella termen för tillitsnivå, ”Assurance Level”, som används såväl i Kantara IAF som i STORK-projektet.

certifikatbaserade. Detta förväntas kunna leda till en högre användbarhet och större spridning inom fler samhällsgrupper. Om det visar sig att en betydande del av de redan utgivna e-legitimationerna inte uppfyller kraven för nivå 3 i tillitsramverket kan det komma att bli nödvändigt att etablera övergångsregler så att dessa kan godtas inom infrastrukturen för Svensk e-legitimation till dess att en anpassning skett. Kvalificerade certifikat utgivna i enlighet med lagen (2000:832) om kvalificerade elektroniska signaturer kan, bland annat beroende på metod för utgivning, komma att uppfylla kraven för nivå 2, 3 eller 4, och därmed också användas inom infrastrukturen för Svensk e-legitimation. Då kraven i tillitsramverket är väsentligt mer specifikt framställda än de som återfinns i 4 kap. signaturlagen, följer att kvalificerade certifikat inte med automatik uppfyller någon tillitsnivå högre än 2. För en analys av konsekvenser om identitetsutfärdare endast ska tillhandahålla kvalificerade certifikat, se *bilaga 10*.

En förutsättning för att en Svensk e-legitimation ska få utfärdas föreslås dessutom vara att användaren har svenskt person- eller samordningsnummer. En e-tjänsteleverantör kan därför, när Svensk e-legitimation använts, veta att det finns möjlighet att få sådan information, i ett identitetsintyg eller efter en manuell förfrågan om en sådan påkallas från persondataskyddssynpunkt. Dessa krav införs liksom regleringen i övrigt genom avtal mellan E-legitimationsnämnden och utfärdare för anslutning till Infrastrukturen för Svensk e-legitimation, i den mån detta inte följer av författningsreglering.

E-legitimationsnämnden ska utöva tillsyn över utfärdare av Svensk e-legitimation så att tillgänglighet, kvalitet och informationssäkerhet blir säkerställda i enlighet med ett regelverk för Infrastrukturen för Svensk e-legitimation. I enlighet med regelverket ska nämnden också kunna ingripa mot missförhållanden – ytterst avveckla en utfärdare om omständigheterna är sådana att de riskerar att leda till oacceptabla konsekvenser för användare, e-tjänsteleverantörer eller andra eller rubba förtroendet för Infrastrukturen för Svensk e-legitimation.

Tillitsnivåerna specificeras närmare i *bilaga 9*.

7 Informationssäkerhet och persondataskydd

I detta avsnitt beskrivs att informationssäkerheten behöver prioriteras. Det betonas att det är av central betydelse för den föreslagna modellen för e-legitimationer att persondataskyddet kan säkerställas inom Infrastrukturen för identifiering. I avsnittet beskrivs hur flödet av personuppgifter ser ut inom infrastrukturen och vilka konsekvenser det får för personuppgiftsansvar och begränsningar av elektroniska spår, betydelsen av bättre skydd genom tekniska anpassningar, kopplingar till anvisnings- och signaturtjänster samt slutligen en bedömning av eventuell relevans i lagen om elektronisk kommunikation.

7.1 Informationssäkerheten behöver prioriteras

Enligt utkastet till regelverk för Infrastrukturen för Svensk e-legitimation ska e-tjänsteleverantörer och Identitets- och Attributsutfärdare tillämpa ett ledningssystem för informationssäkerhet, på sätt som närmare anges där (*bilaga 6*). Även i övriga delar av regelverket finns regler som är av direkt betydelse från säkerhetssynpunkt. Dessa regler har i huvudsak hämtat sin förebild i föreskrifter av Myndigheten för samhällsskydd och beredskap (MSB).

Regler om informationssäkerhet finns dessutom i den bilaga där en närmare redovisning ges av ett tillitsramverk (*bilaga 9*). Här har emellertid det internationella standardiseringsarbetet rörande e-legitimationer och identitetsfederationer varit den främsta inspirationskällan.

Reglerna i dessa två utkast överlappar delvis varandra. Materialet ska emellertid ses som ett första underlag inför en grundläggande genomlysning där inte bara Infrastrukturen för identifiering utan hela Infrastrukturen för Svensk e-legitimation måste sättas in i sitt

organisatoriska och samhälleliga informationssäkerhetssammanhang. Härvid behöver också närmare övervägas hur Infrastrukturen för Svensk e-legitimation ska fungera i förhållande till redan existerande lösningar, t.ex. dagens lösningar för e-legitimationer (under en övergångstid) och landstingens tjänstekort (SITHS). Här finns även andra kontaktytor såsom system som tillhandahåller attribut, t.ex. uppgifter om juridisk behörighet. Flera sådana system har tillkommit enligt lag eller författning – t.ex. aktiebolagsregistret – och behöver kunna verka inom ramen för den nya nationella modellen. Utöver en skyldighet att införa fungerande ledningssystem bör krav också ställas på revision och rapporteringsskyldighet; jfr redovisningen av ett tillitsramverk.

En närmare analys behövs också av hur standarderna för informationssäkerhet ska kunna tillämpas i detta sammanhang där huvudfrågan är identifiering med stöd av e-legitimationer och Identitetsintyg samt hur den praktiska hanteringen hos respektive myndighet ska kunna bli tillräckligt enkel. Härmed avses både den principiella frågan, om hur en riskanalys kan göras av system för identifiering och underskrift, och hur mindre organisationer utan egen särskild kompetens på IT-säkerhetsområdet ska kunna hantera dessa frågor inom tillgängliga kostnadsramar. Dessa frågor, som bör genomlysas i nära samverkan mellan berörda aktörer, behöver prioriteras i det fortsatta arbetet.

7.2 Persondataskyddet ska säkerställas

7.2.1 Frågor av central betydelse

Det är av central betydelse för den föreslagna modellen för e-legitimationer att persondataskyddet kan säkerställas inom Infrastrukturen för identifiering. I avsnitt 5.2 har också förklarats att det behövs vissa föreskrifter i denna del, bl.a. förbud mot registrering av vissa uppgifter och bevarande av vissa uppgifter och handlingar. Där har också en allmän föreskrift föreslagits om att så få personuppgifter som möjligt ska samlas in, lämnas ut eller annars behandlas och att inte fler uppgifter än nödvändigt får samlas in och bevaras.

Efter att utredningens delredovisning II lämnats har den registrering och annan behandling av personuppgifter som kan bli följden av Infrastrukturen för Svensk e-legitimation analyserats och flödet av uppgifter granskats. En central fråga i detta sammanhang

är vem eller vilka som ska anses vara personuppgiftsansvariga för de behandlingar som avses ske inom olika delar av Infrastrukturen för Svensk e-legitimation.

7.2.2 Inga personuppgifter i registren

Det föreslås som framgått att E-legitimationsnämnden ska föra

- ett Utfärdarregister över de Identitets- och Attributsutfärdare som ansluts till Infrastrukturen för identifiering, och
- ett E-tjänsteregister över de E-tjänsteleverantörer som ansluts till infrastrukturen för identifiering.

I dessa register ska uppgifter finnas om elektronisk adress till anslutna aktörer, vilken information respektive E-tjänsteleverantör behöver, vilka uppgifter en Identitets- eller en Attributsutfärdare kan tillhandahålla och certifikat och publika nycklar som behövs för att skydda uppgifter och kontrollera att intyg är äkta. Dessa register ska därmed inte innehålla information om kommunikation mellan användare och E-tjänsteleverantörer, innehållet i Identitets- eller Attributintyg, handlingar som ska undertecknas eller har undertecknats eller andra uppgifter som direkt eller indirekt kan hänföras till en fysisk person som är i livet.

Dessa begränsningar är av sådan betydelse från persondataskyddssynpunkt att de bör framgå av författning. I en förordning om Infrastrukturen för svensk e-legitimation föreslås därför föreskrifter om att E-legitimationsnämnden ska föra Utfärdar- och E-tjänsteregister. Vidare anges vad dessa register ska få innehålla. I tydlighetens intresse föreslås också en uttrycklig föreskrift om att registren inte får innehålla information om kommunikation mellan användare och E-tjänsteleverantörer, innehållet i intyg eller handlingar som undertecknas eller uppgifter som direkt eller indirekt kan hänföras till en fysisk person som är i livet. Dessa register får alltså inte innehålla några personuppgifter. Så länge inga personuppgifter förekommer i dessa register blir personuppgiftslagen inte tillämplig. För de fall det skulle förekomma personuppgifter i registren, blir E-legitimationsnämnden personuppgiftsansvarig.

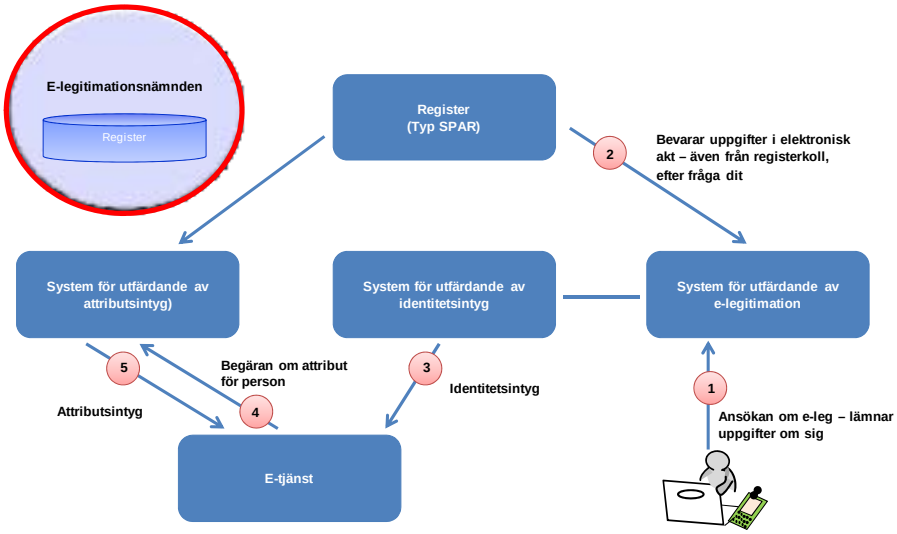
När utvecklingen av Infrastrukturen för identifiering kommit så långt att förutsättningarna klarnat i detalj bör frågan om personuppgifter kan förekomma övervägas på nytt. Skulle det därvid visa sig att det inte kan uteslutas att en uppgift kan förekomma som

indirekt kan hänföras till en individ bör den föreslagna föreskriften om förbud mot behandling av personuppgifter begränsas till sådana som *direkt* kan hänföras till en person som är i livet.

7.2.3 Personuppgifter inom infrastrukturen

Inom Infrastrukturen för identifiering ska e-legitimationer och Identitets- och Attributsintyg utfärdas och brukas så att E-tjänsteleverantörer kan göra de kontroller som behövs. Det flöde av uppgifter och handlingar som därmed uppkommer kan något förenklat beskrivas genom följande figur.

Figur 7.1 Flöde av uppgifter och handlingar



1. Användare ansöker om Svensk e-legitimation och lämnar de uppgifter som behövs till en Identitetsutfärdare som kontrollerar uppgifterna, t.ex. via SPAR-registret, och förser sina användare med privata e-legitimationer eller e-tjänstelegitimationer.
2. Utfärdaren bevarar uppgifter om sökanden i en elektronisk akt, håller dem uppdaterade och registrerar de uppgifter som behövs om spärr.

3. Utöver det system som Identitetsutfärdaren behöver för att hantera e-legitimationerna krävs med föreslagen lösning också ett system för att utfärda Identitetsintyg. När användaren loggar in i en e-tjänst som begär identifiering styrs användaren till rätt utfärdare och legitimerar sig, varefter ett Identitetsintyg skapas i dennes system för att utfärda Identitetsintyg och överförs via nät till e-tjänsten.
4. Behövs även attribut i e-tjänsten – t.ex. uppgifter från aktiebolagsregistret om juridisk behörighet – sänder e-tjänsten en begäran till Bolagsverket via Infrastrukturen för identifiering.
5. Hos Attributsutfärdaren finns ett system för utfärdande av Attributsintyg där utfärdaren skapar ett intyg och sänder det till E-tjänsteleverantören.

I de här beskrivna delarna blir det fråga om personuppgifter. Hela hanteringen tar nämligen sikte på att knyta uppgifter till en viss individ, att på tillräckligt säkert sätt se till att intyg är utfärdade av angiven utställare (en Identitets- eller Attributsutfärdare) och att säkerställa en sådan hantering att det finns skäl för mottagaren att lita på att uppgifterna är riktiga.

7.2.4 Personuppgiftsansvar och begränsningar av elektroniska spår

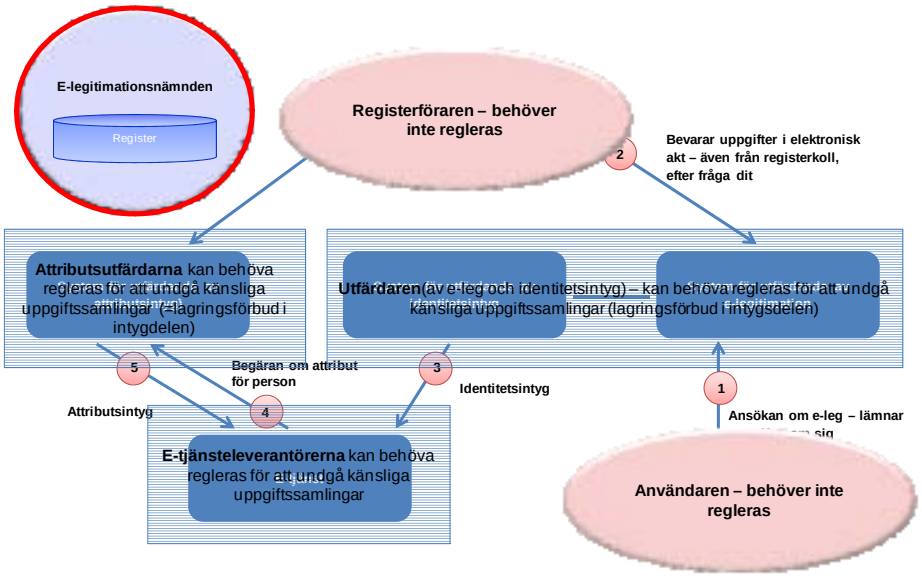
Enligt 3 § personuppgiftslagen (1998:204; PUL) är den personuppgiftsansvarig som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter. Den som behandlar personuppgifter för en personuppgiftsansvarigs räkning betecknas personuppgiftsbiträde. Bedömningar av dessa gränsdragningar med anknytning till komplex infrastruktur har nyligen gjorts av den s.k. Artikel 29-gruppen (yttrande från februari 2010, WP 169). Liknande frågor har prövats av Kammarrätten i Stockholm i en dom den 22 juni 2010 i mål mellan Försäkringskassan och Datainspektionen (mål nr 1191-09). Vidare har Artikel 29-gruppen i ett arbetsdokument den 29 januari 2003 behandlat frågor om autentiseringstjänster på Internet (WP 68).

Artikel 29-gruppen har konstaterat att det blivit svårt att göra de rättsliga bedömningarna och att tillämpa berörda begrepp i komplexa miljöer, där olika scenarier kan tänkas som omfattar personuppgiftsansvariga och personuppgiftsbiträden, ensamma eller

tillsammans, med olika grader av självständighet och ansvar. Gruppen har härvid betonat att efterlevnaden av bestämmelserna om persondataskydd måste kunna garanteras. Samtidigt har gruppen konstaterat att den konkreta tillämpningen blivit svårare när berörda IT-miljöer blivit alltmer komplexa och tjänster utvecklats över organisationsgränser och lagts ut på entreprenad för att nyttja specialiseringar och skalfördelar. Detta måste beaktas när en ny Infrastruktur för identifiering ska införas. Det följer emellertid också av Artikel 29-gruppens yttrande att parter som agerar tillsammans har en viss flexibilitet när det gäller att fördela skyldigheter och ansvar sinsemellan, så länge de garanterar en fullständig efterlevnad av reglerna om persondataskydd (s. 23). Denna möjlighet att skapa en sund fördelning av personuppgiftsansvaret bör tas tillvara så att regeringens intentioner med att införa en ny Infrastruktur för Svensk e-legitimation blir verklighet. Hit hör att förenkla, bredda och effektivisera denna struktur samtidigt som ett ökat skydd ges för enskildas personliga integritet.

Vilka aktörer som skulle kunna ha ett personuppgiftsansvar framgår något förenklat av följande figur.

Figur 7.2 Aktörer med personuppgiftsansvar



Som framgått uppkommer inget personuppgiftsansvar för E-legitimationsnämnden beträffande Utfärdar- eller E-tjänsteregistren så länge registren inte innehåller några personuppgifter. Det föreslås emellertid att nämnden också ska tillhandahålla anvisnings- och signaturtjänster se vidare avsnitt 7.2.6.

De som för register som ska användas av Identitets- och Attributsutfärdare för vissa kontroller (registerföraren i figuren ovan) är personuppgiftsansvariga för sina register och de behandlingar som de utför för att lämna ut uppgifter till utfärdarna. För detta behövs inte någon särskild reglering. De behandlingar som innehavare av e-legitimationer (se användaren i figuren ovan) utför med sin e-legitimation behöver inte heller regleras särskilt. Utformas denna hantering rätt bör den kunna avgränsas så att det varken uppkommer någon tvekan om vem som har personuppgiftsansvaret för de olika behandlingarna eller några särskilda risker från persondataskyddssynpunkt.

Därmed återstår E-tjänsteleverantörerna och Identitets- och Attributsutfärdarna (se de fyrkantiga blå rutorna i figuren ovan). Här blir det av central betydelse att respektive utfärdares *system för att utfärda intyg* inte utformas så att de kan bli en samlingsplats för nya och gamla Identitetsintyg eller för loggar och liknande som kan användas för att kartlägga en eller flera användare. Det enda som bör få bevaras är debiteringsunderlag och liknande i aggregerad form, avidentifierat så att elektroniska spår inte kan återskapas. Denna begränsning bör gälla också för vad som loggas och annars bevaras i brandväggar, intrångsdetekteringssystem och liknande som är knutna till respektive system för utfärdande av Identitetsintyg. På motsvarande sätt bör det i system för utfärdande av Attributsintyg och i kringliggande säkerhets- och kommunikationssystem få bevaras endast debiteringsunderlag och liknande i aggregerad form, avidentifierat så att elektroniska spår inte kan återskapas. En sådan begränsning föreslås i 14 § förslaget till förordningen om Infrastrukturen för svensk e-legitimation. Bestämmelsen får naturligtvis inte förstås så att den skulle hindra bevarande eller andra behandlingar som är nödvändiga för att infrastrukturen ska fungera.

På så sätt undviks att personuppgifter samlas in när det inte är nödvändigt och att känsliga personuppgiftssamlingar uppkommer hos Identitets- och Attributsutfärdare. Dessa risker skulle bli särskilt kännbara om t.ex. en utfärdare blir helt dominerande på marknaden eller dessa funktioner utkontrakteras till en och samma

underleverantör. Ges sådana system en olämplig utformning skulle det kunna skapas en närmast komplett bild av Användares kontakter och kommunikationsvägar i elektronisk miljö. Det bör härvid föreskrivas att sambearbetningar av uppgifter, som rör kommunikation för elektronisk legitimering eller elektronisk underskrift, inte får ske mellan olika Identitets- eller Attributsutfärdare. Dessa system behöver istället avgränsas och skyddas så att de kan vinna allmänhetens tillit från både säkerhets- och persondataskyddssynpunkt; se 15 § förslaget till förordningen om Infrastrukturen för svensk e-legitimation. En sambearbetning som krävs för att Infrastrukturen för Svensk e-legitimation ska fungera ska dock naturligtvis få äga rum.

Beträffande system för att utfärda Svensk e-legitimation gäller delvis detsamma. En granskning av dagens system har också visat att endast ett fåtal uppgifter lagras i dessa system och att de i praktiken inte används så att Användares transaktionsmönster eller annat liknande kan tas fram. Det utfärdaren ser är själva slagningen mot en server för att se att e-legitimationen inte är spärrad. Utfärdaren ser därvid endast vilken förlitande part som ställer frågan och – genom serienummer – vilken e-legitimation som slagningen gäller. Här kan emellertid, närmast av ordningsskäl, den begränsning som gäller för s.k. öppna system enligt 16 § lagen (2000:832) om kvalificerade elektroniska signaturer, utvidgas genom bestämmelser i förordning till att gälla även för dagens slutna system där alla aktörer är anslutna genom avtal. Enligt 16 § signaturlagen får en utfärdare inhämta personuppgifter endast direkt från den som uppgifterna avser eller med dennes uttryckliga samtycke och endast i den utsträckning som är nödvändig för att utfärda eller upprätthålla ett certifikat. Vidare föreskrivs att uppgifterna inte får samlas in eller behandlas för andra ändamål utan uttryckligt samtycke från den som uppgifterna avser. Motsvarande bör gälla för Användare av s.k. slutna system; dvs. när alla berörda aktörer är anslutna genom avtal. Identitetsintyg kan utfärdas med stöd av e-legitimationer från såväl öppna som slutna system och samma persondataskydd bör för dessa fall ges inom Infrastrukturen för identifiering. En sådan anpassning föreslås genom 13 § förslaget till förordningen om Infrastrukturen för svensk e-legitimation. En detalj i detta sammanhang är att bestämmelsen i 16 § signaturlagen – så som den formulerats – skulle kunna uppfattas som ett förbud mot behandlingar som behövs för att utfärda Identitets- eller Attributsintyg, men inte är

nödvändiga för att utfärda eller upprätthålla själva certifikatet. I denna del bör emellertid signaturlagen och bakomliggande direktiv tolkas så att utfärdande och användning av Identitets- och Attributsintyg får ses som en integrerad del i hanteringen av e-legitimationer, som inom föreslagen infrastruktur får anses nödvändig, även för att upprätthålla e-legitimationerna.

Till denna fråga om hur 16 § andra meningen signaturlagen ska förstås kommer de fall där en utfärdare vill tillhandahålla uppgifter som kan uppfattas som bra att ha för Användare eller utfärdare, men som *inte är nödvändiga* för att utfärda eller upprätthålla certifikat eller intyg. Användningen i paragrafens andra mening av ”uppgifterna” i bestämd form skulle visserligen kunna läsas så att inga andra uppgifter än de som avses i första meningen skulle få användas för andra ändamål. Detta kan emellertid knappast ha varit avsikten. Har den registrerade lämnat sitt uttryckliga samtycke till att andra uppgifter behandlas torde dessa behandlingar således få äga rum. Samma tolkning får göras av den bestämmelse som föreslagits i 13 § förslaget till förordningen om Infrastrukturen för svensk e-legitimation.

Det framstår däremot som naturligt att E-tjänsteleverantörer som mottar Identitets- och Attributsintyg ska få använda dessa inte bara för att initialt kontrollera en persons identitet och behörighet eller handlingars äkthet. De bör också få bevara intygen så länge det behövs för att styrka sådana uppgifter, t.ex. om en tvist skulle uppkomma eller behov annars skulle uppkomma av att visa att åtkomst till uppgifter och system skett på lovligt sätt eller att handlingar undertecknats av en behörig person och att texten inte har ändrats. Detta torde inte kräva någon särskild reglering.

Mot dessa begränsningar får ställas de behov av spårbarhet som kan visa sig finnas för att motverka och beivra förfalskningar och andra missbruk. E-tjänsteleverantören ställer upp de krav som en e-tjänst behöver uppfylla utifrån det skyddsvärde som den enskilda e-tjänsten anses ha. Denna bedömning blir avgörande för vilka krav på spårbarhet som ställs. Detta bör emellertid lösas genom att infrastrukturen utformas så att Identitets- och Attributsintygen kompletteras med uppgifter som visar sig nödvändiga för att skapa erforderlig spårbarhet när denna saknas hos Identitets- och Attributsutfärdare som en följd av det föreslagna förbudet mot loggar och liknande. Skulle sambearbetningar därvid behövas av uppgifter hos flera aktörer får detta ske inom ramen för den brottsutredning och de straffprocessuella tvångsmedel som kan aktualiseras.

Utformas Infrastrukturen för Identifiering på detta sätt bör frågan om fördelning av personuppgiftsansvar kunna bli förhållandevis enkel genom att personuppgiftsansvaret flyttas över stegvis som i en slags stafett när en transaktion för legitimering, underskrift, identifiering av den som legitimerat sig eller kontroll av en underskrifts äkthet flödar genom Infrastrukturen för Svensk E-legitimation. Användaren (personlig e-legitimation) eller Användarens arbets- eller uppdragsgivare (e-tjänstelegitimation) blir personuppgiftsansvarig för de behandlingar som sker hos denne, t.ex. för att hantera e-legitimationen och eventuellt bevara ett exemplar av en elektroniskt underskriven handling. Utfärdaren svarar som idag för behandlingar vid utfärdande och i tjänster för spärr och spärrkontroll samt för de uppgifter som utfärdaren i övrigt behandlar i sitt system för e-legitimationer. På liknande sätt svarar Attributsutfärdare för sina tjänster medan E-tjänsteleverantören svarar för sina behandlingar av personuppgifter i e-tjänsten – däribland för identifiering och kontroll av underskrifter samt bevarande och senare användning om behov av kontroller skulle uppkomma.

Genomförs en sådan enkel lösning i enlighet med personuppgiftslagens reglering – utan något för aktörer gemensamt personuppgiftsansvar – och stöds den av en systemuppbyggnad i enlighet med denna modell, så att gränserna blir tydliga, krävs ingen särskild författningsreglering av personuppgiftsansvaret inom Infrastrukturen för Identifiering.

Även i övrigt bör personuppgiftslagens regler kunna tillämpas utan någon särreglering.

På en punkt bör emellertid e-legitimationshanteringens och identitets- och attributsintygshanteringens många led särskilt beaktas. Om en personuppgiftsansvarig utfärdare lämnar de Användare som tilldelas e-legitimationer tydlig information om de behandlingar för identifiering och kontroll av underskrift som kan komma att ske i senare led torde myndigheter och andra som i egenskap av förlitande part behandlar personuppgifter i e-legitimationer m.m. normalt inte behöva lämna samma information på nytt. Förslag bör tas fram till hur sådan information kan utformas så att den blir tydlig och för att begränsa behovet av återkommande upprepningar i senare led (i varje e-tjänst). Själva informationen bör kunna lämnas till Användarna redan i samband med att avtal sluts med utfärdare.

7.2.5 Bättre skydd genom tekniska anpassningar

När personuppgifter ska behandlas av olika aktörer, på olika platser och med olika skyddsmekanismer och skilda administrativa lösningar har det visat sig att författningsregleringens teknikneutrala bestämmelser inte alltid fungerat som ett tillräckligt styrmedel. Persondataskyddet har kunnat motverkas redan vid valet av teknisk lösning. Forskning har därför initierats för att ta fram tekniska lösningar, byggda för att främja persondataskyddet; s.k. integritetsfrämjande teknik (eng. Privacy-Enhancing Technologies; PETs). Genom sådana lösningar kan

- behandlingen av personuppgifter minimeras,
- avidentifierade uppgifter eller pseudonymer används,
- vissa uppgifter krypteras eller blockeras, och
- policies för integritetsskydd analyseras automatiserat så att den som t.ex. besöker en webbplats enkelt kan göra välgrundade bedömningar av vilket skydd som ges.

Den Infrastruktur för identifiering som föreslås bygger på en standard (SAML) som är särskilt utformad för att kunna tillgodose sådana behov. Rätt utformad kan alltså Infrastrukturen för identifiering göra det svårare rent tekniskt att genomföra kränkningar av den personliga integriteten.

Som exempel på integritetsfrämjande teknik kan nämns bl.a. användningen av e-legitimationer med pseudonym (jfr 6 § första stycket 3 signaturlagen) som hindrar direkt identifiering och möjliggör anonyma betaltjänster till skillnad från kontokortsbaserade betalningar. I ett meddelande från Europeiska Kommissionen den 2 maj 2007 till Europaparlamentet och Rådet (KOM(2007) 228), om främjande av dataskydd genom integritetsfrämjande teknik, har Kommissionen som sin mening uttalat bl.a. att integritetsfrämjande teknik bör utvecklas och få en bredare användning och att en sådan utveckling skulle förbättra integritetsskyddet och bidra till att bestämmelserna om persondataskydd följs. Kommissionen har vidare i ett meddelande om e-förvaltningens roll i Europas framtid (KOM(2003) 567) förklarat att teknik som höjer skyddet för privatlivet bör främjas inom e-förvaltningen i syfte att skapa tilltro och förtroende så att e-förvaltningen utvecklas på ett framgångsrikt sätt.

Frågor om integritetsfrämjande teknik har nyligen behandlats också i Norges offentliga utredningar (NOU 2009:1) *Individ og integritet – Personvern i det digitale samfunnet* samt i en akademisk avhandling från Universitetet i Oslo.

Den fokusering på frågor om informationssäkerhet och autentisering som hittills präglat utvecklingen av e-legitimationer och elektroniska underskrifter bör – när området samordnas nationellt genom E-legitimationsnämnden och vidgas till utfärdande av Identitets- och Attributsintyg – kompletteras med en strategi för integritetsfrämjande teknik. Teknikens möjligheter behöver tas tillvara för att förena en framtida infrastruktur med ett effektivt persondataskydd. Vi föreslår därför att det i varje skede för att utveckla en Infrastrukturen för Svensk e-legitimation ska genomlysas om eftersträvad informationssäkerhet, effektivitet, användarvänlighet och rättssäkerhet kan uppnås genom en alternativ teknisk lösning, där riskerna för enskildas personliga integritet blir mera begränsade.

Någon författningsreglering behövs inte i denna del, utöver den redan föreslagna bestämmelsen om att så få personuppgifter som möjligt ska samlas in, lämnas ut eller annars behandlas och att inte fler uppgifter än nödvändigt får samlas in och bevaras. Däremot bör det i t.ex. E-legitimationsnämndens arbetsordning anges att en granskning ska göras i varje fas i utvecklingen av Infrastrukturen för Svensk e-legitimation av om eftersträvade mål kan uppnås genom en alternativ teknisk lösning där risken blir mindre för att enskildas personliga integritet kränks.

Dessa tekniska begränsningar blir långtgående, särskilt om de ses tillsammans med de föreslagna begränsningarna enligt författning. Ett sådant skydd är emellertid av central betydelse för att den framtida infrastrukturen ska vinna allmän tillit och inte riskera att missbrukas genom att elektroniska spår skapas, bevaras och sambearbetas för andra ändamål än dem för vilka den nya infrastrukturen tillskapats. Det blir en viktig uppgift att genomlysa dessa begränsningar och vad som krävs inom den nya infrastrukturen så att den föreslagna regleringen inte hindrar behandlingar som krävs för att skydda infrastrukturen mot angrepp och att granska och åtgärda fel.

7.2.6 Anvisnings- och signaturtjänster

Enligt förslaget till definitioner menas med anvisningstjänst det tekniska och administrativa stöd som E-legitimationsnämnden lämnar åt en E-tjänsteleverantör för att användare ska kunna välja e-legitimation. I vissa fall kommer användaren att kunna se att en särskild tjänst för anvisning används, i andra fall inte. Så som denna tjänst fungerar är det naturligt att se E-legitimationsnämnden som underleverantör av den till respektive tillhandahållare av e-tjänster (se avsnitt 5.4).

Eftersom E-tjänsteleverantören därmed får anses tillhandahålla Anvisningstjänsten och bestämma om och hur den ska införas för aktuell e-tjänst bör ett personuppgiftsansvar för de uppgifter som behandlas där anses vila på respektive E-tjänsteleverantör, med E-legitimationsnämnden och en eventuell underleverantör till nämnden som personuppgiftsbiträden. Avsikten är emellertid att införa sådana tekniska lösningar att de uppgifter som behandlas i en Anvisningstjänst inte kan kopplas till person så att personuppgifter anses föreligga personuppgiftslagens mening. Det återstår att i det fortsatta arbetet se om persondataskyddet med teknisk hjälp kan drivas så långt.

Beträffande en signeringstjänst blir det av avgörande betydelse att ta tillvara de möjligheter som integritetsfrämjande teknik kan ge så att handlingar m.m. inte samlas och bevaras på ett ställe. I denna del har utvecklingsarbetet emellertid inte kommit tillräckligt långt för att en närmare analys av persondataskyddet ska bli verkningsfull. Frågan får därför tas upp i det fortsatta arbetet.

7.2.7 Lagen om elektronisk kommunikation

Enligt 1 kap. 4 § lagen (2003:389) om elektronisk kommunikation (LEK) gäller lagens bestämmelser elektroniska kommunikationsnät och elektroniska kommunikationstjänster med tillhörande installationer[1] och tjänster samt annan radioanvändning. Den föreslagna Infrastrukturen för Svensk e-legitimation innefattar inte något tillhandahållande av allmänna kommunikationsnät. Därmed återstår frågan om E-legitimationsnämnden, Identitets eller Attributs-

[1] Med tillhörande installation menas enligt 1 kap. 7 § LEK anordning, funktion eller annat som inte utgör men har samband med en elektronisk kommunikationstjänst eller ett elektroniskt kommunikationsnät, och som möjliggör eller stöder den tjänsten eller tillhandahållandet av tjänster via det nätet.

utfärdare eller E-tjänsteleverantörer kan komma att tillhandahålla någon *allmänt tillgängliga elektronisk kommunikationstjänst*.

Enligt 1 kap. 7 § LEK menas med *elektronisk kommunikationstjänst* en tjänst som vanligen tillhandahålls mot ersättning och som helt eller huvudsakligen utgörs av överföring av signaler i elektroniska kommunikationsnät. Den föreslagna Infrastrukturen för Svensk e-legitimation torde falla utanför tillämpningsområdet för LEK redan till följd av att de tjänster som E-legitimationsnämnden, Identitetsutfärdare, Attributsutfärdare och E-tjänsteleverantörer ska tillhandahålla inte innefattar ”överföring av signaler”. För att sådan överföring ska anses föreligga behöver de ha rådighet över signalen (bäraren av informationen) och därmed ha inflytande över faktorer som t.ex. överföring och kvalitet. Den föreslagna lösningen innebär emellertid att såväl E-legitimationsnämnden som Identitetsutfärdare, Attributsutfärdare och E-tjänsteleverantörer förlitar sig på att det finns andra kommunikationstjänster som fungerar som bärare för den egna tjänsten; se vidare Post- och telestyrelsens rapport den 11 mars 2009 (PTS-ER-2009:12) s. 20 ff.

8 Verksamhetsplan för E-legitimationsnämnden

Detta avsnitt börjar med att beskriva omvärlds- och marknadsutvecklingen för e-legitimationer samt marknadens drivkrafter. En ny svensk affärsmodell för e-legitimationer beskrivs med start i dess utgångspunkter, nyttor och incitament som skapas, betalströmmar till nämnden och mellan aktörerna i Svensk e-legitimation beskrivs också. E-legitimationsnämndens förslag till mål för verksamheten tydliggörs, dess roll och nämndens målsättningar vad gäller bearbetning av modellens aktörer samt tjänster. Ett förslag till nämndens ansvarsområden och organisation presenteras följt av en genomförandeplan vilken bland annat lyfter fram vikten av att etablera nära samråd med modellens aktörer för att säkra bästa tänkbara upplägg samt en smidig övergångslösning. Avsnittet avslutas med att gå igenom nämndens ekonomi och budget samt vilka risker som är förknippade med den fortsatta utvecklingen.

8.1 Omvärldsutveckling

Ett stort antal länder arbetar aktivt med lösningar för hantering av e-legitimationer. Exempelvis Finland var tidigt ute och introducerade redan 1999 ett identitetskort med e-legitimation. Lösningen gavs ut av regeringen till alla medborgare över 18 år, dock nyttjades inte existerande infrastruktur och lösning som etablerats av de finska bankerna, vilket innebar att spridningen blivit mycket begränsad.[1] Nederländerna har skapat en central part för att samordna och hantera e-legitimationer, kallad eHerkenning, vars roll verkar ha stora likheter med E-legitimationsnämnden i Sverige. eHerkenning kommer till en början att överta DigiDs roll som

[1] Electronic identity in Finland: ID cards vs. bank IDs, Teemu Rissanen, 6 March 2010.

autentisering för organisationer och företrädarskap för organisationer vid inloggning till statliga e-tjänster.[2]

Belgien har under ett antal år försett sina medborgare med elektronisk ID-kort med e-legitimation som skall omfatta en majoritet av befolkningen.

I Norge ger bankerna ut e-legitimationer som baseras på centralt lagrade nycklar för identifiering och signering, det så kallade Norska BankID som främst används för att logga in på och utnyttja tjänster i Norska nätbanker. Samtidigt har ett antal aktörer i en nyligen avgjord upphandling getts uppdraget att ge ut personliga e-legitimationer för åtkomst till myndighetstjänster.

SuisseID är en nyligen introducerad nationell e-legitimationsmodell baserat på federering med SAML. Medborgare som registrerar sig får ett unikt SuisseID som inte är kopplat till personnummer etc. Det finns för närvarande fyra ackrediterade identitetsutfärdare och antalet tjänster växer kontinuerligt. Den finansiella modellen bygger på att en kostnad är relaterad till utfärdande av e-legitimationer, vilken tas ut av slutanvändarna. Användningen av e-legitimationer stimuleras av att en stor del av den initiala avgiften återbetalas efter ett visst antal användningar.[3]

Inom EU projektet STORK (Secure idenTity acrOss boRders linKed) utvecklas och testas en lösning för att knyta samman identifieringsinfrastrukturer i medlemsstater för att möjliggöra gränsöverskridande e-förvaltningstjänster för medlemsstaternas medborgare och organisationer. Gränsöverskridande e-legitimationer anses nödvändiga för att reducera den administrativa bördan inom Europa, vilket anses kunna förbättra områdets konkurrensposition.[4] Prioriterade e-tjänsteområden inom EU är främst riktade mot startande och bedrivande av affärsverksamhet, studier, arbete samt att bo och pensionera sig inom unionens gränser.

Inom ramen för STORK-projektet samt det så kallade Kantarainitiativet utvecklas ett tillitsramverk som grund för klassning av olika e-legitimationers tillitsnivåer (se även avsnitt 6 rörande tillitsnivåer). Dessa aktiviteter utgör grunden för skapandet av en ny ISO standard (ISO 29115) för ett tillitsramverk som ska vara färdigt 2013.

---

[2] <http://www.eherkenning.nl/>.
[3] <http://www.suisseid.ch/index.html?lang=fr>.
[4] STORK, *Towards pan-European recognition of electronic IDs (eIDs), D2.2 – Report on legal interoperability*, 2009-02-23.

EU kommissionens IDABC program (Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens) avslutades i december 2009 och efterföljs av det nya ISA programmet (Interoperability Solutions for European Public Administrations). ISA programmet skall ta vid och bygga på erfarenheterna som vunnits i IDABC-programmet. Vid STORK-projektets avslutande i maj 2011 kommer ISA-programmet att ta över ansvaret för att den infrastruktur som tagits fram inom STORK-projektet drivs vidare.

Tjänstedirektivets införande ställer krav på elektronisk utväxling av information med myndigheter, företag och medborgare i Europa. Inom ramen för den svenska kontaktpunkten bedrivs i dag utveckling och pilotprojekt med syfte att stödja svenska myndigheters befattning med elektroniskt underskrivna handlingar från utlandet. Detta område berörs även av EU projekt som SPOCS (Simple Procedures Online for Cross-border Services) och PEPPOL (Pan-European Public Procurement Online).

Marknaden och dess utveckling

Som tidigare nämnts har vi i Sverige en relativt lång och god erfarenhet av att nyttja e-legitimationer under en ca 10-årsperiod. Den offentliga sektorn har utgjort en viktig del av denna marknad. På senare tid har det skett en snabb utveckling inom banksektorn som kommit att bli en stor användare av e-legitimationstjänster exempelvis i form av BankID. I dagsläget finns det ca 3,8 miljoner e-legitimationer utgivna från BankID, Nordea och TeliaSonera[5]. Vilket resulterar i en hög penetration av e-legitimationer inom viktiga grupperingar i samhället.

E-tjänster har kommit att bli en mycket viktig del i många offentliga organisationers sätt att arbeta, många organisationer har även som mål att erbjuda mer och mer tjänster via Internet. För många av dessa tjänster utgör e-legitimationer en väsentlig förutsättning för hanteringen.

Med utgångspunkt från direktivets önskan om att kostnaden för nuvarande aktörer om möjligt ej ska öka har utredningen försökt identifiera storleken på dagens marknad för e-legitimationer. En preliminär uppskattning av marknadens storlek har gjorts utifrån

[5] Synpunkter på rapporten Verksamhetsplan för e-legitimationsnämnden del II, Finansiell ID-teknik, Swedbank, Handelsbanken.

uppgifter från Kammarkollegiet vilka har analyserats och där icke relevanta kostnader dragits ifrån. Resultatet av denna preliminära skattning är att den offentliga marknaden för användandet av e-legitimation i Sverige uppgår till ca 15–20 MSEK exklusive mervärdesskatt. Denna uppskattning behöver säkras i det fortsatta arbetet i nämnden. Delar av denna marknad baseras i dag på fastprisöverenskommelse medan andra delar bygger på löpande användningskostnad det kan även finnas en del signeringstjänster vilka ingår i dessa siffror.

Marknadsvolymen för e-legitimationer har historiskt utvecklats i relativt långsam takt, men förväntas växa i framtiden allt eftersom mognadsgraden och nyttorna för användare och aktörer i modellen ökar. I dag används e-tjänster av myndigheter, landsting och kommuner i olika stor utsträckning och med stor variation i antalet erbjudna tjänster. Bland landets 290 kommuner använder i dag bara ett fyrtiotal e-tjänster som kräver e-legitimering, tyngdpunkt ligger på tjänster inom skola och barnomsorg. För landsting används e-tjänster framförallt genom funktionen Mina Sidor där individen kan boka och omboka tider, förnya recept och ställa frågor. E-tjänster används i dag inom 15 av de 20 (inklusive två regioner) lanstingen i Sverige där de flesta tjänster har stora likheter med varandra mellan respektive landsting.

Det finns en stor variationsrikedom i såväl vilken utsträckning dessa aktörer har e-tjänster, hur de är utformade samt till vilken grad de utnyttjas, delvis baserat på respektive aktörs uppdrag. Mer än 25 av landets myndigheter erbjuder i dag e-tjänster till individer och/eller organisationer.[6] Bland dessa 25 myndigheter återfinns de största, med flest antal anställda och flest interaktioner med medborgarna. Det bör dock finnas en potential även bland resterande 89 % av Sveriges 259 operativa myndigheter[7].

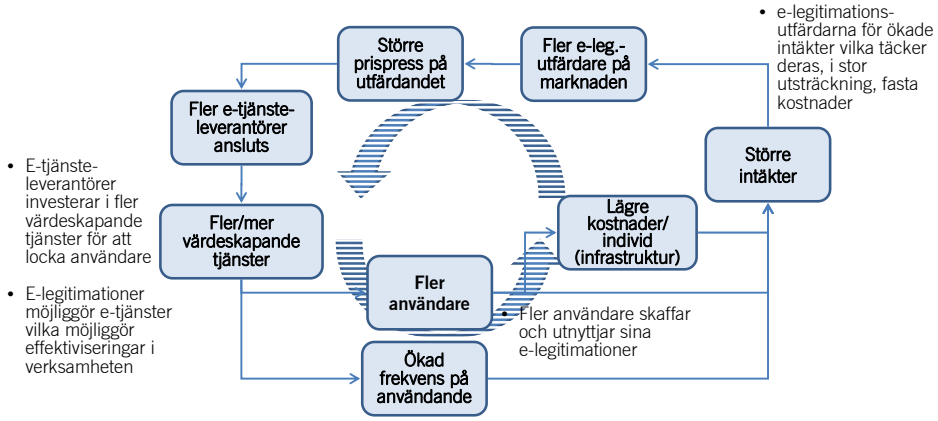
Tittar man framåt kan en fortsatt tillväxt även på andra områden som att kunna identifiera vem en aktör är det kan vara i en tjänst, kopplat till sociala medier, vem som gör uttalanden i olika frågor, etc. en utveckling som kan ske såväl inom offentlig som privat sektor.

Marknaden för e-legitimationer, dvs. behovet av dessa för att kunna utföra olika e-tjänster drivs av faktorer så som utbudet av attraktiva tjänster, antalet utfärdade e-legitimationer, frekvensen i e-legitimationernas användning, arbetsprocesser inom offentlig och

[6] <www.e-legitimation.se>, samt ett antal av e-tjänsteleverantörernas hemsidor.
[7] *Så enkelt som möjligt för så många som möjligt*, SOU 2010:62, 2010.

privat sektor etc. i en modell med en rad beroendeförhållanden, förenklat åskådliggjort i bilden nedan.

Figur 8.1 Faktorer och beroenden med påverkan på marknadens utveckling



En viktig startpunkt är att e-tjänsteleverantörer utvecklar e-tjänster vilka användare finner attraktiva, dvs. som fyller ett behov, är enkla att använda, och därmed används frekvent. Det ska dock noteras att utvecklingen av själva e-legitimationen endast utgör en mindre del i ett betydligt mer omfattande utvecklingsarbete som kan omfatta system och arbetsprocesser hos den offentliga sektorns aktörer för att e-tjänster ska kunna lanseras och nå sin fulla potential.

Identitetsutfärdarna underlättar hanteringen och användandet genom att utveckla attraktiva erbjudanden med bra och användarvänliga lösningar samt främjar ett stort utfärdande av e-legitimationer för att skapa en hög penetration på marknaden bland användarna. Tillgång till attraktiva e-tjänster vilka upplevs tillföra ett värde för användarna, kombinerat med en bred spridning av e-legitimationer förväntas öka användningen vilket i sin tur ökar intresset bland fler att utöka sina aktiviteter på området. Denna omställning vilken kommer att ske successivt skapar förutsättningar för att effektivisera och öka kvaliteten inom den offentliga sektorn, men kan åtminstone under en period komma att öka kostnaderna i kundservice.

För att denna kedja av förändringar ska komma att fungera effektivt är det viktigt att det tidigt skapas en kritisk massa av e-

legitimationer och attraktiva e-tjänster, annars finns risk för att intresset för e-tjänster förblir begränsat.

8.2 En ny svensk affärsmodell

8.2.1 Utgångspunkter

E-legitimationsnämnden ska i den nya modellen samordna statens arbete med och användning av metoder och tjänster för elektronisk identifiering och legitimering. Myndigheten ska säkerställa att nödvändiga tjänster och funktioner för e-legitimationer finns tillgängliga för den offentliga förvaltningen. Detta kommer att ske i enlighet med den nationella modell för Svensk e-legitimation som presenterats tidigare.

Direktivet beskriver att statliga myndigheters, landsting och kommuners användning av tjänster för identifiering och signering ska, liksom nu, finansieras av e-tjänsteleverantörerna. De samlade avgiftsintäkterna ska i så stor utsträckning som möjligt finansiera de samlade kostnaderna som nämnden har för att handla upp och tillhandahålla tjänster för identifiering och signering. Avgiftsfinansieringen bör, om möjligt, leda till lägre totala kostnader för såväl varje statlig myndighet och kommun som förvaltningen som helhet.

Förslaget till verksamhet inom Svensk e-legitimation har byggts utifrån en affärsmodell vilken syftar till att skapa förutsättningar och incitament för såväl innehavare av e-legitimationer (personer i såväl rollen som invånare som representanter för en organisation) att använda e-legitimationer samt för e-tjänsteleverantörer, organisationer som ser ett behov av e-legitimationer för sitt interna bruk, identitetsintygsutfärdare och attributsutfärdare att utveckla tjänster kring detta.

Utformningen av affärsmodellen vilar på de utgångspunkter som fastslagits för Svensk e-legitimation och E-legitimationsnämndens verksamhet

- Affärs- och prismodellen ska vara enkel, transparent och långsiktig. Den ska leda till mer förutsägbara och om möjligt lägre kostnader för offentlig sektor än dagens ramavtalsmodell
- Användarna i form av privata individer eller organisationer ska kunna välja leverantör av e-legitimationer

- Modellen ska primärt fokusera på offentlig sektor men vara utvecklings- och skalbar för att därigenom kunna skapa förutsättningar för en bra hantering av e-legitimationer även i övriga delar i samhället, vilket underlättar för såväl användare, e-tjänsteleverantörer samt leverantörer till modellen
- Det ska vara enkelt för en statlig myndighet, landsting eller kommun att få tillgång till tjänster för elektronisk identifiering och signering. En statlig myndighet, landsting eller kommun ska genom en part få tillgång till alla tjänster som omfattas av modellen
- En statlig myndighet, landsting eller kommun ska i så liten utsträckning som möjligt själv behöva ha kompetens och funktioner för att kunna använda tjänster för elektronisk identifiering och signering i verksamheten
- Modellen bör, om det med hänsyn till övriga förutsättningar är möjligt, stödja teknikneutralitet samt bygga på lösningar som utvecklas av marknaden. Befintliga e-legitimationer bör, eventuellt med viss anpassning för att klara vald tillitsnivå, fungera i den nya modellen
- Modellen ska skapa förutsättningar för ökad valfrihet och mångfald vad gäller utfärdare av identitetsintyg och e-legitimationer. Alla aktörer på marknaden som uppfyller relevanta krav ska kunna bli leverantörer i den nya modellen

I tillägg till punkterna ovan föreslår utredningen ett den framtida affärsmodellen bygger på att;

- Den preliminära uppskattningen av marknadens storlek har gjorts utifrån uppgifter från Kammarkollegiet, utifrån ramavtal eID 2008 och eID 2004, vilka har analyserats och där icke relevanta kostnader dragits ifrån. Denna uppskattade marknadsstorlek utgör grunden för den ersättning som inledningsvis utgår till identitetsutfärdarna, utan avdrag för E-legitimationsnämndens kostnader, antaget 100 % övergång till den nya modellen
- Tillväxt i marknaden skapas genom att nya e-tjänsteleverantörer ansluts och betalar en årsavgift
- Avgifter inom Svensk e-legitimation inklusive grundersättningen till identitetsutfärdarna bestäms på årsbasis

- In- och utbetalningar i Svensk e-legitimation sker kvartalsvis
- Aktörer, identitetsutfärdare, e-tjänsteleverantörer och attributsutfärdare, ansluts kvartalsvis
- Nya aktörer som ansluts till Svensk e-legitimation betalar del av årsavgiften baserat på kvarvarande kvartal vid inträde
- Identitetsutfärdare erhåller ersättning baserat på andel av totala antalet utfärdade identitetsintyg per unik användare och tidsenhet
- Den summa som tilldelas identitetsutfärdarna i ersättning uppgår till marknadens uppskattade storlek, samt 50 % av den årliga tillväxten beräknad utifrån föregående års totala ersättning, upp till att nämnden når full finansiering av kostnader relaterade till drift av Svensk e-legitimation. Därefter tilldelas identitetsutfärdarna 100 % av tillväxten
- Beroende på vilken lösning som väljs för signering kan den finansiella modellen kopplad till det se olika ut. Vid en central lösning så kan det komma att krävas ytterligare en betalström som finansierar den tjänsten
- Nämndens budget består av två typer av kostnader
  - Operativa kostnader, relaterade till drift av Svensk e-legitimation och dess tjänster
  - E-legitimationsnämndens övriga kostnader, ej direkt kopplade till drift och tjänster
- De operativa kostnaderna bör på sikt helt och hållet finansieras via avgifter. De indirekta kostnaderna täcks även fortsättningsvis via statliga anslag

8.2.2 Affärs- och betalmodell

Affärsmodellen bygger på de roller och aktörer vilka förväntas ingå i modellen för Svensk e-legitimation som presenterats i avsnitt 3.2, dvs. användaren (individen i form av privatperson alternativt anställd i en organisation), E-tjänsteleverantörer (myndigheter, landsting och kommuner), identitetsutfärdare och attributsutfärdare.

Nyttor och kostnader i den nya modellen

E-tjänsteleverantörerna i form av myndigheter, landsting och kommuner kommer genom etableringen av modellen för Svensk e-legitimation att få tillgång till ett förenklat förfarande vad gäller e-legitimationer, en viktig förutsättning för att utveckla e-tjänster. Ett större utbud av e-tjänster skapar förutsättningar för ökad servicegrad och kvalitet i e-tjänsteleverantörernas kundrelationer och därmed nöjdhet bland kunder och användare. I tillägg till ökad servicegrad kan e-tjänsterna även möjliggöra verksamhetsmässiga förbättringar inte minst i processarbetet i den egna organisationens i form av ökad kvalitet och produktivitet samt kanske även ett mindre behov att i egen regi ha specialist kompetens på området. Exempel på detta kan vara korrekt ifyllda blanketter, onlinestöd vid ifyllande av blanketter för vissa tjänster, en kvalitativ dialog mellan användare och e-tjänsteleverantör, korrekt elektroniskt ifyllda deklarations- och skattehandlingar, anmälan om skolgång och sjukanmälan.

Införandet av Svensk e-legitimation innebär att nuvarande e-tjänsteleverantörer behöver se över och i vissa fall modifiera och uppdatera sina e-tjänster i enlighet med den nya modellen. E-tjänsteleverantörerna bör även identifiera och ta hänsyn till eventuella risker i förberedelserna inför övergång till den nya modellen. Detta kommer att ställa krav på såväl kompetens och resurser under en övergångsfas. Det kan vidare noteras att det stora jobbet med att utveckla och driva e-tjänster inte är förknippat med e-legitimationer utan snarare med system- och processutveckling i övrigt vilket ligger utanför denna utredning.

Användaren, den privatperson alternativt anställd, som har tillgång till en e-legitimation och därmed får tillgång till de tjänster vilka e-tjänsteleverantörerna erbjuder. Användaren kan själv välja vilken av de godkända e-legitimationsutfärdarna som han eller hon vill använda för att legitimera sig. Ökat utbud och attraktivitet i erbjudna tjänster kombinerat med en trovärdig och förenklad hantering av e-legitimationer förväntas öka frekvensen i användarnas nyttjande av e-tjänster.

Identitetsutfärdare kommer att behöva anpassa sin verksamhet till de regler som gäller inom modellen för att bli godkänd som leverantör. För dagens leverantörer kan detta komma att innebära exempelvis att sätta upp en identitetsutfärdartjänst, anpassning till SAML, ansökan om medlemskap i Svensk e-legitimation. Vilken

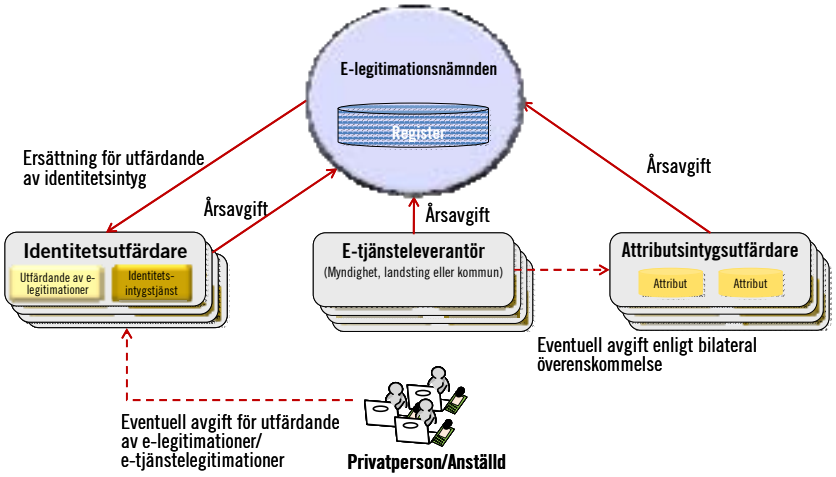
grad av förändring detta innebär kan variera mellan aktörerna. Förändringarna samt själva övergångsperioden då två parallella system behöver drivas kan komma att vara förknippade med vissa kostnader och kanske även risker aktörerna behöver bära. Målsättningen är att den nya modellen kommer att skapa en väl fungerande marknad som kommer att växa genom att nya myndigheter, landsting och kommuner utvecklar e-tjänster och ansluter sig till modellen. I tillägg till den offentliga sektorn ska E-legitimationsnämnden även verka för att Svensk e-legitimation utvecklas till att även omfatta det privata näringslivet.

Attributsutfärdarna innehar en viktig roll i modellen då de kompletterar den grundläggande rollen för identifiering med att vid behov även tillhandahålla annan viktig information. Svensk e-legitimations infrastruktur kan innebära ett förenklat förfarande även för dessa utfärdare.

Betalströmmar

Betalströmmarna i Svensk e-legitimation har definierats för att stödja målsättningarna i kommittédirektivet. Det finns en önskan om att modellen i så hög grad som möjligt ska vara avgiftsfinansierad, samt att e-tjänsteleverantörerna ska få en förutsägbar och om möjligt lägre avgift. Betalströmmarna i modellen åskådliggörs i figuren nedan.

Figur 8.2 Betalströmmar i Svensk e-legitimation



Bilden visar på två olika typer av betalströmmar, markerade med heldragna respektive streckade linjer. De heldragna linjerna visar på betalströmmar vilka går via och vars prisnivå styrs av E-legitimationsnämnden. Denna struktur möjliggör en betalmodell i flödet in till nämnden från e-tjänsteleverantörerna och en annan för utbetalning av ersättning till identitetsutfärdarna, vilket bidrar till dynamik i marknaden.

Den andra typen av betalströmmar, i bilden markerade med streckade linjer, visar på potentiella betalströmmar som ligger utom E-legitimationsnämndens ansvar. För dessa gäller separata överenskommelser mellan de involverade parterna.

E-tjänsteleverantörerna föreslås även fortsättningsvis stå för större delen av den offentliga sektorns finansiering av modellen. För att möta direktivets krav om ökad förutsägbarhet i de offentliga aktörernas kostnader föreslås e-tjänsteleverantörerna betala en fast avgift till E-legitimationsnämnden baserad på för landsting och kommuner antal invånare samt för myndigheter antal anställda. Till detta kommer dels att kommuner och landsting betalar samma avgift per invånare samt att det för respektive kategori finns en fastställd miniminivå. Betalningen är inte avhängig i vilken grad organisationen har e-tjänster vilka kräver e-legitimationer, ej heller i vilken grad de utnyttjas.

Modellen möjliggör för e-tjänsteleverantörerna att uppskatta sina kostnader på förhand samtidigt som den innebär ett incitament att utveckla och sätta i drift e-tjänster i syfte att öka servicegraden mot användare men även för att vidareutveckla, höja kvaliteten i och effektivisera den egna verksamheten.

Avgiften syftar till att täcka såväl tillsyn, relevanta administrativa kostnader hos nämnden samt ersättning till identitetsutfärdarna.

Utifrån den uppskattade storleken på dagens marknad för användande av e-legitimationer kombinerat med uppskattade kostnader för nämndens operativa verksamhet har ett förslag tagits fram på avgiftsmodell. I denna modell föreslås följande avgifter

- Landsting och kommuner betalar 0,50 kronor per invånare och har en minimiavgift på 10 000 kronor per år
- Myndigheter betalar ca 350 kronor per anställd och har en minimiavgift på 10 000 kronor per år

Kostnaden för landsting och kommun uppgår till 50 öre per invånare. Nivån är satt för att stimulera utvecklingen och användandet av e-tjänster som kräver e-legitimation inom landsting och kommuner samt för att främja en övergång till den nya modellen. Minimiavgiften innebär att kommuner med mindre än 20 000 invånare samt de mindre myndigheterna får betala denna minimiavgift för att delta i Svensk e-legitimation. Modellen kan vidare exemplifieras genom att beskriva vad de fem största myndigheterna, landstingen och kommunerna som i dag nyttjar e-legitimationstjänster skulle betala:

Tabell 8.1 Föreslagna årsavgifter för de största aktörerna

Myndigheter	**Antal anställda**	**Avgift** [1]
Försäkringskassan	12 500	4 200 000
Skatteverket	10 800	3 636 000
Arbetsförmedlingen	9 875	3 320 000
Länsstyrelserna	6 500	2 180 000
Lantmäteriet	2 397	800 000
Landstinget	**Antal invånare**	**Avgift**[1]
Stockholm	1 974 827	980 000
V:a Götaland	1 570 000	780 000

Region Skåne	1 231 062	610 000
Östergötland	415 990	200 000
Jönköping	329 884	160 000
Kommun	**Antal invånare**	**Avgift[1]**
Stockholm Stad	832 641	590 000
Linköping	144 934	100 000
Örebro	134 466	90 000
Helsingborg	128 569	90 000
Umeå	114 300	80 000

[1] Alla avgifter har avrundats nedåt till närmaste 10 000-tal.

Den största fördelen med denna modell är att den i linje med utgångspunkter för den nya modellen är enkel och förutsägbar. Beräkningen av kostnaderna utifrån antal anställda respektive antal invånare utgör en modell som används inom andra områden i offentlig sektor. Tillväxten i marknaden beräknas som att varje nytillkommen e-tjänsteleverantör tillför marknaden en avgift. Den fasta avgiften, vilken ej är relaterad till de facto antal utnyttjade e-legitimationer fungerar som ett incitament för respektive aktör att utveckla och driva på användandet av e-tjänster. Denna avgiftsmodell har likheter med avgiftsmodell för access till Internet.

En nackdel med modellen kan vara att den riskerar att bli något statisk där eventuella stordriftsfördelar och produktivitetsförbättringar på e-legitimationssidan inte fullt ut slår igenom. Detta hanteras dock via att den fasta avgift som e-tjänsteleverantören betalar inte är knuten till nivån på användandet, en beräknad kostnad per identitetsintyg kommer därmed att sjunka när volymen användande ökar. En alternativ modell skulle kunna ha varit att relatera avgiften för e-legitimationer till den volym legitimationer som används, en sådan modell har dock bedömts svårförenlig med direktivets krav.

Med den fördelning av avgifterna som presenterats kommer marknaden det första fulla verksamhetsåret, med antagande om att alla nu anslutna e-tjänsteleverantörer gör över till Svensk e-legitimation, att uppgå till knappt 25 MSEK. Av detta belopp föreslås ca 20 MSEK (det preliminära antagandet om marknadens storlek) utbetalas till identitetsutfärdarna som ersättning, resterande

5 MSEK går till nämnden för att bidra till att täcka de operativa kostnaderna och .

Identitetsutfärdarna betalar en årlig avgift som ersättning för att delta i modellen för Svensk e-legitimation. Denna avgift syftar till att täcka såväl relevanta administrativa kostnader hos nämnden som en avgift för den årliga tillsynen. Identitetsutfärdaren kommer i tillägg att i samband med inträde i modellen, alternativt vid förändrad roll i modellen, behöva intyga att regler och krav för medlemskap i Svensk e-legitimation kan uppfyllas. Detta sker genom att en extern part utför en revision, t.ex. en revisionsbyrå. Avgiften relaterad till detta är utom nämndens kontroll och betalningen sker direkt till den externa parten. Den del av avgiften som relateras till tillsyn gäller förutsatt att identitetsutfärdaren följer och lever upp till Svensk e-legitimations regelverk. Om aktören gör överträdelser som föranleder särskild tillsyn tas en särskild avgift ut.

Årsavgiften för identitetsutfärdarna beslutas av E-legitimationsnämnden föreslås i ett inledande skede uppgå till 20 000 SEK, med följande uppdelning:

- Administration: hantering av metadata och årligt registerunderhåll. Uppskattad initial avgift 10 000 SEK
- Tillsyn: Uppskattad initial avgift 10 000 SEK

Privata identitetsutfärdare föreslås erhålla en ersättning som uppgår till den marknadsandel av totalt antal utfärdade identitetsintyg per unik användare under en definierad tidsperiod som respektive aktör utgivit relaterat till E-legitimationsnämndens totala intäkt från e-tjänsteleverantörerna med avdrag för relevanta operativa kostnader, i utgångsläget beräknas detta uppgå till ca 20 MSEK vid 100 % anslutning. Ersättningen betalas ut kvartalsvis. I tillägg till den grundläggande ersättningen kan en extra tillväxtbaserad ersättning tillkomma vilken utbetalas årligen. Den tillväxtbaserade ersättningen fördelas så att E-legitimationsnämnden fram till att de direkta operativa kostnader samt investeringsbehov täckts tilldelas 50 % av marknadsökningen och resten går till identitetsutfärdarna. När nämnden nått full kostnadstäckning för direkta operativa kostnader samt ränta och avskrivningar på investeringar tilldelas 100 % av tillväxten identitetsutfärdarna.

Baserat på utfallet ett visst år bestämmer nämnden den grundläggande ersättningen för efterföljande år.

Då respektive aktörs ersättning bygger på uppnådd marknadsandel av antal utfärdade identitetsintyg per unik användare och tidsenhet ligger det i identitetsutfärdarens intresse att vinna marknadsandelar genom att skapa spridning på och hög användning av sina e-legitimationer.

Identitetsutfärdaren har rätt att ta betalt för utfärdandet av e-legitimationer till privatpersoner. Det är ett civilrättsligt mellanhavande mellan utfärdaren och privatpersonen och ligger därmed inte inom ramen för E-legitimationsnämnden. E-tjänstelegitimationer förutsätts finansieras av arbetsgivarna.

Skatteverket utfärdar idag ID-kort vilka inkluderar en e-legitimation och Rikspolisstyrelsens nationella ID-kort är förberedda för samma syfte. Dessa ID-kort skiljer sig inte ur ett affärsmodellperspektiv från andra typer av e-legitimationer, dock anser utredningen att det vore önskvärt att det införs valfrihet för användaren. Detta skulle för användaren innebära en möjlighet att välja vilken identitetsutfärdare bland samtliga medlemmar i Svensk e-legitimation som man önskar ha på denna typ av legitimationer.

Identitetsutfärdare som utfärdar e-tjänstelegitimationer och kan styrka att Svensk e-legitimations regler och krav uppfylls och följs samt betalar avgift kan delta i modellen utan att vara en del av valfrihetssystemet. Detta kan gälla aktörer med en väl utvecklad existerande infrastruktur och ett redan etablerat användande, så som är fallet med t.ex. SITHS. Medlemskap i Svensk e-legitimation utan att vara en del av valfrihetssystemet är dock inte ersättningsgrundande.

Vid utfärdandet av tjänstelegitimationer till organisationer kan olika upplägg bli aktuella beroende på behov. I de fall organisationen endast är intresserad av den mest grundläggande formen för tjänstelegitimationer bör stora likheter finnas med utfärdandet av sådana för privatpersoner. Vid utfärdandet av tjänstelegitimationer tillkommer dock ofta en rad andra tjänster som exempelvis kopplingar till organisation, roll, rutiner för reservförfaranden för att hantera förluster av e-tjänstelegitimationer, inpassering, fysiska legitimationer med fotografi, SIS-märkning etc. Specifikationer kring vad dessa e-tjänstelegitimationer ska innehålla kan variera mellan olika organisationer varför de ur ett upphandlings- och utförarperspektiv föreslås hanteras separat. E-legitimationsnämnden avser ej att styra över detta.

Attributsutfärdarna kan delta i modellen och på så sätt underlätta användandet av deras e-tjänster. För en aktör att vara införd i

registret bör innebära att affärsmöjligheterna för attributsutfärdarna ökar. Attributsutfärdarnas möjlighet att ta betalt för attributsintyg regleras inte av Svensk e-legitimation. Eventuell intäkt från e-tjänsteleverantörerna vid betaltjänster sker enligt bilateralt överenskomna affärsupplägg.

Årsavgiften ska täcka administrativa kostnader vid hantering av metadata samt årligt registerunderhåll och uppskattas till 5 000 SEK. Avgiftens nivå motiveras med att det är viktigt för modellens framgång att relevanta attributsutfärdare ansluts.

Alla prisnivåer angivna ovan är förslag för tillitsnivå 3 enligt tillitsramverket. Om och i så fall när fler tillitsnivåer introduceras i modellen kan ytterligare prisnivåer komma att införas relaterade till dessa. I det fallet finns möjlighet att påverka de sammanlagda kostnaderna genom att nyttja lägsta möjliga tillitsnivå efter tjänstens behov.

Ytterligare utredning är nödvändig innan beslut kan tas kring hur signaturtjänsten ska hanteras och därmed eventuella konsekvenser för hur tjänsten ska hanteras i affärsmodellen. Väljs exempelvis en central modell och tjänsten ses som en extratjänst som e-tjänsteaktörer kan välja att nyttja kommer tjänsten antagligen att finansieras separat via en avgift.

Avgifter beskrivna i detta avsnitt beslutas av E-legitimationsnämnden.

8.3 Verksamhetsmål

8.3.1 E-legitimationsnämndens mål

Målsättningen med bildandet av E-legitimationsnämnden är att skapa förutsättningar för en väl fungerande Svensk e-legitimation med stark tillit såväl i Sverige som internationellt. Svensk e-legitimation ska möjliggöra för såväl användare av e-tjänster som e-tjänsteleverantörer i offentlig sektor att på ett effektivt sätt etablera och nyttja e-tjänster vilka kräver e-legitimationer. Nämnden ska vidare verka för att en parallell modell skapas inom näringslivet med målsättningen att användarna ska kunna använda sina Svensk e-legitimationer även där.

E-legitimationsnämnden inrättas som ett självständigt beslutande organ med uppgift att samordna myndigheternas befattning

med e-legitimationer, elektroniska underskrifter och gemensamma elektroniska tjänster.

8.3.2 E-legitimationsnämndens roll

E-legitimationsnämnden ska samordna myndigheternas, landstingens och kommunernas arbete med och användning av metoder och tjänster för elektronisk identifiering och signering, vilket har beskrivits i avsnitt 3. E-legitimationsnämnden ska säkerställa att nödvändiga tjänster och funktioner för e-legitimationer finns tillgängliga för den offentliga förvaltningen. I detta ingår:

- att styra, utveckla och svara för den verksamhet som faller inom ramen för Svensk e-legitimation. Hit hör, i de delar verksamheten inte regleras i lag eller förordning
- att säkerställa att nödvändiga tjänster och funktioner (t.ex. identitetsintygsgivare, anvisningstjänster samt register över godkända identitetsintygsgivare och e-tjänsteleverantörer) finns tillgängliga för förvaltningen
- att tillse att de aktörer som ansluts följer regelverket för Svensk e-legitimation

Även i fortsättningen bör förvaltningen använda sig av tjänster och metoder som utvecklas och tillhandahålls av aktörer på marknaden. Det är viktigt att nämndens organisation och verksamhet utformas på ett sådant sätt att goda förutsättningar ges för konkurrens och för utvecklingen av ytterligare tjänster.

Nämnden bör därför tillhandahålla tjänster till myndigheter, landsting och kommuner endast om det är nödvändigt för att säkerställa förvaltningens tillgång till elektronisk identifiering och signering under de förutsättningar och med de mål som angivits. Utförandet av sådana tjänster bör i normalfallet upphandlas på marknaden.

Nämnden ska samverka med berörda myndigheter, landsting och kommuner samt näringsliv, leverantörer och andra intressenter. Särskilt viktigt är att kommuner och landsting i sådan samverkan får möjlighet att utvecklas i samma riktning som de statliga myndigheterna.

8.4 Verksamhetsområden

8.4.1 Användare och medlemmar

Användare

Målsättningen är att främja en ökad penetration av e-legitimationer i samhället samt att främja användandet av dessa. Användarna ska därigenom på ett effektivt och säkert sätt få tillgång till samt kunna använda e-tjänster vilka kräver e-legitimering eller signering. Detta gäller såväl för privatpersoner som anställda vilka i sin yrkesroll behöver kunna legitimera sig för att utföra vissa aktiviteter elektroniskt.

E-tjänsteleverantörer

Målsättningen med verksamheten är att etablera en modell för Svensk e-legitimation som e-tjänsteleverantörerna känner stor tillit till och vilket förenklar för dem i utveckling och drift av e-tjänster där e-legitimationer är ett krav. Det ligger i E-legitimationsnämndens intresse, och nämnden föreslås verka för, att samtliga myndigheter, landsting och kommuner för vilka denna typ av e-tjänster är relevanta ansluter sig snarast till modellen.

Identitetsutfärdare

Målsättningen med den nya modellen är att skapa valfrihet för användaren och mångfald vad gäller identitetsutfärdare. Nämnden ska verka för inrättandet av ett valfrihetssystem där användare kan välja e-legitimationsutfärdare och där nuvarande så väl som nya identitetsutfärdare kan anpassa alternativt bygga sin verksamhet efter definierade krav med mål om anslutning till Svensk e-legitimation.

Attributsutfärdare

Attributsutfärdarna är en viktig aktör i Svensk e-legitimation och står för mycket av det utökade värdet. Målsättningen är att i modellen ansluta de attributsintygsutgivare som är av allmänt

intresse och kan tillföra modellen viktig information, som exempelvis Bolagsverket och Socialstyrelsen.

Dagens leverantörer av E-förvaltningsstödjande tjänster innehar en viktig roll i modellen inte minst i form av att stödja offentlig sektor med det arbete som bedrivs med att förbättra och ta fram nya e-tjänster, med att göra nödvändiga förändringar under övergångsfasen till den nya modellen samt som eventuella attributsutfärdare i den nya modellen.

8.4.2 Tjänster

Inom Svensk e-legitimation finns ett antal grundläggande tjänster, där vissa tillhandahålls via E-legitimationsnämnden och andra direkt från godkända medlemmar i modellen, vilka kan indelas i följande grupper

- Registertjänster
- E-legitimationer
- Anvisningstjänst
- Attributsintygstjänst
- Signeringstjänst

Registertjänster

En central del i modellen för Svensk e-legitimation utgörs av de register som innehåller information om identitetsutfärdare (utfärdare av e-legitimationer och identitetsintyg), e-tjänsteleverantörer och attributsutfärdare. Denna funktion eller tjänst är viktig för att skapa tillit mellan aktörerna inom Svensk e-legitimation. Registren publicerar bl.a. varje aktörs (identitetsutfärdare, e-tjänsteleverantör och eventuella attributsintygsgivare) certifikat så att utställarens elektroniska stämpel kan verifieras i varje identitets- och attributsintyg. E-legitimationsnämnden ansvarar för utfärdarregistret och säkrar att det kommer alla e-tjänsteleverantörer tillhanda. Nämnden ansvarar även för e-tjänsteleverantörsregistret för offentlig sektor, vilket identitetsutfärdarna är beroende av samt för att verka för en lösning kommer tillstånd inom näringslivet.

De register som E-legitimationsnämnden ansvarar för ska vara i drift i samband med att nämnden blir operativ, troligen under våren 2012 och senast vid halvårsskiftet.

Den tekniska driften av Svensk e-legitimations register för identitetsutfärdare samt e-tjänsteleverantörer ska upphandlas av E-legitimationsnämnden.

E-legitimationer

E-legitimationer utfärdas till individer och organisationer vilka är godkända som medlemmar i Svensk e-legitimation.

Utfärdare av e-legitimationer till privatpersoner ska upphandlas enligt inrättande av ett valfrihetssystem. E-legitimationsnämnden bidrar i såväl upphandlings- som ansökningsprocesserna för identitetsutfärdare. E-legitimationstjänsten ska finnas tillgänglig i anslutning till att nämnden går i operativ drift.

Användningen av e-tjänstelegitimationer som har upphandlats utanför valfrihetssystemet, via avtal direkt mellan de involverade parterna utan nämndens inblandning, är inte ersättningsgrundande.

Anvisningstjänst

Anvisningstjänsten anvisar användaren utifrån utfärdarregistret till sin identitetsutfärdare för att på ett enhetligt sätt förenkla användningen för den enskilda användaren. Anvisningstjänsten kan vara såväl central som lokal.

Utveckling av en anvisningstjänst handlas upp externt. Drift av anvisningstjänst bör kunna ingå som en del i den upphandling som görs kopplat till drift och underhåll av nämndens register.

Attributsintygstjänster

Attributstjänster kompletterar uppgifter om såväl fysiska som juridiska personer utöver den information som lämnas i identitetsintyg. Attributstjänster som anses vara av allmänt intresse ansluts till infrastrukturen för Svensk e-legitimation. E-tjänsteleverantörer kan även inhämta attributsintyg från attributstjänster som ej är medlemmar i Svensk e-legitimation genom att upprätta bilateral

tillit och överenskommelse mellan e-tjänsteleverantör och attributsintygsutgivare.

De mest centrala attributsintygsutgivarna, primärt medlemmarna i Svensk e-legitimation, bör vara anslutna i samband med att E-legitimationsnämnden går i operativ drift.

Signeringstjänst

En signeringstjänst kommer att ingå som en del i E-legitimationsnämndens serviceutbud. Det krävs ytterligare utredningsarbete innan det är klart hur signeringstjänsten ska se ut och därmed även hur en realistisk plan ser ut när den kan vara tillgänglig på marknaden. Driften av e-signeringstjänsten kommer antagligen att upphandlas externt, formerna för detta ingår som del i den fortsatta utvecklingen av tjänsten.

8.4.3 Internationell samverkan och eventuellt kompletterande områden

E-legitimationsnämndens verksamhet kan i tillägg till områdena ovan i framtiden efter beslut även komma att innehålla andra delar. Exempel på detta kan vara det utvecklingsarbete som sker inom EU kring internationell standardisering och samverkan med andra EU-länder. Ett flertal aktiviteter kan komma att inordnas under e-legitimationsnämndens verksamhet för att uppfylla denna instruktion

- Den svenska implementeringen av STORK-projektet för gränsöverskridande användning av e-legitimationer föreslås övergå i fortsatt drift efter det att STORK-projektet avslutas i maj 2011. Den fortsatta driften behöver förvaltas och eventuellt utvecklas för att möta framtida behov
- En standard för ett tillitsramverk som avses ligga till grunden för ett svenskt tillitsramverk för svensk e-legitimation skall tas fram inom ramen för ISO 29115. Aktiviteten beräknas pågå minst fram till och med 2013
- EU-projekt inom området såväl som aktiviteter inom EU-programmet ISA behöver bevakas och kan komma att kräva ett svenskt engagemang

- Den tjänst som utvecklas av Tillväxtverket inom ramen för den svenska kontaktpunkten för att stödja svenska myndigheters befattning med signerade handlingar från utlandet behöver förvaltas efter utveckling och pilotdrift. I framtiden kan det övervägas om nämnden ska få ansvaret att förvalta denna tjänst
- Standarder och normer för e-legitimationer och elektroniska signaturer kommer under 2011-2013 att på uppdrag av EU-kommissionen att utvecklas för att stödja införandet av tjänstedirektivet. Här finns behov av svenskt engagemang och påverkan

Även andra områden kan i den fortsatta utvecklingen komma att övervägas huruvida de bör ingå som en del i nämndens verksamhetsområde, exempelvis;

- Standardisering och regelverk för stämpelcertifikat
- Standardisering och regler för servercertifikat

8.4.4 Upphandling

E-legitimationsnämnden ska inrätta ett valfrihetssystem för svensk E-legitimation samt upphandla tekniska tjänster mm. Vid både inrättandet av valfrihetssystemet och upphandlingen av tekniska tjänster bör E-legitimationsnämnden, utifrån eventuellt regeringsbeslut om att Kammarkollegiet ska stödja E-legitimationsnämnden med dessa upphandlingar, ta tillvara på Kammarkollegiets kompetens och erfarenheter inom relevanta områden. Vid fastställande av hur stödet från Kammarkollegiet lämpligen ska utformas får bland annat beaktas de uppgifter som E-legitimationsnämnden ska ha avseende valfrihetssystemet under avtalstiden.

När det gäller inrättande av valfrihetssystemet är denna upphandlingsform tämligen ny och det finns därför inte så stor samlad erfarenhet på området. Detta förhållande måste beaktas vid planeringen av den tid och de resurser som kan beräknas erfordras för arbetet. Inför ett inrättande är det väsentligt att E-legitimationsnämnden fortsätter med ett samråd med aktörerna på marknaden.

Valfrihetssystemet måste innefatta de tekniska och andra krav som ska ställas på Identitetsutfärdarna för anslutning. Dessa krav ska vara förutsägbara och rimliga och de måste inom ramen för den

föreslagna lösningen i största möjliga utsträckning beakta de förhållanden som gäller för marknaden i dag så att det blir ett naturlig utvecklingssteg från dagens lösningar till den lösning som föreslås av utredningen. Särskild uppmärksamhet bör ägnas åt de frågeställningar som kan uppkomma vid en övergång från dagens struktur till den nya strukturen.

En fortsatt utveckling kan förväntas ske på det tekniska området och det är viktigt att de villkor som gäller för identitetsutfärdarna utformas så att de möjliggör förändringar av villkoren föranledd av teknisk och annan utveckling. För att uppnå förutsebarhet och god planering måste samråd ske med identitetsutfärdarna även på detta område.

Den ersättningsmodell som föreslagits tar sin utgångspunkt i dagens förhållande. Området kan dock förväntas få en stark tillväxt med nya e-tjänster och fler användare. En sådan utveckling kan innebära att det under avtalstiden för valfrihetssystemet kommer att finnas behov av att i delar förändra och utveckla ersättningsmodellen. Även på detta område måste avtalsvillkoren för anslutning till valfrihetssystemet innefatta möjlighet till utveckling av ersättningsmodellen. Sådana förändringar måste dock ske som ett resultat av förhandlingar mellan parterna. För att inte hämma en utveckling på området måste både E-tjänsteleverantörer och Identitetsutfärdare långsiktigt uppfatta ersättningarna som skäliga och rimliga.

8.5 Nämndens organisation

8.5.1 Nämndens uppbyggnad

Elektronisk identifiering och signering är centrala funktioner för e-förvaltningen för samhället. Det är viktigt att myndigheten har ett högt förtroende och en hög legitimitet i hela den offentliga förvaltningen, näringslivet samt hos de enskilda användarna. Det är vidare angeläget att verksamheten bedrivs med en stor grad av självständighet gentemot de myndigheter som använder nämndens tjänster eller vars verksamhet i övrigt påverkas av dess beslut. Verksamheten ska organiseras som en nämndmyndighet som placeras hos Skatteverket.

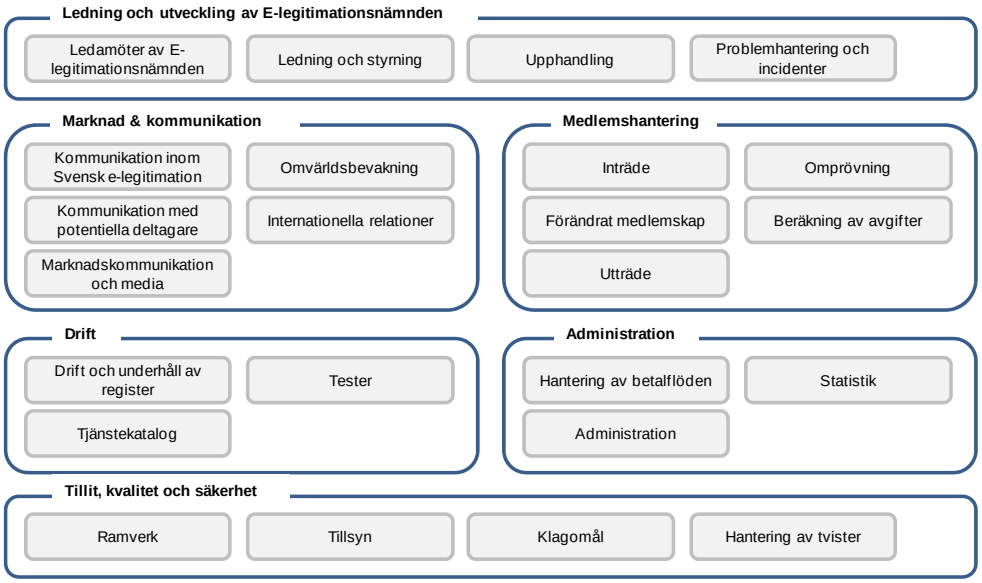
Enligt författningsförslaget ska E-legitimationsnämnden ledas av en nämnd. Nämndens ordförande och övriga ledamöter utses av regeringen för en bestämd tid.

E-legitimationsnämnden ska ha ett kansli med ansvar för det löpande arbetet. Kansliet ska ha en kansliansvarig som utses av myndigheten i samråd med Skatteverket. Skatteverket ska också upplåta lokaler för myndighetens kansli samt sköta administrativa och handläggande uppgifter åt myndigheten.[8] Personalen ska vara anställd i Skatteverket. Kansliansvarig ska ansvara för arbetsledning avseende personalens arbete med nämndens uppgifter.

8.5.2 Nämndens ansvarsområden

E-legitimationsnämndens verksamhet kan delas in i ett antal huvudprocesser och ansvarsområden som krävs för att driva nämndens verksamhet, se översiktsbild nedan.

Figur 8.3 Nämndens ansvarsområden



[8] Promemoria, 2010-09-06.

Ansvarsområdena indikerar den typ av kompetens som krävs för att utöva nämndens roll och därmed vilken typ av kompetens som behöver rekryteras. Beskrivningen av roller ska dock ej direkt översättas i bemanningens storlek. E-legitimationsnämnden kan vidare besluta att utföra delar av dessa uppgifter i egen regi medan andra handlas upp externt.

Ledning och utveckling av E-legitimationsnämnden

Ledamöter av E-legitimationsnämnden

E-legitimationsnämnden ska ledas av en nämnd. Ledamöterna deltar i nämndmöten tillsammans med kansliansvarig och fattar beslut i de frågor där nämnden har beslutanderätt. Mötena leds av nämndens ordförande. Beroende på vilka ämnen som avhandlas kan även ytterligare personer adjungeras vid specifika tillfällen. Beslut och överenskommelser dokumenteras och distribueras.

Ledning och styrning

Enligt förslaget får myndigheten i arbetsordning eller särskilda beslut överlämna till ordföranden eller kansliansvarig att avgöra ärenden som är av administrativ art och andra ärenden som är av sådan art att de inte behöver prövas i nämnden och eventuellt skyndsamma ärenden. Genom detta förslag skapas möjlighet till en högre grad av flexibilitet vid avgörande av ärenden som är av administrativ eller enklare art.

Upphandling

E-legitimationsnämnden ansvarar för att genomföra de upphandlingar som krävs för att utföra nämndens uppdrag. Nämnden bör för dessa upphandlingar, utifrån eventuellt regeringsbeslut om att Kammarkollegiet ska stödja E-legitimationsnämnden med dessa upphandlingar, ta tillvara på Kammarkollegiets kompetens och erfarenheter inom relevanta områden.

Problemhantering och incidenter

Problem som rapporteras in till E-legitimationsnämnden ska hanteras inom ansvarsområdet för styrning och ledning. Problemhanteringsprocessen inleds med att ett problem eller en avvikande händelse identifieras av E-legitimationsnämnden eller av medlemmar i modellen. Rapporterade händelser dokumenteras i en logg, därefter följer en analys och en kategorisering av rapporterade problem. Rapporterade incidenter skickas vidare till incidenthanteringsprocessen.

Incidenter kan rapporteras in av identitetsutfärdare, e-tjänsteleverantörer och användare. Alla rapporterade incidenter registreras i en logg eller ett rapporteringssystem och prioriteras av E-legitimationsnämnden. Nämnden ansvarar för att genomföra nödvändiga aktiviteter för att hantera incidenten, i samråd med/ tillsammans med den part som rapporterade incidenten, samt att utföra eventuella uppföljningsaktiviteter.

E-legitimationsnämnden ansvarar för att regelbundet sammanställa incidenter, relaterade åtgärder för att hantera incidenten samt förslag för att undvika liknande händelser i framtiden. Dessa sammanställningar presenteras sedan för E-legitimationsnämndens ledamöter.

Medlemshantering

Inträde

Nya parter kan vara intresserade av att ansluta sig till Svensk e-legitimation. De aktörer som önskar bli medlemmar visar sitt intresse genom att skicka en ansökan till E-legitimationsnämnden och en process som omfattar följande steg inleds, se även regelverket för Svensk e-legitimation:

- En identitetsutfärdare som önskar delta genomför nödvändiga aktiviteter för att bevisa att reglerna uppnås. Erforderliga kontroller genomförs av extern part, t.ex. en revisionsfirma.
- Intyg och dokumentation lämnas in till nämnden som kontrollerar dess riktighet
- Om reglerna är uppfyllda utgår en avgift som ska täcka administration och tillsyn för kommande verksamhetsår

- När kraven uppfyllts och avgiften betalats blir identitetsutfärdaren godkänd som medlem och registren uppdateras med relaterad metadata
- Identitetsutfärdare kan därefter använda begreppet Svensk e-legitimation

Förändrat medlemskap

Aktörer som är deltagare i Svensk e-legitimation kan komma att ändra omfattningen på sitt medlemskap, exempelvis gå från att vara en attributsutgivare till att bli en identitetsutfärdare. En sådan förändring innebär att aktören behöver genomgå de procedurer som krävs för att bli godkänd i sin nya roll.

Utträde

En aktör som är medlem i Svensk e-legitimation kan välja att lämna denna. Formerna för detta regleras i regelverket för Svensk e-legitimation.

Ompröva medlemskap

Situationer kan uppkomma då E-legitimationsnämnden har misstankar om att en deltagare i Svensk e-legitimation inte uppfyller modellens legala, affärsmässiga eller tekniska krav. Nämnden har då möjlighet att initiera en kontroll för att undersöka om så är fallet. Deltagarorganisationen är förpliktigad till att godkänna denna kontroll och att bidra med den information och expertis som krävs för att E-legitimationsnämnden ska kunna fullfölja sitt uppdrag.

Beräkning av avgifter

E-legitimationsnämnden ansvarar inom ramen för Svensk e-legitimation för att anpassa, vidareutveckla och använda modellen för att beräkna hur betalströmmarna inom Svensk e-legitimation ska se ut. Nämnden ska erhålla underlag från såväl e-tjänsteleverantör i form av underlag för fakturering samt faktisk användning samt utfärdande statistik från respektive identitetsutfärdare. Beräkning av

avgifter och ersättningsnivåer inom Svensk e-legitimation sker på årsbasis enligt fastställda riktlinjer. Fakturering och utbetalning sker på kvartalsbasis. Alla förändringar ska godkännas av E-legitimationsnämnden.

Ett system för uppföljning av antal utfärdade identitetsintyg etableras exempelvis genom att respektive identitetsutfärdare regelbundet rapporterar aktuellt utfall. I modellen för hur ersättningen beräknas bör mekanismer för att förhindra möjligt missbruk etableras. Hur modellen konkret ska utformas och upprättas bör utredas vidare efter att nämnden etablerats.

Marknad och kommunikation

E-legitimationsnämnden ansvarar för att bearbeta marknaden, sprida budskapet om Svensk e-legitimation och kommunicera med externa parter. En viktig roll är att inrätta och driva ett antal forum och aktiviteter för samråd med viktiga intressenter inte minst e-tjänsteleverantörer inom offentlig sektor, identietsutfärdare, attributsutfärdare, användare samt initiera ett samarbete mellan aktörer inom det privata näringslivet, se vidare under genomförandeplan.

Kommunikation inom Svensk e-legitimation

Tillit är ett huvudtema inom Svensk e-legitimation vilket bland annat förutsätter en god information kring regler, förändringar och andra viktiga frågor.

Kommunikation med potentiella deltagare

E-legitimationsnämnden ska kommunicera kring och uppbygga ett intresse för modellen bland potentiella medlemmar.

Marknadskommunikation och media

E-legitimationsnämnden ska verka för att Svensk e-legitimation framställs på ett sakligt, korrekt och positivt sätt i media.

Omvärldsbevakning

Myndigheten ska på ett övergripande plan följa utvecklingen inom området. Myndigheten ska följa utvecklingen såväl i Sverige som internationellt när det gäller tekniska och administrativa lösningar för elektronisk identifiering och signering.

Internationella relationer

Myndigheten ska vara Sveriges kontaktpunkt gentemot organ med motsvarande ansvar i andra länder. Myndigheten föreslås ansvara för att utveckla samarbetet och informationsutbytet med dessa organ samt delta i internationellt standardiseringsarbete.

Drift

Drift och underhåll av register

E-legitimationsnämnden ansvarar för att registren och dess innehåll är korrekt och tillförlitligt. Den tekniska driften av registren kan komma att upphandlas från extern part. Nämnden innehar relevant kompetens inom teknik och säkerhet för att kunna hantera frågeställningar samt kunna fungera som en professionell beställare.

Tjänstekatalog

E-legitimationsnämnden ansvarar för att sammanställa en tjänstekatalog för Svensk e-legitimation och för att hålla denna uppdaterad. Tjänstekatalogen presenterar de tjänster som nämnden tillhandahåller samt presenterar gränssnitt, ansvar och servicenivåer.

Testning

Autentiseringsmekanismer och protokoll som används inom Svensk e-legitimation ska testas för säkra att de fungerar bland dem som är anslutna.

Administration

Inom nämndens ansvarsområde ingår även viss stödverksamhet.

Hantering av betalflöden

Nämnden hanterar administrativt definierade betalflöden i modellen, i form av anslutningsavgifter som tas in från e-tjänsteleverantörer, identitetsutfärdare och attributsutfärdare samt utbetalningar som görs till främst identitetsutfärdare.

Administration

Inom administration ingår nödvändig stödverksamhet för myndigheten så som ekonomi, lön, HR och IT. För att hantera dessa områden används stöd från värdmyndigheten Skatteverket.

Statistik

Detta arbetsområde innebär att information från aktörerna inom Svensk e-legitimation samlas in och sammanställs till rapporter kring användning av modellens tjänster. Nätverket av aktörer används för att samla in information, som sedan anonymiseras och sprids för att tydliggöra användandet inom modellen. Rapporterna fungerar som en informationskälla kring utveckling av systemet, prioritering av initiativ samt för att upptäcka operationella problem.

Tillit, kvalitet och säkerhet

E-legitimationsnämnden ska verka för att Svensk e-legitimation karaktäriseras av tillit, kvalitet och säkerhet.

För nämndens arbete kommer det bland annat att vara viktigt att känslig information hanteras gäller strikt konfidentialitet och tystnadsplikt för E-legitimationsnämndens anställda. Viktigt är att nämndens arkiv måste utformas med hänsyn till detta. Nämnden bör vidare utveckla en strategi för integritetsstödjande teknik.

En beredskapsfunktion inordnas för att möta kraven i förordning (2006:942) om krisberedskap och höjd beredskap. Inom denna roll ingår vidare ett ansvar för nämnden totala

informationssäkerhetsperspektiv vilket bl.a. omfattar fungerande processer för risk- och sårbarhetsanalyser, kontinuitetsplanering och krisberedskap, granskning och uppföljning (tillsyn). Dessa processer bör täcka hela infrastrukturen för svensk e-legitimation, och inte endast myndighetens egen interna informationshantering.

Ramverk

E-legitimationsnämnden upprätthåller och förvaltar ramverket för Svensk e-legitimation inklusive regler, tekniska standarder, processer för verksamheten, krav på informationssäkerhet, former för övergångsarbetet etc.

Tillsyn

Regelbunden tillsyn sker av alla aktörer inom modellen för Svensk e-legitimation. Detta för att säkra att aktörerna som verkar i inom modellen uppfyller de fastställda kraven.

Verktyget för styrning av informationssäkerheten utanför myndigheten är tillitsramverket, via de civilrättsliga avtalen med utgivarna av svensk e-legitimation samt federationsoperatören.

Andra kontroller (för behörighetsstyrning, säkerhet i systemutveckling, informationsklassificering, fysisk säkerhet m.m.) avgränsas till att endast innefatta myndighetens interna arbete.

Klagomål

Klagomål som inkommer från någon av medlemsorganisationer sammanställs och analyseras regelbundet. Vid återkommande klagomål genomförs detaljerade analyser för att komma tillrätta med problemet.

Hantering av tvister

Nämnden ansvarar för att tillhandahålla stöd för att lösa frågor när aktörerna inte är eniga och att testa överensstämmelse med tekniska normer och förmågan att samverka (s.k. interoperabilitet).

8.6 Genomförandeplan

8.6.1 Uppbyggande av verksamheten

Framgång i att etablera en ny lösning för e-legitimationer och nå en bred acceptans för Svensk e-legitimation och E-legitimationsnämnden kommer att ställa stora krav på såväl förankring, design och genomförande.

E-legitimationsnämnden inrättas från första januari 2011. Verksamhetsplan syftar till att stödja nämnden i att bygga upp och etablera verksamheten samt att skapa strukturen för Svensk e-legitimation. Nämndens utveckling under kommande period kan delas in i tre faser

- Uppbyggnad av E-legitimationsnämnden, primärt 2011–12
- Lansering av Svensk e-legitimation och övergång till ny modell, primärt 2012–13
- Vidareutveckling och expansion Svensk e-legitimation, primärt 2013–14

De tre faserna beskrivs på kommande sidor och avslutas med att väsentliga aktiviteter sammanfattas i en tabell.

Uppbyggnad av E-legitimationsnämnden (2011–2012)

Under den första fasen, uppbyggnad av E-legitimationsnämnden, kommer ett stort antal aktiviteter att initieras för att skapa den framtida modellen. I detta ingår en lång rad praktiska frågor som måste hanteras, exempelvis nämndens arbete, uppbyggnad av kansliets verksamhet, bemanning av viktiga roller, etc.

En annan viktig del i arbetet kommer vara att driva ett antal utvecklings-, konkretiserings- och planeringsfrågor. Vissa av dessa frågor kommer att drivas av nämnden och dess kansli medan andra föreslås hanteras i samråd med andra intressenter.

Nämnden föreslås vidare etablera och driva ett antal forum för samråd med de viktigaste intressenterna i Svensk e-legitimation i syfte att säkerställa bästa tänkbara lösning för och införande av Svensk e-legitimation. I dessa samrådsaktiviteter kan ingå såväl att informera, fånga synpunkter som att diskutera viktiga förutsättningar för den nya modellen, lösa och hantera konkreta frågor, vidareutveckla och förfina såväl tekniska som affärsmodellrelaterade förslag. Därtill bör eventuella risker identifieras

och hanteras. Samrådsaktiviteterna bör vidare bidra till att konkretisera viktiga steg i en genomförande- och övergångsplan till den nya modellen.

Genom dessa samråd skapas förutsättningar för att belysa viktiga frågor ur flera perspektiv, skapa involvering samt förutsättningar för att driva genomförandet med så lite påverkan som möjligt på användare, e-tjänsteleverantörer, identitetsutfärdare och andra aktörer. I sådana diskussioner kan det uppkomma förslag vilka kan innebära att ändringar behöver göras i det förslag till upplägg som utredningen presenterar.

Samrådsaktiviteterna bör initieras tidigt och sannolikt omfatta såväl offentliga e-tjänsteleverantörer som nuvarande och tänkta framtida identitetsutfärdare, centrala attributsutfärdare och eventuella andra viktiga intressenter. En särskild samverkan med Sveriges kommuner och landsting är angelägen för att säkerställa att gjorda investeringar i infrastruktur för gemensam e-tjänstelegitimation på detta område kan nyttjas i den framtida modellen.

Ett annat viktigt område under denna fas kommer att vara att driva arbetet med att få tillstånd de juridiska förutsättningar som krävs för den nya modellen. Vilket bl a kommer att omfatta att vidareutveckla, förankra och förbereda för lagförändringar, framtagande av underlag för avtal, förbereda och genomföra ramavtalsupphandlingar, etc.

Lansering av Svensk e-legitimation och övergång till den nya modellen

Under 2012, senast vid halvårsskiftet, förväntas förutsättningarna vara på plats för att en lansering av Svensk e-legitimation ska vara möjlig. Denna tidpunkt är viktig då den sammanfaller med att möjligheten att göra avrop baserat på Kammarkollegiets ramavtal eID 2008 och E-förvaltningsstödjande tjänster 2010 försvinner.

Lanseringen och övergången till Svensk e-legitimation kommer sannolikt att ske stegvis över en period. Under denna period kommer två parallella modeller och system behöva drivas, den nuvarande och Svensk e-legitimation. Detta dels för att minska påverkan på användarna och aktörer men även på grund av att det kan finnas giltiga avrop av e-legitimationstjänster via Kammarkollegiets ramavtal under upp till fyra år efter ramavtalens utgång. Det sannolika är därför att det sker en gradvis övergång till den nya

modellen och därmed en över tiden ökande volym som hanteras i Svensk e-legitimation. Det är även tänkbart att vissa e-tjänsteleverantörer som är starkt beroende av fungerande e-tjänster själva väljer att genomföra en gradvis övergång.

Målsättningen är att övergången till Svensk e-legitimation ska kunna genomföras utan att e-tjänsteleverantörerna behöver betala dubbel avgift. Nya e-tjänsteleverantörer bör anslutas till Svensk e-legitimation och nämnden bör därför genomföra riktade insatser mot denna målgrupp för att säkra att så sker. Parterna bör arbeta för att övergångsperioden ska bli så kort som möjligt för att därigenom begränsa behovet av dubbla lösningar, kostnadsdrivande samt eventuell osäkerhet kring hur en framtida modell ska fungera och därmed risk för tempoförlust i införandet av nya e-tjänster i offentlig sektor.

En viktig faktor är att identitetsutfärdarna ansluts så snart som möjligt i samband med modellens lansering. De är centrala för modellens funktion och utan deras medverkan är det inte möjligt att uppnå avsedd nytta.

Från och med lanseringsfasen bör statistik och erfarenheter kring användande, intäkter och kostnader att samlas in och analyseras.

De forum för samråd som bildats under uppbyggnadsfasen kan under denna period helt eller delvis omvandlas till att främst omfatta anslutna aktörer. Utredningens förslag är att separata forum bildas för offentliga och privata e-tjänsteleverantörer, identitetsutfärdare, attributsutfärdare och samt andra relevanta grupperingar som exempelvis användare. E-legitimationsnämnden ansvarar för forum med koppling till den offentliga sektorn, samt för att initiera arbetet med ett motsvarande forum för den privata sidan.

Dessa forum fokuserar på att diskutera gemensamma frågor, modellens vidareutveckling, problem samt aktuella frågor. Det övergripande syftet är att säkra att marknadens aktörer kan göra sin röst hörd och att viktiga frågor lyfts och hanteras.

Därtill föreslås att E-legitimationsnämnden skapar en ”Svensk e-legitimationsdag” som ett återkommande årligt arrangemang. Denna aktivitet syftar till att samla alla typer av aktörer inom både den offentliga och den privata modellen för samverkan kring e-legitimations och e-signeringsfrågor. Denna dag bör även innefatta internationellt deltagande och erfarenhetsutbyte. För löpande kommunikation kommer E-legitimationsnämndens hemsida utgör

en viktig kanal för dialog och samverkan. Formerna för ovan nämnda samverkansaktiviteter bör vidareutvecklas och förankras så snart som möjligt efter nämndens bildande.

Vidareutveckling och expansion av Svensk e-legitimation

När Svensk e-legitimation är i drift, verksamheten fungerar och ett antal aktörer är anslutna vidtar nästa fas att ansluta ytterligare aktörer till modellen.

Utifrån erfarenheter, statistik och annan information som samlats in kan även visa på behov av att vidareutveckla affärsmodell, teknik eller juridik. Justeringarna kan innebära både förändringar i modellen som sådan och förändrade kostnads- och ersättningsnivåer, bland annat baseras på ny information om marknadsvolym, fördelning mellan typer av aktörer, frekvens på användning, tillväxt, utveckling av nya tjänster som signering, koppling till nya affärssegment som exempelvis det privata näringslivet, modifieringar i tillitsramverk, eller liknande.

I det fortsatta arbetet bör E-legitimationsnämnden arbeta vidare med relevanta forum för samråd med viktiga intressenter i viktiga frågor kring verksamhetens drift och utveckling.

Genomförandearbetet för att bygga upp, etablera samt vidareutveckla och expandera Svensk e-legitimation kommer förutom ovan nämnda aktiviteter att innefatta en rad ytterligare aktiviteter. Genomförandeplanen nedan är ett första utkast till en detaljerad plan med delmål, aktiviteter som behöver utföras och tid för genomförande. Det ska noteras att planen kommer att vara ett levande dokument där ytterligare uppgifter kommer att tillkomma under perioden 2011–13. Planens inledande delar bör exempelvis diskuteras och beslutas i samband med nämndens inledande möten.

Tabell 8.2 Genomförandeplan år 2010

Delmål	Aktiviteter	År/kvartal
Ledning och utveckling		
Nämnden skapad	Kansliansvarig utses	Kv4
	Nämndens ledamöter utses	Kv4
	Praktiska former för nämndens arbete (samarbete med Skatteverket, lokaler, stöd, etc.)	2010–11

Tabell 8.3 Genomförandeplan år 2011

Delmål	Aktiviteter	År/kvartal
Ledning och utveckling		
Nämnden skapad	Praktiska former för nämndens arbete (samarbete med Skatteverket, lokaler, stöd, etc.)	2010–11
	Nödvändiga arbetsformer inom nämnden skapas inklusive konkreta ledningsprocesser för arbetets genomförande	Kv1
	Centrala, kortsiktigt nödvändiga kompetenser rekryteras	Kv1
	En projektorganisation etableras för att bygga upp verksamheten	Kv1
	Konkretiserad tidplan för arbetets genomförande	Kv1
Upphandlade identitetsutfärdare	Framtagande av underlag inklusive juridiska, ekonomiska och tekniska specifikationer	Kv1–2
	Genomförande av upphandling	Kv3–4
Upphandlad teknisk drift och underhåll	Framtagande av underlag för upphandling	Kv1
	Upphandling	Kv2–3
Anpassad och vidare utvecklad affärsmodell	Insamling av statistik och erfarenheter i syfte att tydliggöra modellen	Kv1–2
Marknad och kommunikation		
Verksamhetsformer och processer	Tydliga processer utvecklas för verksamhetens genomförande	Kv3
Samverkan etablerad	Samverka med ledande e-tjänsteleverantörer kring vidareutveckling och förankring av modellen	Kv1–4, fortgående hela perioden
	Samverka med leverantörer av e-legitimationer och andra viktiga aktörer på marknaden	Kv1–4 fortgående hela perioden

Delmål	Aktiviteter	År/kvartal
	Verka för samverkan med näringslivet för att etablera en motsvarande lösning för Svensk e-legitimation	Kv1–4 fortgående hela perioden
Internationellt arbete	Deltagande i standardiseringsarbete och annat relevant arbete	Kv1–4 fortgående hela perioden
Medlemshantering		
Verksamhetsformer och processer	Tydliga processer utvecklas för verksamhetens genomförande	Kv3
Övergångsplan	Detaljerad plan för överflyttning e-tjänsteleverantörer inkl. regelverk, ekonomiska konsekvenser samt praktisk hantering	Kv2
Marknadsplan	Marknadsplan för att bearbeta och ansluta av nya medlemmar	Kv3
Drift		
Plan för verksamheten	Detaljerad plan för utveckling, försörjning och driftssättning av verksamheten	Kv1
Verksamhetsformer och processer	Utarbeta tydliga processer för verksamhetsområdet	Kv3
Teknisk infrastruktur skapad	Detaljering av tekniska specifikationer och gränssnitt	Kv1
	Register: detaljering av förutsättningar, förankring, teknisk utveckling	Kv2
	Anvisningstjänst: Kravspecifikation och utveckling	Kv3
	Signeringstjänst – Analys och utvärdering av förutsättningar och behov	Kv2

Delmål	Aktiviteter	År/kvartal
Tillit, kvalitet och säkerhet		
Verksamhetsformer och processer omfattande hela infrastrukturen för Svensk e-legitimation	Tydliga processer utvecklas inom för verksamhetens genomförande; – Tillitsarbetet – Tillsyn i form av granskning och uppföljning – Ledningssystem för informationssäkerhet – Risk och säkerhetsanalyser – Kontinuitetsplanering och krisberedskap	Kv3
Behörighetskontroller i E-legitimations-nämndens arbete	Utformning av – Behörighet – Säkerhet i systemutveckling – Informationsklassificering – Fysisk kontroll	Kv2
Uppdaterat regelverk för Svensk e-legitimation	Stödja processen för genomförande av föreslagen lagförändring – framtagande underlag och förankring	Kv4
	Komplettering av ramverk	Kv2–3
Kvalitetssäkrad modell för e-legitimationer	Genomlysning av modellen för Svensk e-legitimation utifrån Riksarkivets perspektiv	Kv2
	Riskanalys av modellen för Svensk e-legitimation via MSB	Kv2
	Genomförande av eventuell åtgärdsplan från RA och MSB	Kv3

Tabell 8.4 Genomförandeplan år 2012

Delmål	Aktiviteter	År/kvartal
Marknad och kommunikation		
Samverkan etablerad	Samverka med ledande e-tjänste-leverantörer kring vidareutveckling och förankring av modellen	2011–13
	Samverka med leverantörer av e-legitima-tioner och andra viktiga aktörer på marknaden	2011–13
Internationellt arbete	Deltagande i standardiseringsarbete och annat relevant arbete	2011–13
Medlemshantering		
Övergång	Anslutning av nuvarande e-tjänsteleverantörer när kontroll och ansökningsprocessen är klar	Kv1–4
Marknadsplan	Kommunikation och bearbetning av e-tjänsteleverantörer att ansöka om medlemskap	Kv1–4
Drift		
Teknisk infrastruktur skapad	Register: driftssättning, drift och underhåll	Kv1
	Eventuell pilot och test av infrastruktur	Kv1–2
	Signeringstjänst – Utveckling av vald lösning – Eventuell upphandling	Kv1 Kv2

Tabell 8.5 Genomförandeplan år 2013

Delmål	*Aktiviteter*	*År/Kvartal*
Ledning och utveckling		
Anpassad och vidare-utvecklad affärsmodell	Dra lärdomar från den första tiden och vidareutveckla affärs- och prismodell	Kv1–2
Marknad och kommunikation		
Samverkan etablerad	Samverka med ledande e-tjänste-leverantörer kring vidareutveckling och förankring av modellen	2011–13
	Samverka med leverantörer av e-legiti-mationer och andra viktiga aktörer på marknaden	2011–13
Internationellt arbete	Deltagande i standardiseringsarbete och annat relevant arbete	2011–13
	Deltagande i relevanta EU-projekt, exempelvis STORK	2011–13
Medlemshantering		
Marknadsplan	Kommunikation och bearbetning av e-tjänsteleverantörer att ansöka om medlemskap	2012–13
Drift		
Uppdaterade tekniska specifikationer	Uppdatering av tekniska specifikationer och standardprofiler efter behov och lärdomar från första fasen	Kv1–2

8.6.2 Organisation av genomförande och bemanning

E-legitimationsnämnden ansvarar för att etablera nämndens verksamhet inom Svensk e-legitimation. Arbetet med att etablera nämnden bör kunna indelas i två delar dels en som fokuserar på att etablera den dagliga driften och dels en som fokuserar på att under byggande- och lanseringsfasen driva ett antal utvecklingsområden i projektform under ledning av kansliansvarige.

Den uppskattade bemanningen i nämnden, formellt anställda via Skatteverket, föreslås uppgå till fyra årsanställda. Dessa personer

föreslås på övergripande nivå ha följande roller och ansvarsområden:

Kansliansvarig
- Ledning och utveckling av E-legitimationsnämnden, 0.6 Årsarbetskraft (Årsarbetskraft, ÅAK)
- Tillit, kvalitet och säkerhet, 0.4 ÅAK

Jurist
- Hantering av medlemmar, 0.5 ÅAK
- Tillit, kvalitet och säkerhet, 0.5 ÅAK

Marknad och kommunikation
- Hantering av medlemmar, 0.75 ÅAK
- Marknad och kommunikation, 0.25 ÅAK

Drifts- och säkerhetsansvarig
- Drift (utveckling, upphandling, teknisk support), 1 ÅAK

8.7 Ekonomi

8.7.1 Förutsättningar för att finansiera verksamheten

I direktivet beskrivs att nämndens verksamhet på sikt i så stor utsträckning som möjligt ska täckas av avgiftsintäkter. Då osäkerhetsfaktorerna i modellen för Svensk e-legitimation fortfarande är många ska uppgifterna i denna modell ses som indikativa. Nämnden behöver arbeta vidare med att konkretisera och uppdatera såväl affärsmodell som budget allt eftersom fortsatt arbete bedrivs med att säkra rätt förutsättningar och korrekt indata.

Då infrastrukturen för Svensk e-legitimation sätts i drift 2012 finns, som tidigare angetts, fortfarande möjligheten för e-tjänsteleverantörer att avropa e-legitimationstjänster genom nuvarande ramavtal. Kommande beräkningar bygger dock på att nuvarande e-tjänsteleverantörer går över till Svensk e-legitimation fullt ut. Övergången kan dock komma att ske gradvis vilket innebära att betalningarna via nämnden minskas med motsvarande nivåer.

Alla ekonomiska beräkningar i rapporten baseras på belopp exklusive mervärdesskatt.

8.7.2 Budget 2011–2013

En utgångspunkt och ambition har varit att nämndens verksamhet ska hållas så smal och kostnadseffektiv som möjligt. Initialt beräknas E-legitimationsnämndens löpande ansvarsområden kunna hanteras av fyra årsarbetskrafter.

Under perioden 2011–2013 beräknas antalet årsarbetskrafter öka något. Detta främst beroende av att Svensk e-legitimation sätts i drift vilket innebär att andelen operativa uppgifter kommer att öka, för att hantera drift samt attrahera och ta hand om nya medlemmar. Det ökade antalet årsarbetskrafter kan antingen lösas via anställda eller extern inhyrd tillfällig personal.

Uppskattat behov av årsarbetskrafter per år framgår av tabellen nedan. Notera att nämnden och Svensk e-legitimation förväntas vara uppbyggd och lanseringsfasen avslutad efter år 2013. Därefter förväntas verksamheten nå en mer normal period med möjligt behov av utökat antal årsanställda om tillväxt alternativ utveckling i verksamheten ställer krav på detta.

Tabell 8.6 Nämndens behov av årsarbetskrafter år 2011–2013

Ansvarsområden	2011	2012	2013
Ledning och utveckling av E-legitimationsnämnden (övrig)	0.6	0.6	0.6
Hantering av medlemmar (operativ)	1.25	1.25	1.25
Marknad och kommunikation (övrig)	0.25	0.5	1
Drift (utveckling, upphandling, teknisk support) (övrig)	1	2	3
Tillit, kvalitet och säkerhet (50 % övrig, 50 % operativ)	0.9	0.9	0.9
Totalt antal ÅAK	***4***	***5.25***	***6.75***
Total kostnad (900 000/år) SEK	***3 600 000***	***4 725 000***	***6 075 000***

Kostnaden per årsarbetskraft är beräknad till 900 000 SEK per år vilket inkluderar lön, sociala avgifter, arbetsplats samt nödvändiga tekniska hjälpmedel. Beloppet inkluderar även administrativa avgifter uppskattade av Skatteverket till knappt
100 000 SEK per ÅAK och år.

För att kunna avgöra hur finansieringen ska ske av kostnaderna som uppkommer i Svensk e-legitimation och E-legitimationsnämnden görs en distinktion mellan tre typer av kostnader, vilka beskrivs i kommande avsnitt.

- Investeringar (utvecklingskostnader)
- Operativa kostnader (drift av Svensk e-legitimation)
- E-legitimationsnämndens övriga kostnader (ej direkt relaterade till drift av Svensk e-legitimation)

Investeringar

De största kostnaderna under de första åren är relaterade till initiala investeringar för att etablera infrastrukturen för Svensk e-legitimation. En uppskattning av nödvändigt utvecklingsarbete visar på en investering under år 2011 till 2013 på upp till 9,5 MSEK. Infrastrukturen beräknas vara etablerad 2012 och därefter bör behovet av utvecklingsarbete minska.

Tabellen nedan ger en uppskattning av det utvecklingsarbete som behöver genomföras under de första två åren. Uppgifterna är skattade och ej baserade på konkreta offerter.

Tabell 8.7 Uppskattade investeringskostnader år 2011–2012

Utvecklingsområde	Aktiviteter	2011	2012
Register	Utvecklingsarbete inklusive aggregeringsverktyg (1000 timmar)	1000000	
Anvisningstjänst	Kravspecifikation och utvecklingsprojekt. Efter en första fas kan arbetet koordineras med arbetet kring registren	500000	
Signeringstjänst	Framtagande av kravspecifikation samt förankring och inhämtning av synpunkter från myndigheter kring behov, lösning, väg framåt samt utformning av tjänsten. Uppskattningen bygger på signering enligt alternativ 2 (hypotes, under utredning). Minimikostnad 0.75 MSEK	1000000	
	Framtagande av upphandlingsunderlag i form av tekniska och juridiska specifikationer samt utkast till offertförfrågan (RFI). Kostnad exklusive upphandlingsarbete. Genomförs om möjligt i samarbete med Kammarkollegiet. Minimikostnad 0.75 MSEK	1000000	
	Utveckling av lösning inklusive test, integration samt dokument och signatur format, etc. Skapa förutsättningar för säker driftsmiljö, rutiner och policy dokument. I dagsläget finns flera viktiga risker vilka måste utredas under första fasen av arbetet då bl a ett vägval och fördjupad projektdefinition och kalkyl tas fram. Minimikostnad 2 MSEK	2000000	2000000
Tillitsramverk	Uppbyggande av infrastruktur kring accreditering och certifiering. Utveckla och äga regelverk och process. Minimikostnad 0.5 MSEK/år	1000000	1000000
	Totalt SEK:	6500000	3000000

Inom offentlig förvaltning ska immateriella anläggningstillgångar, så som IT-utveckling, finansieras via lån från Riksgälden. I tabellen ovan antas alla poster, utom framtagande av kravspecifikation för signeringstjänsten (1 MSEK) och framtagning av upphandlingsunderlag för signeringstjänsten (1 MSEK), falla inom denna kategori. Dessa två poster på totalt 2 MSEK anses kunna kategoriseras som tillhörande forskningsfasen, varpå de kommer

att hanteras som vanliga kostnader[9]. Ovan kategoriseringar är uppskattningar som kan komma att omarbetas.

Med presenterad kategorisering uppskattas att 7,5 MSEK av de totala investeringarna på 9,5 MSEK bör finansieras via lån från Riksgälden och resterande 2 MSEK hanteras som kostnader, finansierade via statliga anslag.

Operativa kostnader (drift av Svensk e-legitimation)

De operativa kostnaderna är direkt relaterade till drift av tjänster och infrastruktur i Svensk e-legitimation. Dessa kostnader inkluderar bland annat de ansvarsområden som kategoriserats som operativa, drift av Svensk e-legitimations register, räntekostnader samt avskrivningar. Då lånet till investeringarna antas gå via Skatteverkets låneram uppgår räntekostnaderna till 1.3 % 2011, 1.5 % 2012 och 1.5 % 2013. Räntesatserna och avskrivningar aktiveras då investeringen driftssätts, vilket enligt prognos är juni 2012. Fram till dess gäller kreditivränta om 1.32% (prognostiserad reporänta samt ett påslag om 0.02%) under perioden 2011/01–2012/06. Det totala lånebeloppet uppgår då till 7.7 MSEK inklusive kreditivränta, vilket skrivs av på 5 år, 1.5 MSEK per år. Första avskrivningen sker för det andra halvåret 2012, efter att modellen driftssatts. Beloppen för både ränta och avskrivning har därför halverats.

Tabell 8.8 Operativa kostnader år 2011–2013

E-legitimationsnämndens operativa kostnader (drift av Svensk e-legitimation)	2011	2012	2013
Ansvarsområden (operativa kostnader)	2 430 000	3 330 000	4 230 000
Drift av register		500 000	1 000 000
Räntekostnader (investeringsbelopp 7.5 MSEK)		58 106	116 213
Avskrivning		774 750	1 549 500
Totala kostnader (SEK)	***2 430 000***	***4 662 856***	***6 895 713***

[9] Immateriella anläggningstillgångar, Ekonomistyrningsverket.

E-legitimationsnämndens övriga kostnader

Dessa kostnader är relaterade till nämndens interna verksamhet och utveckling av Svensk e-legitimation generellt och kan inte hänföras till någon av de övriga aktörerna. Kostnaderna omfattar exempelvis myndighetsutförande kostnader förknippade med t.ex. konferenser, resor och marknadsföring, samt investeringskostnader som anses befinnas i forskningsfasen. På grund av kostnadsposternas karaktär föreslås de fortvarigt finansieras via anslag. När det gäller investeringskostnader för projekt i forskningsfasen innefattar det bland annat framtagande av kravspecifikationer och upphandlingsunderlag.

Tabell 8.9 E-legitimationsnämndens övriga kostnader år 2011–2013

E-legitimationsnämndens övriga kostnader	2011	2012	2013
Ansvarsområden (övriga kostnader)	1 170 000	1 395 000	1 845 000
Omkostnader, inkl. deltagande i utv. arb. kring ISO	700 000	700 000	700 000
Investeringskostnader (forskningsfas)	2 000 000		
Utveckling, samråd och stöd	3 700 000	3 294 644	6 289 288
Totala kostnader (SEK)	***7 570 000***	***5 389 644***	***8 834 288***

Den kostnadspost som är inlagd för Utveckling, samråd och stöd symboliserar kostnader som tillkommer under modellens uppbyggnads- och lanseringsfas. Efter år 2013 förväntas dessa kostnader försvinna eller avsevärt minska.

Finansiering

Med en bibehållen marknad utifrån skattad ersättning till identitetsutfärdarna och en ökad kostnadsmassa, introduktionen av E-legitimationsnämnden och infrastrukturen för Svensk e-legitimation, och utan att signifikant öka avgifterna för e-tjänsteleverantörerna är det svårt att nå full kostnadstäckning för nämnden. Potentialen i affärsmodellen för E-legitimationsnämnden och identitetsutfärdarna kan komma att finnas i:

- Ytterligare anslutna e-tjänsteleverantörer inom offentlig förvaltning (myndigheter, kommuner, landsting)

- Ökad användning av tjänster som kräver e-legitimation i statliga och kommunala bolag
- Potential för identitetsutfärdarna i skapandet av en liknande struktur för näringslivet

År 2011 genomgår E-legitimationsnämnden en uppbyggnadsfas och inga e-tjänsteleverantörer eller identitetsutfärdare kommer att vara anslutna. Verksamheten kommer detta år inte ha några intäkter utan föreslås finansieras via anslag.

Senast halvårsskiftet 2012 förväntas Svensk e-legitimation lanseras och gå i drift. Från och med då förväntas marknadens aktörer vara med och finansiera de operativa kostnaderna och andelen statlig finansiering kan minskas. Vid denna tidpunkt påbörjas även avskrivningsperioden för investeringarna. Vid en sammanställning av intäkter och kostnader för E-legitimationsnämnden år 2011 till 2013 görs uppskattningen enligt följande tabell.

Tabell 8.10 E-legitimationsnämndens budget år 2011–2013

	2011	2012	2013
Marknadsstorlek Svensk e-legitimation årets början	0	12,500,000	25,000,000
Tillväxttakt	0.00%	0.00%	10.00%
Marknadsstorlek Svensk e-legitimation årets slut	0	12,500,000	27,500,000
E-legitimationsnämnden			
Intäkter			
Årsavgift IdP (avgift * antalet anslutna)	0	40,000	80,000
Årsavgift attributsintygsutfärdare (avgift*antal)	0	12,500	25,000
Årsavgift E-tjänsteleverantörer (nya ansluts inför kv3)	0	12,500,000	26,250,000
Totala intäkter:	0	12,552,500	26,355,000
Kostnader			
Operativa kostnader (Drift av Svensk e-legitimation)	2,430,000	4,662,856	6,895,713
Grundersättning till identitetsutfärdarna	0	12,500,000	20,000,000
Tillväxtbaserad ersättning till identitetsutfärdarna			625,000
E-legitimationsnämndens övriga kostnader	7,570,000	5,389,644	8,834,288
Totala kostnader:	10,000,000	22,552,500	36,355,000
Resultat			
	-10,000,000	**-10,000,000**	**-10,000,000**
Behov av statlig finansiering			
	10,000,000	**10,000,000**	**10,000,000**

Uppskattningen bygger på att inte några intäkter kommer nämnden tillhanda under år 2011. Halvårsskiftet 2012 går den operativa driften igång och samtliga nuvarande aktörer ansluts till systemet, en osäkerhetsfaktor är när denna anslutning i praktiken

kommer att ske. Den totala marknadsstorleken beräknas vara 25 MSEK 2012 baserat på vald prismodell för e-tjänsteleverantörerna. Den totala marknadsstorleken halveras då systemet inte kommer att driftsättas förrän vid halvårsskiftet. Modelleringen bygger på att fem attributsutfärdare ansluts under 2012. Kostnader relaterade till drift av registren antas uppkomma från 2012. En ytterliggare kostnadspost kallad utvecklings- och aktiveringskostnader har lagts till för att hantera utvecklingsprojekt i samband med Svensk e-legitimations uppbyggnad och lansering.

För att kompensera identitetsutfärdarna bör ersättningen så snart det är möjligt uppgå till nuvarande marknadsstorlek, alltså ca 20 MSEK. Med denna modell kommer nämnden att nå kostnadstäckning för de operativa kostnaderna år 2014.

I modellen har antagits att ersättningen som betalas ut från nämnden till identitetsutfärdarna är momspliktig och att E-legitimationsnämnden kan rekvirera ingående moms, vilket överensstämmer med de preliminära synpunkter som inhämtats från Ekonomistyrningsverket.

8.7.3 Övergång från anslagsfinansiering till avgiftsfinansiering

Det finns i direktivet en önskan om att minska de statliga anslagen till E-legitimationsnämnden och att övergå till en avgiftsfinansierad modell. För att finansiera E-legitimationsnämndens verksamhet finns avsatta statliga anslag om 10 MSEK årligen under år 2011 till 2013. Om antagandena som ligger till grund för beräkningarna är korrekta uppskattas detta belopp i dagsläget kunna täcka nämndens omkostnader, då vissa initiala investeringar finansieras via lån från Riksgälden. Budgetförslaget på föregående sida indikerar att det från 2014 ska vara möjligt att finansiera operativa kostnader (drift av Svensk e-legitimation) endast med avgiftsintäkter. En förutsättning för att detta ska vara möjligt är dock att de totala avgifterna för e-tjänsteleverantörerna höjs från dagens ca 20 MSEK till 25 MSEK (siffrorna behöver bekräftas av nämnden). Det finns även en stor osäkerhet i modellen då den bygger på anslutning av 100 % av dagens e-tjänsteleverantörer 2011. Då det finns ett alternativ till Svensk e-legitimation i existerande ramavtal inledningsvis är det sannolikt att anslutningen av aktörerna sker gradvis under en längre övergångsperiod. Vid en exempelvis 25 % anslutning av dagens

aktörer och en ökning av antalet e-tjänsteleverantörer med 20 % per år kommer anslag i storleksordningen 10 MSEK krävas under betydligt fler år framöver, troligtvis till och med 2020.

Resonemangen kring prismodell och budget tenderar att bli komplex då det är flera krav i direktivet att förhålla sig till. Det gäller exempelvis att ersättningsnivåerna för e-tjänsteleverantörerna ska vara oförändrad eller helst sänkas, det ska finnas mångfald i modellen dvs. det ska vara attraktivt för identitetsutfärdarna att ansluta sig samt att man via etableringen av nämnden tillför systemet nya kostnader. Utredningen har därför i detta avsnitt beräknat en höjning av e-tjänsteleverantörernas avgifter, för att finansiera verksamheten. Detta inte minst för att ersättningen till identitetsutfärdarna ska kunna hållas konstant så att de ser det som attraktivt att ansluta sig till modellen. Samtidigt är tanken att den nya modellen ska medföra besparingar för e-tjänsteleverantörerna i deras integrering och hantering av e-legitimationer.

Beskrivet räkneexempel visar på att hälften av marknadens tillväxt används för att täcka nämndens operativa kostnader istället för att betalas ut som extra ersättning till identitetsutfärdarna. Alternativet vore att istället endast låta en mycket liten del av tillväxten tillfalla E-legitimationsnämnden, vilket dock resulterar i att övergången till avgiftsfinansiering kommer att ta längre tid. Ytterliggare en åtgärd som har liknande påverkan på övergångstiden till avgiftsfinansieringen är möjligheten att erbjuda gratis deltagande i Svensk e-legitimation under en viss tid för att kompensera de investeringar som måste genomföras hos respektive aktör.

Då utredningens förslag för att övergå till en avgiftsfinansierad modell bygger på en höjning av e-tjänsteleverantörernas avgift finns en risk att dessa aktörer kommer att avvakta i att ansluta sig till Svensk e-legitimation så länge alternativ finns i existerande ramavta, vilket gör att anslagsfinansiering istället kommer att krävas under en längre tid. Det kan på grund av detta vara lämpligt att omvärdera önskan om avgiftsfinansiering. Om anslagen till E-legitimationsnämnden höjs och säkras under en längre tidsperiod skapas bättre förutsättningar för att etablera en affärsmodell som både e-tjänsteleverantörer och identitetsutfärdare kan finna attraktiv, vilket förbättrar förutsättningarna för en framgångsrik etablering av Svensk e-legitimation.

8.7.4 Risker med affärsmodellen

Under budgetperioden 2011–2013 kan marknadssituationen komma att ändras väsentligt, bland annat baserat på antalet identitetsutfärdare, e-tjänsteleverantörer och attributsutfärdare som väljer att medverka i Svensk e-legitimation. Dessa faktorer kommer alla att påverka E-legitimationsnämndens finansiella situation vilket innebär att såväl affärsmodell som budget kan behöva ses över.

Det finns ett antal komponenter i affärsmodellen som anses som kritiska för Svensk e-legitimations etablering och för att beskriven budget ska kunna nås;

1. Identitetsutfärdarna väljer att inte delta i Svensk e-legitimation

Identitetsutfärdarna är grunden för modellen och en nödvändighet för att Svensk e-legitimation ska kunna etableras. För att denna risk ska kunna undvikas är det väsentligt att skapa tillräckliga incitament för identitetsutfärdarna för att de ska välja att gå över till Svensk e-legitimation.

2. *E-tjänsteleverantörerna väljer att avropa e-legitimationstjänster i existerande ramavtal så länge det är möjligt istället för att övergå till Svensk e-legitimation*

För att Svensk e-legitimation ska bli framgångsrikt krävs en kritisk massa av användare och anslutna e-tjänsteleverantörer. Om majoriteten av myndigheter, landsting och kommuner som idag avropar e-legitimationstjänster väljer att även fortsättningsvis avropa via existerande ramavtal kommer nyttan med den nya modellen bli begränsad, vilket kommer att påverka modellens framgång. Utredningen föreslår att e-tjänsteleverantörernas avgifter sätts till en sådan nivå att incitament skapas för anslutning till Svensk e-legitimation.

3. De statliga anslagen avbryts eller minskas kraftigt efter de inledande tre åren

Det kommer inte att vara möjligt att finansiera Svensk e-legitimation och E-legitimationsnämnden i dess operativa delar endast med avgifter såvida inte 100 % av nuvarande e-tjänsteleverantörer ansluts vid introduktionen av modellen. Utmaningen ligger i att en betydande kostnad tillförs ett existerande system via etableringen

av E-legitimationsnämnden och dess påverkan på marknaden måste begränsas. Som tidigare visats i denna rapport är det möjligt att på relativt kort tid nå täckning för nämndens operativa verksamhet av marknaden, dock anses det viktigt att prioritera identitetsutfärdarnas ersättning och att minska påverkan på e-tjänsteleverantörernas avgifter istället för att säkra full kostnadstäckning av marknaden för nämnden. Resultatet av detta är dock att betydande anslagsfinansiering krävs under lång tid, baserat på vald fördelningsgrund.

4. Lönsamhet i affärsmodellen uppnås inte då näringslivet inte inkluderas i Svensk e-legitimation

Marknaden relaterad till offentliga Sveriges användning av tjänster som kräver e-legitimation är relativt begränsad. Kostnaden för driften av Svensk e-legitimation uppgår till 12–35 % av nuvarande marknadsstorlek under år 2011 till 2013. På sikt, då en kritisk massa av deltagare nåtts och affärsmodellen är etablerad, kan situationen vara en annan vilket kan innebära att en större grad av avgiftsfinansiering kan nås.

Internationellt finns ytterliggare exempel på att det inte är självklart att det är möjligt att nå lönsamhet vid etableringen av en nationell modell för e-legitimationer. Erfarenheter visar på att det är den privata sektorn som är nyckeln till att nå lönsamhet. För att full kostnadstäckning ska nås bör ett förslag utarbetas där del av näringslivets andel av totalmarknaden kan komma E-legitimationsnämnden tillhanda.

9 En motsvarande infrastruktur för privat sektor

I detta avsnitt beskrivs hur den av utredningen föreslagna modellen för Svensk e-legitimation inom offentlig sektor även behöver och kan få en lösning för privat sektor. Tanken är att nämnden verkar för att en parallell struktur etableras vilken verkar i enlighet med reglerna för Svensk e-legitimation. För användaren ska det inte finnas några viktiga skillnader utan snarast uppfattas som att det är samma lösning.

9.1 Utgångspunkt

Den av utredningen föreslagna Infrastrukturen för Svensk e-legitimation har som primär utgångspunkt att tillgodose den offentliga sektorns behov på området. Målsättningen är emellertid att Svensk e-legitimation ska kunna användas även inom den privata sektorn. E-legitimationsnämnden kan dock inte inom ramen för ett valfrihetssystem företräda e-tjänsteleverantörer utanför den offentliga sektorn. Avtal på det området – mellan leverantörer av e-tjänster och Identitetsutfärdare – måste således lösas på annat sätt. Detsamma gäller för hanteringen av betalningar för tjänster som Identitetsutfärdare utför åt e-tjänsteleverantörer utanför offentlig sektor.

Samtidig ska inte e-legitimationer som godtas inom Infrastrukturen för Svensk e-legitimation begränsas så att de får användas endast för e-tjänster inom offentlig sektor. Det är istället, såsom inom dagens system för e-legitimationer, väsentligt och centralt att en ny infrastruktur resulterar i motsvarande lösning för den privata sektorn.

9.2 Förslag till lösning

Detta bör kunna uppnås genom att det bildas två samverkande infrastrukturer för identifiering – en för den offentliga sektorn och en för den privata – som i princip använder sig av samma regelverk. Dessa två samverkande infrastrukturer bör från ett användarperspektiv uppfattas som enhetliga. Hit hör rent praktiska frågor som att samma e-legitimationer, användargränssnitt och transaktionsmönster bör införas. Härigenom kan sådana för informationssamhället grundläggande funktioner som elektronisk legitimering hanteras enhetligt. En sådan samordning är viktig även från juridiska utgångspunkter. Enskildas behov av rättssäkerhet och persondataskydd måste tillgodoses enhetligt och det samma gäller för tolknings- och tillämpningsfrågor. Genom en sådan samordning kan det säkerställas att det uppkommer samverkande lösningar i stället för parallella icke samverkande lösningar.

Utredningen har därför i olika avseende sökt lösningar för att åstadkomma samverkande infrastrukturer. Bland annat har det föreslagna regelverket för Infrastrukturen för Svensk e-legitimation utformats så att det ska kunna fungera inom både offentlig och privat sektor och stödja samverkande infrastrukturer. Detsamma gäller för de framtagna tekniska specifikationerna och tillitsramverket.

En identitetsutfärdare som godkänts inom en ny infrastruktur för offentlig sektor bör, med samma e-legitimationer och identitetsintyg, kunna verka inom en infrastruktur för privat sektor. De register som föreslagits för Infrastrukturen för identifiering, dvs. inom offentlig sektor, bör i väsentliga delar också kunna brukas inom en infrastruktur för privat sektor. Hanteringen blir tekniskt enklare ju längre en sådan integration kan drivas och det bör vara möjligt att etablera en sådan samordning genom att utforma regelverk och rollfördelning så att dessa möjligheter kan tas tillvara. Det är emellertid knappast möjligt att på detta stadium i detalj ange hur en sådan samordning ska regleras eftersom arbetet inte kommit längre än till utformningen av grundkomponenter för en ny infrastruktur för offentlig sektor.

9.3 Genomförande

Det är väsentligt att E-legitimationsnämnden i sitt arbete i största möjliga utsträckning säkerställer att det beskrivna målet med samverkande infrastrukturer verkligen uppnås utan sådana fördröjningar att dagens lösningar och den som nu föreslås av utredningen måste leva parallellt, endast för att tillgodose näringslivets behov. En sådan utveckling kan stödjas exempelvis genom att E-legitimationsnämnden vid inrättandet av valfrihetssystemet ställer krav på att de Identitetsutfärdare som vill leverera tjänster till Svensk e-legitimation även ska kunna tillhandahålla motsvarande tjänster till marknaden i övrigt. Därför bör ett nära samråd ske med företrädare för den privata sektorn inför en upphandling av leverantör av tekniskt stöd m.m. för driften av Infrastrukturen för svensk E-legitimation. Inom ramen för de begränsningar som följer av reglerna för upphandling är det önskvärt att en sådan leverantör, med motsvarande tillämpning av regelverket för offentlig sektor, även kan ikläda sig en roll som federationsoperatör för en infrastruktur för den privata sektorn. E-legitimationsnämnden kan, med de begränsningar som angetts, beakta dessa frågor vid valet av leverantör av tekniskt stöd m.m. men det är givetvis upp till denna leverantör att själv, i samråd med den privata sektorn, finna en lämplig form för denna verksamhet. För förslag till riktlinjer för federationsoperatörer, se *bilaga 7*.

Utifrån dessa utgångspunkter är det önskvärt att den som E-legitimationsnämnden upphandlar som leverantör av tekniskt stöd m.m. för offentlig sektors Infrastruktur för identifiering, också ska kunna fylla uppgifter för att en samverkande infrastruktur för privat sektor ska bli verklighet. Dessa kompletterande uppgifter för att införa motsvarande funktioner för privat sektor bör innefatta att

- etablera en icke-diskriminerande affärsmodell för identitetsintyg,
- teckna avtal med de identitetsutfärdare och e-tjänsteleverantörer som ansluts,
- med stöd av uppgifter från register som förs för offentlig sektor upprätta register över de utfärdare av identitets- och attributsintyg som ansluts och tillhandahålla detta register, och
- upprätta register över de e-tjänsteleverantörer inom privat sektor som ansluts och tillhandahålla detta register.

Denna federationsoperatör för användning av Svensk e-legitimation inom privat sektor bör inte etablera något nytt tillitsramverk för denna federation för privat sektor utan använda det som införs inom Infrastrukturen för identifiering; dvs. inom offentlig sektor. För att nå en samverkande infrastruktur för privat sektor som drivs i samverkan med infrastrukturen för offentlig sektor blir det därför betydelsefullt för E-legitimationsnämnden att den eller de aktörer som verkar som federationsoperatörer inom privat sektor

- redan har hög trovärdighet inom den privata sektorn och kan förväntas få en hög trovärdighet även som federationsoperatör, för privat sektor,
- bedriver en verksamhet som naturligt kan utvecklas till att omfatta även en roll som federationsoperatör för privat sektor i nära samverkan med offentlig sektor,
- får en oberoende ställning, utan stark koppling till någon viss aktör på marknaden och utan att konkurrensen på marknaden störs,
- kan förväntas få allmänhetens tillit och verka långsiktigt och stabilt,
- har erfarenhet av likartad teknisk och administrativ verksamhet, och
- drivs med en inriktning som inte präglas av enbart vinstintresse utan har en form och en struktur som möjliggör även andra mål

Ett exempel på en tänkbar sådan aktör kan vara Stiftelsen för Internetinfrastruktur (.SE), som enligt utredningens uppfattning utifrån sin verksamhetsform och sina erfarenheter av att hantera domännamn borde ha förutsättningar att införa och stödja en kompletterande federation för den privata sektorn. Utredningen har i sitt arbete också berört frågan med såväl stiftelsen som andra aktörer inom den privata sektorn. E-legitimationsnämnden bör i sitt arbete skyndsamt i samråd med den privata sektorn utröna om stiftelsen skulle kunna vara en lämplig federationsoperatör. Skulle det visa sig att så är fallet, bör E-legitimationsnämnden snarast, i samverkan med stiftelsen, söka få ett utvecklingsarbete till stånd.

10 Konsekvensbeskrivning

I detta avsnitt görs en konsekvensbeskrivning av föreslagen modell med utgångspunkt från problemet som ska lösas, direktivets krav, vilka bedömningar som gjorts i olika frågor och av alternativa lösningsmodeller samt konsekvenser av utredningens förslag.

Beskrivning av problemet och vad som önskas uppnås

Dagens lösning för e-legitimationer fungerar relativt väl och i en internationell jämförelse är det förhållandevis många medborgare i Sverige som kan utföra legitimering och underskrift i en elektronisk miljö.

Dagens system har dock brister. Det finns ingen sammanhållen och enhetlig infrastruktur för identifiering vilket försvårar och förmodligen hämmar utvecklingen av e-tjänster inom den offentliga sektorn. En samordnad infrastruktur för användning av e-legitimationer underlättar och förenklar för den offentliga sektorn och bör främja en utveckling av e-tjänster. Dagens modell är ett system som inte öppnar upp för möjliga nya aktörer att komma in på marknaden och därigenom bidra till en mångfald. Vidare bygger dagens modell för e-legitimationer på en upphandling som går ut per halvårsskiftet 2012 och som inte kan förlängas.

Aktörer inom den offentliga sektorn har i linje med det anfört vissa synpunkter på nuvarande modell exempelvis att det krävs fler än ett avtal med leverantörer, vilket krävs om e-tjänster ska kunna tillhandahållas oavsett vilken e-legitimation den enskilde använder. E-legitimationerna har tekniskt blivit anpassade till dagens identitetsutfärdare vilket gör det svårt att släppa in nya aktörer utan att det innebär integrationskrav hos E-tjänsteleverantörerna. Upphandlingsformen har vidare skapat svårigheter för nya aktörer att få tillträde till marknaden.

Dagens e-legitimationer måste hanteras direkt av myndigheter, landsting och kommuner, vilket ställer krav på integreringstjänster, harmonisering av den information om användaren som olika e-legitimationer är bärare av.

Målet med utredningen är att förbereda bildandet av en nämnd-myndighet för samordning av statens och kommunernas hantering av metoder och tjänster för elektronisk identifiering och signering. Myndighetens verksamhet syftar till att skapa en modell för Svensk e-legitimation i vilken privatpersoner och företag ska kunna använda en och samma e-legitimation vid utnyttjande av alla e-tjänster som tillhandahålls av statliga myndigheter, landsting och kommuner. Konkurrensen och förutsättningarna för utvecklingen av nya tjänster för elektronisk identifiering och signering ska förbättras. Myndigheternas, landstingens och kommunernas kostnader ska vara lättöverskådliga och på sikt helst minska.

Samtliga invånare, myndigheter, landsting, kommuner samt ett stort antal företag kommer att påverkas av denna förändring.

Alternativa lösningar

Projektet har analyserat problemställningen utifrån förutsättningarna i direktivet och har därefter formulerat ett antal olika alternativ. Av dessa har utredningen funnit att det förslag som presenterats i denna rapport är det som på bästa sätt motsvarar ställda krav. Det är dock viktigt att ha i åtanke att denna rapport presenterar en föreslagen lösning i en komplex fråga bestående av ett stort antal delkomponenter. Lösningen ska ses som utredningens förslag baserat på nuvarande kända förutsättningar, det är dock möjligt att komponenter av förslaget kommer att korrigeras i fortsatt arbete, bland annat baserat på erhållen feedback.

Det kan finnas alternativa genomföranden på organisatoriska och tekniska plan där det kanske viktigaste alternativet är att låta en civilrättslig aktör, till exempel .SE, ta juridiskt ansvar som federationsoperatör och där E-legitimationsnämnden fokuserar på att samordna det nationella intresset samt fungerar som reglerande- och tillsynsmyndighet. Detta alternativ skulle underlätta näringslivets deltagande i Svensk e-legitimation samt innebära att E-legitimationsnämndens verksamhet, organisation och kostnader kan hållas till ett minimum. Detta skulle dock kräva en helt annan reglering än nuvarande förslag.

Det finns även ytterliggare vägval, bland annat gällande signeringslösning och prismodell, som kan komma att vidareutvecklas eller omprövas. Exempelvis skulle en prismodell kunna övervägas vilken bygger på att ersättningen är kopplad till volym. Ytterligare ett alternativ som observerats i vissa andra länder innebär att staten utvecklar och finansierar en central e-legitimationslösning. Utredningen har dock ej funnit att dessa alternativ ligger i linje med direktivet eller den tidigare utarbetade strategin för e-legitimationer i Sverige.

Kostnadsmässiga konsekvenser

För användare av e-legitimationer och företag som tillhandahåller e-legitimationer till sina anställda är kostnaderna begränsade till avgifter för anskaffning och installation av e-legitimationer.

Utfärdare av e-legitimationer och tillhandahållare av attributstjänster drabbas av egna kostnader för tillhandahållandet av tjänster, kostnader för certifiering samt avgifter till E-legitimationsnämnden. Detta ska kompenseras av en modell där identitetsleverantörer ges ersättning när deras utgivna e-legitimationer används för legitimering samt där attributsleverantörer på egen hand får söka skälig ersättning från dem som begär attributsintyg.

Organisationer som ges möjlighet att agera som e-tjänsteleverantörer drabbas av kostnader för att integrera sina e-tjänster samt av en avgift till E-legitimationsnämnden för att få tillgång till legitimeringstjänster. Gällande pris- och betalmodell har utredningens förslag fokuserats på önskemålet om att e-tjänsteleverantörernas kostnader ska vara budgeterbara, samt på principen att ersättningen till identitetsutfärdarna i utgångsläget ska beräknas utifrån samma nivå som i nuvarande lösning. Då introduktionen av Svensk e-legitimation och E-legitimationsnämnden innebär att nya kostnader introduceras i systemet resulterar detta initialt i något högre kostnader för e-tjänsteleverantörerna samt ett underskott i nämndens budget vilket föreslås täckas av anslag. Detta ska dock ställas i relation till att andra kostnader så som integration förutsätts minska och ett på sikt minskat kompetensbehov hos varje organisation när fler funktioner är centralt samordnade eller upphandlas på marknaden.

Regleringen och hur den följer Sveriges anslutning till Europeiska unionen

Önskemålet om en ny lösning för e-legitimationer beror också på att den modell för upphandling som tidigare tillämpats inte kan användas eftersom det inte är möjligt för e-tjänsteleverantörerna att skriva leveransavtal med alla utfärdare enligt det nya upphandlingsregelverket. Genom att utforma den nya lösningen som en tjänstekoncession kommer emellertid alla utfärdare av e-legitimationer som uppfyller ställda krav att kunna anslutas. Den analys som hittills genomförts har inte visat annat än att den föreslagna infrastrukturen kan göras förenlig med de skyldigheter som följer av Sveriges anslutning till Europeiska unionen, bl.a. på det upphandlings- och konkurrensrättsliga området.

Här uppkommer också frågor om marknadstillträde, kvalificerade certifikat, säkra anordningar och kvalificerade elektroniska signaturer som måste beaktas när en ny infrastruktur tas fram på området. Även i denna del har analysen hittills inte visat annat än att den föreslagna infrastrukturen kan göras förenlig med de skyldigheter som följer av Sveriges anslutning till Europeiska unionen. Införs en signeringstjänst ökar dessutom Sveriges möjligheter att låta svenska medborgare utnyttja utländska tjänster i samband med tjänstedirektivet i de fall det krävs en personlig elektronisk underskrift av elektroniska handlingar. Dessa underskrifter avses kunna uppfylla kraven för kvalificerade elektroniska underskrifter enligt EU:s signaturdirektiv.

Utredningen föreslår vidare ett tillitsramverk vilket bedöms ligga i linje med det utvecklingsarbete som sker inom EU. Nämnden föreslås vidare delta i EUs fortsatta standardiseringsarbete samt att om det upplevs relevant anpassa den svenska strukturen till den framtida EU standarden.

Tidpunkten för ikraftträdande

Det är mycket viktigt att nuvarande lösningar inte sätts ur spel så att samhället står utan lösning för identifiering och signering. Nuvarande lösning vilar på ramavtal eID2008 som är avtalad till och med juni 2012 vilket måste beaktas vid ett införande av Svensk e-legitimation i dagens e-tjänster. Även därefter finns det möjlighet att utnyttja redan avropade tjänster i ytterligare 4 år vilket kommer

att innebära en parallelldrift under övergångsperioden. eID2008 ligger också till grund för e-legitimationstjänster i nyligen upphandlade ramavtalet E-förvaltningsstödjande tjänster 2010, vilket dock ej kommer att kunna användas för avrop av e-legitimationstjänster efter utgången av eID 2008s giltighetstid. Dagens marknad kommer under övergångsperioden att vara uppdelad mellan Svensk e-legitimation och nuvarande ramavtal och de både modellerna kommer att behöva drivas parallellt fram till nuvarande ramavtals utgång.

Konsekvenser för företag

Utfärdare av e-legitimationer berörs på så sätt att de ska uppfylla regelverkets krav (certifiering) samt ska operera under de allmänna ekonomiska villkor som gäller för identitetsutfärdare för att bli godkända som medlemmar i Svensk e-legitimation. Alla företag som uppfyller regelverket kan anslutas som identitetsleverantörer.

Dagens leverantörer av infratjänster kan i modellen komma att få en ändrad roll då E-legitimationsnämnden kommer att hantera vissa samordnings- och avtalsrelaterade frågor. Deras fortsatta roll såsom stöd till förvaltningen vid utveckling och drift av e-tjänster kommer fortsatt att vara viktig. Därtill kan en roll uppstå som attributsutfärdare.

Attributsutfärdare ska uppfylla regelverkets krav (certifiering). Alla attributsleverantörer som uppfyller regelverket och som anses tillföra attribut som är av allmänt intresse för infrastrukturens e-tjänster, kan anslutas som attributstjänster.

En majoritet av dagens e-tjänster använder tredjepartsprodukter för att realisera identifiering och signering. En majoritet av dessa tredjepartsprodukter har redan i dag förmåga att konsumera identitets- och attributsintyg i enlighet med modellen för Svensk e-legitimation. I samtliga kända fall med tredjepartsprodukter som kan hantera dagens- och morgondagens lösning så kan dessa användas parallellt vilket ger en smidig övergång. Identitetsutfärdare förutsätts göra en egen analys av kostnader och intäkter innan de beslutar sig för att ansluta sig till infrastrukturen.

Konsekvenser för konkurrensförhållandena mellan företag och särskilda hänsyn

Ett valfrihetssystem medför fri konkurrens mellan leverantörer av e-legitimationstjänster. En signeringstjänst kan konkurrera med möjliga framtida tjänster för signering av liknade art vad avser signering inom ramen för e-tjänsteleverantörernas tjänster.

Fri konkurrens mellan e-legitimationsutfärdare ger förutsättningar för lägre priser för utfärdande av e-legitimationer till privatpersoner såväl som personer kopplade till en organisation. Genom att anslutna e-legitimationsutfärdare erhåller ersättning från E-legitimationsnämnden utifrån prestation när deras utfärdade e-legitimationer används, kan dessa få en konkurrensfördel gentemot leverantörer av e-legitimationer som inte är anslutna och som inte får ersättning. Dels genom att deras produkter kan säljas till ett lägre pris och dels genom att de kan användas inom ramen för en nationell infrastruktur.

Vissa system för utfärdande av e-tjänstelegitimationer kan komma att anpassas till företag som har en viss minimistorlek. Detta för att köpande företag ska kunna stå för vissa administrativa funktioner i samband med ansökningar, utlämning, spärrning och hantering av reservfunktioner.

Det är viktigt att även små företag kan ges en möjlighet att legitimera sig på lämpligt sätt inom ramen för infrastrukturen och att det skapas incitament som gör det attraktivt för marknadens aktörer att erbjuda sådana lösningar.

11 Författningskommentar

11.1 Förslag till lag om valfrihet för Svensk e-legitimation

1 §
I paragrafens första stycke anges att E-legitimationsnämnden får tillhandahålla valfrihetssystem för tjänster som upphandlas för elektronisk identifiering. Med valfrihetssystem menas enligt paragrafens andra stycke ett förfarande där användaren har rätt att välja den leverantör som ska tillhandahålla en tjänst för elektronisk identifiering och som nämnden godkänt och tecknat kontrakt med. Med användare avses brukaren av tjänsten vare sig denne är en fysisk eller en juridisk person.

Förslaget har behandlats i avsnitt 4.2.1

2 §
Paragrafen innebär att E-legitimationsnämnden ska tillämpa lagen (2008:962) om valfrihetssystem, som annars gäller endast för den kommunala sektorn. Begreppen leverantör, tjänst och upphandlande myndighet får vid E-legitimationsnämnden tillämpning av lagen delvis en annan innebörd än den som framgår av definitionerna i 2 kap. lagen om valfrihetssystem.

Paragrafens andra stycke innebär att E-legitimationsnämnden inte behöver tillhandahålla sådant icke-val som avses i 9 kap. 2 § lagen (2008:962) om valfrihetssystem.

Förslaget har behandlats i avsnitt 4.2.1

3 §
Paragrafen innebär att kommuner och landsting ges möjlighet att uppdra åt E-legitimationsnämnden att på kommunens eller landstingets vägnar fatta de beslut som är nödvändiga för inrättandet av valfrihetssystemet.

Förslaget har behandlats i avsnitt 4.2.3.

Kommittédirektiv

En myndighet för samordning av elektronisk identifiering och signering

Dir. 2010:69

Beslut vid regeringssammanträde den 17 juni 2010

Sammanfattning

En särskild utredare ska förbereda och genomföra bildandet av en nämndmyndighet för samordning av statens och kommunernas hantering av metoder och tjänster för elektronisk identifiering och signering (e-legitimationer). Nämnden ska ha Skatteverket som värdmyndighet.

Utredaren ska bl.a. besluta om nämndens närmare organisation och arbetssätt samt lämna förslag till författningsreglering.

Nämnden ska kunna inleda sin verksamhet den 1 januari 2011. Uppdraget gäller med förbehåll för riksdagens beslut i de delar det behövs.

Uppdraget ska slutredovisas senast den 31 december 2010.

Bakgrund

Nuvarande system för elektronisk identifiering och signering

För många e-tjänster som statliga myndigheter och kommuner tillhandahåller behöver motparten identifieras elektroniskt på ett säkert sätt. Det behövs också metoder för att signera handlingar elektroniskt, så att det kan avgöras vem handlingen härrör från och att den inte förvanskats. Tillgång till säkra metoder för elektronisk identifiering och signering är därför en grundförutsättning för utveckling av e-tjänster i förvaltningen och en del av en gemensam infrastruktur för e-förvaltning.

Statens och kommunernas användning av metoder för identifiering och signering i samband med e-tjänster bygger på samordnade ramavtalsupphandlingar. Kammarkollegiet genomför

ramavtalsupphandlingar, från vilka statliga myndigheter och anslutna kommuner kan göra avrop. Nuvarande ramavtal (Eid 2008) löper ut den 30 juni 2011 och kan förlängas till den 30 juni 2012. Ett leveransavtal som upprättas efter avrop på befintliga ramavtal kan ha samma avtalslängd som det ursprungliga ramavtalets avtalsperiod. Ett avrop från nuvarande ramavtal (Eid 2008) kan således ske senast den 30 juni 2012 och gälla under fyra år, som längst till den 30 juni 2016.

Det nuvarande systemet med ramavtalsupphandlingar av ett fåtal tjänsteleverantörer har varit utformat i första hand för att få till stånd en snabb utveckling av e-tjänster. En förutsättning har därför bl.a. varit att tjänsteleverantörerna har ett stort antal redan identifierade kunder.

Det nuvarande systemet, som används av ett antal myndigheter och kommuner, har utsatts för viss kritik. Det har framförts att debiteringssystemet leder till höga kostnader för vissa små myndigheter och kommuner samt att kostnaderna är oförutsägbara. Myndigheter har också anfört att det är komplicerat att sluta avtal med flera leverantörer, vilket krävs om e-tjänster ska kunna tillhandahållas oavsett vilken e-legitimation den enskilde använder. Systemet har också skapat svårigheter för nya aktörer att få tillträde till marknaden genom att ett fåtal leverantörer valts ut genom ramavtal. De tekniska lösningarna har också kritiserats för bristande användarvänlighet och tillgänglighet.

I lagen (2000:832) om kvalificerade elektroniska signaturer finns bestämmelser om säkra anordningar för signaturframställning, om kvalificerade certifikat för elektroniska signaturer och om utfärdande av sådana certifikat. Post- och telestyrelsen utövar enligt lagen tillsyn över utfärdare av kvalificerade certifikat till allmänheten. I dag finns en certifikatutfärdare anmäld.

E-delegationens förslag

E-delegationen har i sitt delbetänkande *Strategi för myndigheternas arbete med e-förvaltning* (SOU 2009:86) lämnat förslag till hur förvaltningens framtida arbete med e-legitimationer kan organiseras. Delegationens förslag har sin utgångspunkt i de förslag som redovisas i en rapport från dåvarande Verket för förvaltningsutveckling, Verva, S*lutrapport om säkert elektroniskt informa-*

tionsutbyte och säker hantering av elektroniska handlingar (Rapport 2008:12).

Delegationen föreslår att det inrättas en nämnd med uppgift att fastställa gemensamma krav för myndigheternas användning av e-legitimationer. Nämnden föreslås också få ansvar för att säkerställa att förvaltningen har tillgång till tjänster för elektronisk identifiering och signering samt s.k. identitetsintyg. Enligt förslaget ska samordningsfunktionen också tillhandahålla en identitetsintygstjänst till myndigheter och kommuner om det behövs. Delegationen föreslår att nämnden inrättas i form av ett särskilt beslutsorgan inom Skatteverket. Förslaget syftar till att förenkla för medborgare och företag, att underlätta för myndigheterna och att öppna för fler leverantörer.

Riksrevisionens iakttagelser

I rapporten *E-legitimation – en underutnyttjad resurs* (RiR 2009:19) har Riksrevisionen granskat om systemet för e-legitimation är rättssäkert, tillgängligt, kostnadseffektivt och teknikneutralt samt om regeringen och ansvariga myndigheter har agerat i enlighet med riksdagens intentioner på området. Riksrevisionens bedömning är att systemet för e-legitimationer har haft en positiv effekt på utvecklingen av e-förvaltningen och att det till stora delar uppfyller de krav på rättssäkerhet, tillgänglighet, kostnadseffektivitet och teknikneutralitet som riksdagen har uttalat. I rapporten framhålls dock mindre brister i nämnda avseenden. Riksrevisionen anför att E-delegationens förslag i delbetänkandet *Strategi för myndigheternas arbete med e-förvaltning* (SOU 2009:86) innebär att flera av de påpekade bristerna skulle kunna avhjälpas genom att regeringen och myndigheterna får förutsättningar för att få till stånd den styrning och uppföljning som krävs för att tillgodose riksdagens önskemål om ökad rättssäkerhet, användbarhet och teknikneutralitet.

2010 års förvaltningspolitiska proposition

Regeringen har i propositionen *Offentlig förvaltning för demokrati, delaktighet och tillväxt* gjort bedömningen att statens långsiktiga försörjning av elektroniska legitimationer bör bygga på lösningar

som utvecklas av marknaden (prop. 2009/10:175 s. 70 f.). De bör uppfylla krav på hög säkerhet och tillgänglighet samt teknisk samverkansförmåga. Regeringen uttalade vidare att hanteringen av e-legitimationer bör samordnas och styras i större utsträckning än hittills.

Uppdrag att inordna inköpsverksamheter inom den statliga inköpssamordningen

Regeringen har den 6 maj 2010 uppdragit åt Kammarkollegiet att förbereda och genomföra inordnandet av upphandlingsverksamheterna som sker genom ramavtal och som avser statlig inköpssamordning vid vissa myndigheter (dnr Fi2010/2733). Uppdraget ska vara genomfört senast den 1 januari 2011.

En myndighet för samordning av elektronisk identifiering och signering

Behovet av en myndighet

Tillgång till säkra och effektiva metoder för elektronisk signering och identifiering är en förutsättning för utvecklingen av nya och mer avancerade e-tjänster hos myndigheter och kommuner. Den lösning för samordning av hanteringen av elektronisk identifiering och signering, som E-delegationen föreslagit, syftar till att samtliga e-legitimationer som uppfyller de uppställda kraven ska kunna användas av medborgare och företag när de använder förvaltningens e-tjänster. Lösningen kan också förväntas leda till en effektivisering av arbetssätt hos myndigheter och kommuner, bland annat genom att behovet av specialistkompetens vid den enskilda myndigheten eller kommunen bör minska. Detta är viktigt inte minst för små myndigheter och kommuner.

Den föreslagna lösningen möjliggör vidare att samtliga leverantörer som har en lösning som uppfyller de uppställda kraven kan få tillträde till marknaden. En sådan lösning kan därmed förväntas förbättra förutsättningarna för en fungerande konkurrens på marknaden för elektronisk identifiering och signering. Remissinstanserna stödjer i stort utredningens förslag till förbättring av samordningen genom att inrätta en nämnd.

Regeringen delar uppfattningen att dessa övergripande syften är väsentliga för den fortsatta utvecklingen på området. Regeringen bedömer också, i likhet med ett flertal av de remissinstanser som uttalar sig i frågan, att E-delegationens förslag kan förväntas leda till att dessa syften uppfylls bättre än i dag. Eftersom metoder för elektronisk identifiering och signering är en del av en infrastruktur som är gemensam för statlig och kommunal förvaltning är det enligt regeringens mening rimligt att staten tar ett övergripande ansvar för att en sådan infrastruktur kommer till stånd. Mot denna bakgrund anser regeringen att det bör inrättas en myndighet för samordning av elektronisk identifiering och signering.

Syftet med myndigheten

Myndighetens verksamhet bör ha följande övergripande syften:

- Privatpersoner och företag ska kunna använda en och samma e-legitimation vid nyttjande av alla e-tjänster som tillhandahålls av statliga myndigheter och kommuner.
- Konkurrensen och förutsättningarna för utveckling av nya tjänster för elektronisk identifiering och signering ska förbättras.
- Myndigheternas och kommunernas kostnader ska minska genom att färre kompetenser och funktioner behöver finnas hos varje organisation när fler funktioner är centralt samordnade eller upphandlas på marknaden.

Myndighetens uppgifter

Myndigheten ska samordna statens och kommunernas arbete med och användning av metoder och tjänster för elektronisk identifiering och signering (e-legitimationer) samt, om det behövs, tillhandahålla myndigheter och kommuner tjänster inom området. I detta ingår

- att fastställa de krav som ska vara gemensamma för de statliga myndigheternas användning av elektronisk identifiering och signering, och

- att myndigheten ska säkerställa att nödvändiga tjänster och funktioner (t.ex. identitetsintygsgivare, anvisningstjänster samt register över godkända identitetsintygsgivare, anvisningstjänster och e-tjänsteleverantörer) finns tillgängliga för förvaltningen.

Även i fortsättningen bör förvaltningen använda sig av tjänster och metoder som utvecklas och tillhandahålls av aktörer på marknaden. I detta sammanhang ska lagen (2007:1091) om offentlig upphandling beaktas. Myndigheten ska på lämpligt sätt välja ut och godkänna leverantörer av sådana tjänster. Om det krävs för att säkerställa behovet av nödvändiga tjänster och funktioner ska myndigheten sluta avtal med identitetsintygsgivare och med leverantörer av tjänster för identifiering och signering. Om det är nödvändigt ska myndigheten i egen regi tillhandahålla tjänster för identitetsintyg till anslutna myndigheter.

Det är viktigt att myndighetens organisation och verksamhet utformas på ett sådant sätt att goda förutsättningar ges för konkurrens och för utveckling av tjänster på marknaden.

Myndigheten bör därför tillhandahålla tjänster till myndigheter och kommuner endast om det är nödvändigt för att säkerställa förvaltningens tillgång till elektronisk identifiering och signering under de förutsättningar och med de mål som angivits. Utförandet av sådana tjänster bör i normalfallet upphandlas på marknaden. Detta gäller såväl identitetsintygstjänster som tjänster för identifiering och signering. Myndigheten ska emellertid inte, om det inte finns särskilda skäl, utföra uppgifter som faller inom den statliga inköpssamordningen som Kammarkollegiet ansvarar för (se även ovannämnda uppdrag till Kammarkollegiet).

Utöver dessa löpande uppgifter ska myndigheten ansvara för att på ett övergripande plan följa utvecklingen inom området. Detta avser exempelvis frågor om organisationslegitimationer och anlitande av ombud vid elektroniska kontakter med myndigheterna. Myndigheten ska följa utvecklingen såväl i Sverige som internationellt när det gäller tekniska och administrativa lösningar för elektronisk identifiering och signering. Myndigheten ska också delta i internationellt samarbete i dessa avseenden.

Myndighetens verksamhet ska ge marknaden förutsättningar att utveckla de lösningar som krävs för förvaltningens behov.

Verksamheten bör organiseras på ett sådant sätt att myndighetens informationsresurser och tjänster så långt som möjligt kan utgöra utgångspunkt för kommersiella tjänster.

Myndighetens organisation

Elektronisk identifiering och signering är centrala funktioner för e-förvaltningen och för samhället i övrigt. Det är viktigt att myndigheten har ett högt förtroende och en hög legitimitet i hela den offentliga förvaltningen och hos näringslivet. Det är vidare angeläget att verksamheten bedrivs med en stor grad av självständighet gentemot de myndigheter som använder nämndens tjänster eller vars verksamhet i övrigt påverkas av dess beslut. Förslaget att placera nämnden vid Skatteverket har tillstyrkts av en majoritet av de remissinstanser som uttalat sig i frågan. Några remissinstanser framhåller dock att det är viktigt att inte värdmyndighetens egna behov tillåts styra utvecklingen.

Regeringen anser att den samordning som myndigheten ska ansvara för bör bedrivas med en hög grad av självständighet. Verksamheten ska därför organiseras i form av en nämndmyndighet. Nämndens ordförande och övriga ledamöter ska utses av regeringen. Skatteverket ska tillhandhålla kansliresurser och administrativt stöd till nämnden. Personalen ska vara anställd i Skatteverket. Nämnden ska ansvara för arbetsledning avseende personalens arbete med nämndens uppgifter.

Finansiering av verksamheten

Statliga myndigheters och kommuners användning av tjänster för identifiering och signering ska, liksom nu, finansieras av respektive myndighet eller kommun. När en statlig myndighet eller kommun använder nämndens tjänster ska myndigheten eller kommunen betala en avgift. De samlade avgiftsintäkterna ska helt finansiera de samlade kostnader som nämnden har för användning av upphandlade tjänster för identifiering, signering och tillhandahållande av identitetsintyg. Avgiftsfinansieringen bör leda till lägre totala kostnader för såväl varje statlig myndighet och kommun som förvaltningen som helhet.

Därutöver bör nämndens verksamhet på sikt i så stor utsträckning som möjligt täckas av avgiftsintäkter.

Uppdraget

En särskild utredare ska förbereda och genomföra bildandet av en nämnd för samordning av statens och kommunernas hantering av metoder och tjänster för elektronisk identifiering och signering (e-legitimationer). Nämnden ska ha Skatteverket som värdmyndighet. Utredaren ska utgå från vad regeringen ovan angett om nämndens verksamhetsområde. Utredaren ska bedriva sitt arbete så att nämnden kan inleda sin verksamhet den 1 januari 2011.

Utredaren ska lämna förslag på nämndens ansvarsområde, finansieringsform och mål för verksamheten. Förslagens verksamhetsmässiga, ekonomiska och personella konsekvenser samt konsekvenser för företag ska redovisas. Utredaren ska särskilt uppmärksamma konsekvenserna för statligt och kommunalt ägda bolag och hur dessas deltagande i samordningen förhåller sig till bestämmelserna om offentlig upphandling. Utredaren ska lämna förslag till instruktion för nämnden och andra författningsändringar som bildandet av nämnden föranleder.

Nämndens organisation

Utredaren ska föreslå lämpliga arbetsformer för verksamheten samt en arbetsordning, en arkivplan och en verksamhetsplan för nämnden. Verksamhetsplanen ska avse perioden 2011–2013 och innefatta en tidsplan för genomförandet av olika delar av nämndens verksamhet. Av verksamhetsplanen ska det framgå på vilka områden standarder och liknande krav ska fastställas samt när och i vilken ordning detta kan göras.

I förberedelserna ingår att bedöma vilken kompetens som är nödvändig för nämndens verksamhet samt så långt som möjligt förbereda anställning av den personal som behövs vid kansliet.

Utredaren ska analysera om någon verksamhet vid en befintlig myndighet bör överföras till nämnden.

Nämndens finansiering

Utredaren ska närmare analysera förutsättningarna för att finansiera verksamheten till större delen med avgifter. Hur och i vilken utsträckning en övergång till avgiftsfinansiering kan ske ska redovisas i utredarens slutredovisning. Utredaren ska lämna förslag

till de författningsändringar och reglering i övrigt som krävs för avgiftsfinansiering av verksamheten.

Nämndens tjänster åt andra myndigheter

Utredaren ska analysera vilka tjänster nämnden ska tillhandahålla andra myndigheter. Verksamhetsplanen ska ange vilka tjänster som nämnden ska tillhandahålla myndigheter och kommuner, om tjänsterna ska upphandlas på marknaden samt en tidsplan för när dessa tjänster kan tillhandahållas.

Utredaren bör i första hand överväga om ansvaret för eventuella upphandlingar bör överlåtas till Kammarkollegiets inköps-samordningsverksamhet i syfte att åstadkomma samordnade avtal för statliga myndigheter och kommuner. I detta sammanhang bör regeringens ovannämnda beslut av den 6 maj 2010 beaktas (dnr Fi2010/2733).

Förberedelser för nämndens verksamhet

Utredaren ska förbereda nämndens verksamhet genom att påbörja arbetet med underlag för de krav som ska vara gemensamma för de statliga myndigheternas användning av elektronisk identifiering och signering. Utredaren ska analysera i vilken mån sådana krav bör fastställas i föreskrifter.

I uppdraget ingår att analysera hur förvaltningens behov av metoder och tjänster för elektronisk identifiering och signering kan tillgodoses utan att onödiga investeringar görs i infrastruktur.

Om utredaren bedömer att det finns behov av att upphandla tjänster och produkter för samordningsfunktionens verksamhet i de delar som omfattar tillhandahållande av tjänster till andra myndigheter, ska utredaren påbörja arbetet med att ta fram specifikationer och underlag för sådana upphandlingar.

Utredaren ska också finna former för hur utvärdering av tekniska lösningar och val av leverantörer ska ske i samband med upphandling.

Nämndens samverkan med andra aktörer

Utredaren ska bedöma vilket behov det finns av samverkan mellan nämnden och övriga statliga myndigheter, kommuner samt näringslivet och dess organisationer. Utredaren ska finna former för sådan samverkan.

Utredaren ska analysera hur myndigheten på ett ändamålsenligt sätt ska delta i internationellt samarbete.

Integritetsfrågor

Såväl i E-delegationens ovan nämnda delbetänkande som i några remissyttranden framhålls vikten av att integritetsfrågorna hanteras på ett ansvarsfullt sätt. Samordningsfunktionen kan, såsom framhålls i betänkandet, styra hanteringen av elektronisk identifiering och signering så att integriteten skyddas på ett ändamålsenligt sätt. Felaktigt utformat skulle ett system för samordning av elektronisk identifiering och signering kunna leda till risker för den personliga integriteten, t.ex. om uppgifter om en enskilds alla kontakter med myndigheterna skulle samlas på samma ställe, eller om överflödig information om t.ex. innehållet i kommunikationer skulle behandlas av andra än berörda myndigheter. Det är viktigt att nämndens verksamhet utformas på ett sådant sätt att onödig behandling av personuppgifter och andra integritetsrisker undviks.

Utredaren ska därför särskilt uppmärksamma att nämndens verksamhet organiseras på ett sådant sätt att den nödvändiga behandlingen av personuppgifter minimeras och de registrerade på ett effektivt sätt kan utöva sina rättigheter. Utgångspunkten ska vara att personuppgiftslagens (1998:204) bestämmelser ska gälla. Utredaren ska dock överväga om det krävs särskild reglering av nämndens hantering av personuppgifter, t.ex. sekretessreglering eller reglering i en registerförfattning.

Uppdragets genomförande och tidsplan

Samråd

Uppdraget ska genomföras i samråd med Arbetsförmedlingen, Bolagsverket, Centrala studiestödsnämnden, Datainspektionen, Domstolsverket, Försäkringskassan, Jordbruksverket, Kammar-

kollegiet, Konkurrensverket, Lantmäteriet, Migrationsverket, Myndigheten för samhällsskydd och beredskap, Pensionsmyndigheten, Post- och Telestyrelsen, Riksarkivet, Rikspolisstyrelsen, Skatteverket, Tillväxtverket, Transportstyrelsen, Tullverket, E-delegationen (Fi 2009:01) samt Sveriges Kommuner och Landsting (SKL). Vidare ska utredaren samråda med andra statliga myndigheter, kommuner, organisationer och med näringslivets aktörer i den utsträckning som behövs.

Myndigheterna ska efter samråd med utredaren lämna utredaren det underlag som utredaren och myndigheten bedömer behövs för att genomföra uppdraget.

Redovisning

Utredaren ska senast den 1 september 2010 lämna förslag till instruktion för nämnden samt förslag till andra författningsändringar som krävs för att myndigheten ska kunna inleda sin verksamhet den 1 januari 2011.

Senast den 1 november 2010 ska utredaren lämna förslag till verksamhetsmål och verksamhetsplan för 2011–2013.

Det står utredaren fritt att lämna även andra förslag som behövs för nämndens verksamhet.

Uppdraget ska slutredovisas senast den 31 december 2010.

(Finansdepartementet)

Svensk författningssamling

SFS 2010:1497
Utkom från trycket
den 7 december 2010

Förordning med instruktion för E-legitimationsnämnden;

utfärdad den november 2010.

Regeringen föreskriver följande.

Uppgifter

1 § E-legitimationsnämnden ska stödja och samordna elektronisk identifiering och signering (e-legitimationer) i den offentliga förvaltningens e-tjänster.

2 § Myndigheten ska utveckla specifikationer och liknande krav som ska vara gemensamma för myndigheter under regeringen i deras användning av e-legitimationer. Myndigheten ska delta i internationellt standardiseringsarbete, internationellt samarbete och informationsutbyte inom sitt ansvarsområde.

Ledning

3 § Myndigheten leds av en nämnd.

4 § Nämnden ska bestå av högst sju ledamöter. Ledamöterna utses av regeringen för en bestämd tid.

Organisation

5 § Vid myndigheten ska det finnas ett kansli.

6 § Skatteverket ska upplåta lokaler samt sköta administrativa och handläggande uppgifter åt myndigheten.

7 § Skatteverket ska efter samråd med nämnden uppdra åt någon som är anställd vid verket att ansvara för kansliet.

Denna förordning träder i kraft den 1 januari 2011.

På regeringens vägnar

ANNA-KARIN HATT

Rikard Jermsten
(Finansdepartementet)

REGERINGEN

Regeringsbeslut **IV 1**

2010-12-02 Fi2010/5409

Finansdepartementet

Förordnande av ledamöter i E-legitimationsnämnden

Regeringen förordnar följande personer att vara ledamöter i E-legitimationsnämnden:

generaldirektören Annika Bränström

direktören Gunilla Glasare

generaldirektören Göran Gräslund

verkställande direktören Kerstin af Jochnick

lagmannen Pia Johansson

Förordnandena gäller fr.o.m. den 1 januari 2011 t.o.m. den 31 januari 2010.

Vidare utser Stig Jönsson till att vara ordförande i nämnden.

På regeringens vägnar

Anna-Karin Hatt

Gustaf Johnssén

Begrepp och definitioner

Definitioner av centrala begrepp för den föreslagna infrastrukturen:

1. *Svensk e-legitimation*; de certifikat, säkerhetsdosor eller andra hjälpmedel för identifiering som har anslutits till infrastrukturen för svensk e-legitimation,
2. *Infrastrukturen för svensk e-legitimation*; den infrastruktur för elektronisk legitimering och elektronisk underskrift som E-legitimationsnämnden inrättat för samverkan mellan identitetsutfärdare, e-tjänsteleverantörer och användare av svensk e-legitimation,
3. *Infrastrukturen för identifiering*; en del av infrastrukturen för svensk e-legitimation där e-tjänsteleverantörer kan erhålla identitets- och attributsintyg för att granska om uppgifter som lämnats om identitet eller juridisk behörighet eller andra attribut är riktiga,
4. *Identitetsutfärdare*; den som utfärdar identitetsintyg inom infrastrukturen för identifiering,
5. *Attributsutfärdare*; den som utfärdar attributsintyg inom infrastrukturen för identifiering eller en annan anknytande infrastruktur,
6. *E-tjänsteleverantör*; den som tillhandahåller en e-tjänst som stöds av Svensk e-legitimation.[1]
7. *Användare*; den som har en privat e-legitimation eller en e-tjänstelegitimation som godtas som Svensk e-legitimation,
8. *Identitetsintyg*; ett av en identitetsutfärdare utställt intyg i elektronisk form med uppgifter om en användares identitet och attribut,

[1] Här avses myndigheters, landstings, kommuners och vissa andra organs e-tjänster. Den närmare avgränsningen av dessa organ har inte genomlysts ännu i utredningsarbetet men en avgränsning kan eventuellt utformas med 2 kap 3-4 §§ offentlighets- och sekretesslagen (2009:400) som förebild.

9. *Attributsintyg*; ett av en attributsutfärdare utställt intyg i elektronisk form med uppgifter om användares juridiska behörighet, organisatoriska roll eller andra egenskaper,
10. *Centralt utfärdarregister*; ett register som E-legitimationsnämnden för över identitets- och attributsutfärdare som är anslutna till infrastrukturen för identifiering,
11. *Centralt e-tjänsteregister*; ett register som E-legitimationsnämnden för över e-tjänsteleverantörer som är anslutna till infrastrukturen för identifiering,
12. *Tillitsnivå*; den skyddsklass till vilken en e-legitimation hänförs, och
13. *Signaturtjänsten*; det tekniska och administrativa stöd som E-legitimationsnämnden lämnar åt en e-tjänsteleverantör för att användare ska kunna skriva under handlingar elektroniskt, och
14. *Anvisningstjänsten*; det tekniska och administrativa stöd som E-legitimationsnämnden lämnar åt en e-tjänsteleverantör för att användare ska kunna välja e-legitimation.

Utkast till förordning om infrastrukturen för Svensk e-legitimation

Härigenom föreskrivs följande.

Inledande bestämmelser

Förordningens innehåll

1 § I denna förordning finns bestämmelser om
1. definitioner (2 §)
2. syfte och tillämpningsområde (3 och 4 §§),
3. register och persondataskydd (5–14 §§),
4. anvisningstjänst, signeringstjänst och underleverantörer (15–17 §§),
5. anslutning (18–31 §§),
6. tjänsternas utformning och aktivering (32–35 §§),
7. tjänsternas användning (36–40 §§),
8. avgifter (41 §), och
9. bemyndigande (42 §).

Definitioner

2 § I denna förordning menas med
1. *Svensk e-legitimation*; de certifikat, säkerhetsdosor eller andra hjälpmedel för identifiering som har anslutits till infrastrukturen för svensk e-legitimation,
2. *Infrastrukturen för svensk e-legitimation*; den infrastruktur för elektronisk legitimering och elektronisk underskrift som E-legitimationsnämnden inrättat för samverkan mellan identitetsutfärdare, e-tjänsteleverantörer och användare av svensk e-legitimation,
3. *Infrastrukturen för identifiering*; en del av infrastrukturen för svensk e-legitimation där e-tjänsteleverantörer kan erhålla identitets- och attributsintyg för att granska om uppgifter som

lämnats om identitet eller juridisk behörighet eller andra attribut är riktiga,

4. *Identitetsutfärdare*; den som utfärdar e-legitimationer och tillhörande identitetsintyg inom infrastrukturen för identifiering,

5. *Attributsutfärdare*; den som utfärdar attributsintyg inom infrastrukturen för identifiering eller en annan anknytande infrastruktur,

6. *E-tjänsteleverantör*; den som tillhandahåller en e-tjänst som stöds av svensk e-legitimation,

7. *Användare*; den som har en privat e-legitimation eller en e-tjänstelegitimation som godtas som svensk e-legitimation,

8. *Identitetsintyg*; ett av en identitetsutfärdare utställt intyg i elektronisk form med uppgifter om en användares identitet och attribut,

9. *Attributsintyg*; ett av en attributsutfärdare utställt intyg i elektronisk form med uppgifter om användares juridiska behörighet, organisatoriska roll eller andra egenskaper,

10. *Utfärdarregister*; ett register som E-legitimationsnämnden för över identitets- och attributsutfärdare som är anslutna till infrastrukturen för identifiering,

11. *E-tjänsteregister*; ett register som E-legitimationsnämnden för över e-tjänsteleverantörer som är anslutna till infrastrukturen för identifiering,

12. *Tillitsnivå*; den skyddsklass till vilken en e-legitimation hänförs, och

13. *Signaturtjänsten*; det tekniska och administrativa stöd som E-legitimationsnämnden lämnar åt en e-tjänsteleverantör för att användare ska kunna skriva under handlingar elektroniskt,

14. *Anvisningstjänsten*; det tekniska och administrativa stöd som E-legitimationsnämnden lämnar åt en e-tjänsteleverantör för att användare ska kunna välja e-legitimation,

Förordningens syfte och tillämpningsområde

3 § Denna förordning syftar till att etablera en infrastruktur för Svensk e-legitimation inom offentlig förvaltning och att samordna och förenkla e-tjänsteleverantörernas användning av funktioner för elektronisk legitimering och elektronisk underskrift.

4 § Förordningen gäller för statliga myndigheter under regeringen. Den tillämpas också på myndigheter under riksdagen och kommunala myndigheter som anslutit sig till infrastrukturen för Svensk e-legitimation.

Register och behandling av personuppgifter

Utfärdar- och e-tjänsteregister

5 § E-legitimationsnämnden ska föra register över

1. de identitetsutfärdare och attributsutfärdare som är anslutna till infrastrukturen för identifiering (utfärdarregister), och
2. de e-tjänsteleverantörer som är anslutna till infrastrukturen för identifiering (e-tjänsteregister).

Registrens innehåll

6 § I E-legitimationsnämndens utfärdarregister och e-tjänsteregister får uppgifter finnas om

1. elektronisk adress till anslutna identitetsutfärdare, attributsutfärdare och e-tjänsteleverantörer,
2. vilken identitets- och attributsinformation en e-tjänsteleverantör behöver för en viss e-tjänst,
3. vilka uppgifter en identitets- eller en attributsutfärdare kan tillhandahålla i identitets- eller attributsintyg, och
4. de certifikat och publika nycklar som behövs för att skydda uppgifter i utfärdade identitets- och attributsintyg och att kontrollera om intyg som tagits emot är äkta.

7 § Utfärdar- och e-tjänsteregistren får inte innehålla

1. information om kommunikation mellan användare och e-tjänsteleverantörer,
2. innehållet i identitets- eller attributintyg eller handlingar som ska undertecknas eller har undertecknats, eller
3. uppgifter som direkt eller indirekt kan hänföras till en fysisk person som är i livet.

Elektronisk åtkomst

8 § E-tjänsteleverantörer och användare ska ha elektronisk åtkomst till utfärdar- och e-tjänsteregistren i den omfattning som behövs för att infrastrukturen för identifiering ska fungera.

9 § Utfärdarregistret får göras tillgängligt elektroniskt så att det kan användas för att utfärda identitets- eller attributintyg utanför infrastrukturen för svensk e-legitimation.

Persondataskyddande teknik

10 § De tekniska och administrativa lösningarna ska ges en sådan utformning att så få personuppgifter som möjligt samlas in, lämnas ut eller annars behandlas och att inte fler uppgifter än nödvändigt samlas in eller bevaras så att de blir direkt tillgängliga.

Registrens användning

11 § Uppgifter i utfärdarregistret får användas utanför infrastrukturen för identifiering för att stödja motsvarande tjänster åt företag och andra organisationer som tillhandahålls genom e-tjänsteregister som inte är en del av infrastrukturen för identifiering.

E-tjänsteleverantörers och identitets- och attributsutfärdares behandling av personuppgifter

12 § En identitets- eller attributsutfärdare får inhämta personuppgifter endast direkt från en användare eller med dennes uttryckliga samtycke och endast i den utsträckning som är nödvändig för att utfärda eller upprätthålla certifikat eller identitets- eller attributsintyg. Uppgifterna får inte samlas in eller behandlas för andra ändamål utan uttryckligt samtycke från användaren.

13 § En identitets- eller attributsutfärdare får inte bevara uppgifter som kan användas för att kartlägga en användares nyttjande av

tillhandahållna tjänster i större utsträckning än vad som är nödvändigt för att avtalet med användaren ska kunna fullgöras.

14 § Personuppgifter hos en identitets- eller attributsutfärdare eller en e-tjänsteleverantör får inte sambearbetas med uppgifter hos en annan identitets- eller attributsutfärdare eller e-tjänsteleverantör om det inte krävs för att Infrastrukturen för Svensk e-legitimation ska fungera.

Anvisningstjänst, signeringstjänst och underleverantörer

15 § E-legitimationsnämnden ska tillhandahålla en tjänst genom vilken användare av e-tjänster ges stöd i valet av vilken e-legitimation som ska brukas (anvisningstjänst). E-legitimationsnämnden ska ansvara gentemot användaren för denna tjänst.

16 § E-legitimationsnämnden ska tillhandahålla en tjänst för elektronisk underskrift av handlingar (signaturtjänst). E-legitimationsnämnden ska ansvara gentemot användaren för denna tjänst.

17 § E-legitimationsnämnden får överlämna den tekniska driften och skötseln av register och tjänster till underleverantörer men ska svara för verksamheten som om nämnden hade utfört åtgärderna själv.

Anslutning

Anslutning av identitetsutfärdare till infrastrukturen för identifiering

18 § Efter ansökan ansluter E-legitimationsnämnden en identitetsutfärdare till infrastrukturen för identifiering och registrerar utfärdaren i utfärdarregistret. Anslutning sker genom att nämnden tecknar avtal med utfärdaren. Registrering sker efter ansökan i ett förvaltningsärende.

19 § Den som uppfyller kraven i ett förfrågningsunderlag enligt lagen (2011:000) om valfrihet för svensk e-legitimation och godtar de juridiska, tekniska och administrativa villkoren ska ha rätt att anslutas till infrastrukturen för identifiering.

Anslutning av attributsutfärdare till infrastrukturen för identifiering

20 § Efter ansökan ansluter E-legitimationsnämnden en attributsutfärdare till infrastrukturen för identifiering och registrerar utfärdaren i utfärdarregistret. Anslutning av attributsutfärdare som är en myndighet under regeringen sker genom beslut i ett förvaltningsärende. Anslutning av annan sker genom att nämnden tecknar avtal med attributsutfärdaren. Registrering sker efter ansökan i ett förvaltningsärende.

21 § En attributsutfärdare får anslutas till infrastrukturen för identifiering om utfärdaren

1. enligt lag eller författning ska registrera och tillhandahålla de uppgifter som lämnas i attributsintygen och uppgifterna är av generell betydelse från kontrollsynpunkt, eller
2. det finns särskilda skäl från kontrollsynpunkt att ett visst slag av attribut från en viss utfärdare ska kunna lämnas inom infrastrukturen för identifiering.

22 § Särskilda skäl från kontrollsynpunkt föreligger om det finns ett utbrett behov inom offentlig förvaltning av tillförlitlig åtkomst till uppgiften och den inte finns tillgänglig på fungerande sätt i annan ordning.

23 § E-legitimationsnämnden får i ett beslut om anslutning som villkor ange att attributsutfärdaren ska följa de juridiska, tekniska och administrativa villkor som nämnden bestämmer.

24 § E-legitimationsnämnden får ingå avtal om anslutning av en attributsutfärdare endast om utfärdaren accepterar de juridiska, tekniska och administrativa villkoren för anslutning till infrastrukturen för identifiering.

Anslutning av e-tjänsteleverantörer till infrastrukturen för identifiering

25 § Efter ansökan ansluter E-legitimationsnämnden en e-tjänsteleverantör till infrastrukturen för identifiering. Anslutning av e-tjänsteleverantör som är en myndighet under regeringen sker genom beslut i ett förvaltningsärende. Anslutning av annan sker

genom att nämnden tecknar avtal med e-tjänsteleverantören. Registrering sker efter ansökan i ett förvaltningsärende.

26 § E-legitimationsnämnden får i ett beslut om anslutning som villkor ange att e-tjänsteleverantören ska följa de juridiska, tekniska och administrativa villkor som nämnden bestämmer

27 § E-legitimationsnämnden får ingå avtal om anslutning av en e-tjänsteleverantör endast om utfärdaren accepterar de juridiska, tekniska och administrativa villkoren för anslutning till infrastrukturen för identifiering.

Anslutning av e-tjänsteleverantörer till signaturtjänsten

28 § Efter ansökan ansluter E-legitimationsnämnden en e-tjänsteleverantör till signaturtjänsten. Anslutning av en e-tjänsteleverantör som är en myndighet under regeringen sker genom beslut i ett förvaltningsärende. Anslutning av annan sker genom att nämnden tecknar avtal med e-tjänsteleverantören. Registrering i e-tjänsteregistret sker efter ansökan i ett förvaltningsärende.

29 § E-legitimationsnämnden får i ett beslut om anslutning som villkor ange att e-tjänsteleverantören ska följa de juridiska, tekniska och administrativa villkor som nämnden bestämmer.

30 § E-legitimationsnämnden får ingå avtal om anslutning av en e-tjänsteleverantör endast om utfärdaren accepterar de juridiska, tekniska och administrativa villkoren för anslutning till infrastrukturen för identifiering.

Ansökan om anslutning

31 § En ansökan om anslutning ska ges in till E-legitimationsnämnden.

Tjänsternas utformning och aktivering

32 § En svensk e-legitimation ska vara utformad, skyddas och användas enligt en viss tillitsnivå. Utfärdare av svensk e-legitimation, identitetsutfärdare och attributsutfärdare ska tillämpa sådana regler och rutiner att det utifrån tillämplig tillitsnivå finns fog för att lita på de e-legitimationer, identitetsintyg och attributsintyg som tillhandahålls.

33 § Skyddet för infrastrukturen för svensk e-legitimation ska närmare bestämmas i ett tillitsramverk. Detta ramverk ska löpande anpassas till tekniska standarder och utvecklingen i övrigt samt de hot och risker som kan uppkomma på området.

34 § Identitetsutfärdares, attributsutfärdares och e-tjänsteleverantörers anslutningar och funktioner, som samverkar med infrastrukturen för svensk e-legitimation, får inte aktiveras förrän de testats och E-legitimationsnämnden funnit att de fungerar på ett tillförlitligt sätt i enlighet med tillitsramverket och tekniska specifikationer.

E-legitimationsnämnden ska tillhandahålla stöd för att testa att en tjänst som ska anslutas uppfyller kraven enligt de tekniska specifikationerna och att den kan samverka med infrastrukturen för identifiering.

35 § E-legitimationsnämnden ska bestämma rutiner för hur angrepp mot informationssäkerheten inom Infrastrukturen för Svensk e-legitimation ska hanteras.

E-legitimationsnämnden får genom beslut för enskilda fall avbryta en anslutning eller en funktion som inte fungerar på ett tillförlitligt sätt.

Tjänsternas användning

36 § En användare som tilldelats en privat e-legitimation eller en e-tjänstelegitimation brukar den för

1. *legitimering vid tillträde*, för att elektroniskt få tillgång till uppgifter som får lämnas ut till honom eller henne och för att få skydd mot att obehöriga får tillgång till uppgifterna under sken av att vara honom eller henne, eller

2. *legitimering vid uppgiftslämnande*, för att få lämna uppgifter elektroniskt och för att få skydd mot att obehöriga lämnar uppgifter under sken av att vara honom eller henne,

3. *elektronisk underskrift*, för att ställa ut elektroniska handlingar som är skyddade mot förfalskning och förnekande av elektronisk underskrift på liknande sätt som en handling som är undertecknad på traditionellt sätt.

37 § En myndighet använder identitetsintyg för

1. *identifiering vid tillträde*, för att kunna ge tillgång till uppgifter elektroniskt så att inte obehöriga får ut uppgifterna,

2. *identifiering vid uppgiftslämnande*, för att kontrollera vem som är ansluten när vissa uppgifter lämnas, och

3. *kontroll av elektronisk underskrift*, för att granska att en handling som undertecknats elektroniskt är utställd av den som anges som undertecknare och att texten inte har ändrats.

38 § En myndighet använder ett attributsintyg för att kontrollera om en person har juridisk behörighet att agera för annans räkning, viss befattning eller annan roll eller egenskap eller på annat sätt är förknippad med något som en attributsutfärdare kan intyga.

39 § Privat e-legitimation får användas av fysiska personer när de kommunicerar för egen räkning och när de kommunicerar i egenskap av företrädare för annan. E-tjänstelegitimation får användas av fysiska personer när de kommunicerar i egenskap av anställda eller uppdragstagare och, om arbets- eller uppdragsgivaren godtar det, när de kommunicerar för egen räkning.

40 § Identitetsutfärdares, attributsutfärdares och e-tjänsteleverantörers anslutningar och funktioner, som samverkar med infrastrukturen för Svensk e-legitimation, får inte aktiveras förrän de testats och E-legitimationsnämnden funnit att de fungerar på ett tillförlitligt sätt.

Avgifter

41 § E-legitimationsnämnden [ ].

Bemyndigande

42 § E-legitimationsnämnden får meddela föreskrifter om

1. tillitsnivåer och tillitsramverk för Svensk e-legitimation,
2. e-legitimationernas, anvisnings- och signaturtjänsternas och identitets- och attributsintygens utformning och användning,
3. ansökan om anslutning enligt denna förordning och beredning av sådana ärenden,
4. certifiering och andra förfaranden för att visa överensstämmelse med tillitsnivåer och tillitsramverk,
5. aktivering av identitetsutfärdares, attributsutfärdares och e-tjänsteleverantörers anslutningar och funktioner, och
6. skydd för infrastrukturen för Svensk e-legitimation och samordnade åtgärder och anpassningar med anledning av missbruk eller angrepp.

Denna förordning träder i kraft den [ ] 2011

Regelverk för Infrastrukturen för Svensk e-legitimation

1. Bakgrund

1.1 Av lagen (2011:000) om valfrihet för Svensk e-legitimation följer att E-legitimationsnämnden får tillhandahålla ett valfrihetssystem för en *Infrastruktur för Svensk e-legitimation*. Användare av e-legitimationer ska kunna välja leverantör bland dem som anslutits till denna infrastruktur.

1.2 E-legitimationsnämnden ska enligt förordningen (2010:1497) med instruktion för nämnden stödja och samordna elektronisk identifiering och signering i den offentliga förvaltningens e-tjänster samt utveckla specifikationer och liknande krav som ska vara gemensamma för myndigheter under regeringen i deras användning av e-legitimationer.

1.3 Detta regelverk tillämpas inom *Infrastrukturen för Svensk e-legitimation*. Till denna infrastruktur hör att

a) utfärda, använda, verifiera och spärra *Svensk e-legitimation*,

b) tillhandahålla en *Infrastruktur för identifiering* där

i. e-tjänsteleverantörer kan erhålla *identitets- och attributsintyg* för att granska om uppgifter som lämnats om identitet eller juridisk behörighet eller andra attribut är riktiga,

ii. *centrala register* över aktörer förmedlar uppgifter om aktörernas tjänster och funktioner för tillit och säkert informationsutbyte,

iii. en *anvisningstjänst* kan ge användaren av en e-tjänst hjälp att välja e-legitimation att bruka i e-tjänsten,

c) tillhandahålla en *signeringstjänst* som gör det möjligt för användaren att skriva under elektroniska handlingar.

1.4 Dessa regler har till syfte att etablera funktioner för e-legitimationer, elektroniska underskrifter och identitets- och attributsintyg som är enkla att förstå och använda och som på ett balanserat sätt kan tillgodose skyddet för

rättssäkerheten, informationssäkerheten och enskildas personliga integritet.

1.5 De tekniska och administrativa lösningarna ska utformas så att så få personuppgifter som möjligt samlas in, lämnas ut eller annars behandlas och att inte fler uppgifter än nödvändigt samlas in och bevaras så att de blir direkt tillgängliga.

1.6 Den som tillhandahåller tjänster för identifiering inom Infrastrukturen för Svensk e-legitimation ska få tillhandahålla motsvarande tjänster åt företag och andra organisationer inom ramen för en anknytande infrastruktur för näringslivet. Detta regelverk har utformats i syfte att underlätta införandet av en sådan parallell infrastruktur.

2. Definitioner

I detta regelverk används följande beteckningar i nedan angiven betydelse.

1. *Svensk e-legitimation*; de certifikat, säkerhetsdosor eller andra hjälpmedel för identifiering som har anslutits till Infrastrukturen för Svensk e-legitimation,
2. *Infrastrukturen för Svensk e-legitimation*; den Infrastruktur för elektronisk legitimering och elektronisk underskrift som E-legitimationsnämnden inrättat för samverkan mellan identitetsutfärdare, e-tjänsteleverantörer och användare av Svensk e-legitimation,
3. *Infrastrukturen för identifiering*; en del av Infrastrukturen för Svensk e-legitimation där e-tjänsteleverantörer kan erhålla identitets- och attributsintyg för att granska om uppgifter som lämnats om identitet eller juridisk behörighet eller andra attribut är riktiga,
4. *Identitetsutfärdare*; den som utfärdar identitetsintyg inom Infrastrukturen för identifiering,

5. *Attributsutfärdare*; den som utfärdar attributsintyg inom Infrastrukturen för identifiering eller en annan anknytande infrastruktur,
6. *E-tjänsteleverantör*; den som tillhandahåller en e-tjänst som stöds av Svensk e-legitimation,
7. *Användare*; den som har en privat e-legitimation eller en e-tjänstelegitimation som godtas som Svensk e-legitimation,
8. *Identitetsintyg*; ett av en identitetsutfärdare utställt intyg i elektronisk form med uppgifter om en användares identitet och attribut,
9. *Attributsintyg*; ett av en attributsutfärdare utställt intyg i elektronisk form med uppgifter om användares juridiska behörighet, organisatoriska roll eller andra egenskaper,
10. *Centralt utfärdarregister*; ett register som E-legitimationsnämnden för över identitets- och attributsutfärdare som är anslutna till Infrastrukturen för identifiering,
11. *Centralt e-tjänsteregister*; ett register som E-legitimationsnämnden för över e-tjänsteleverantörer som är anslutna till Infrastrukturen för identifiering,
12. *Tillitsnivå*; den skyddsklass till vilken en e-legitimation hänförs,
13. *Signaturtjänsten*; det tekniska och administrativa stöd som E-legitimationsnämnden lämnar åt en e-tjänsteleverantör för att användare ska kunna skriva under handlingar elektroniskt, och
14. *Anvisningstjänsten*; det tekniska och administrativa stöd som E-legitimationsnämnden lämnar åt en e-tjänsteleverantör för att användare ska kunna välja e-legitimation.

3. Det samordnade området

Aktörer och uppgifter

1.7 *E-legitimationsnämnden* ska utveckla och svara för Infrastrukturen för Svensk e-legitimation. Till nämndens uppgifter hör att

a) *utarbeta underlag* för föreskrifter beträffande Infrastrukturen för Svensk e-legitimation, avtal och allmänna

villkor i de delar Infrastrukturen för Svensk e-legitimation regleras genom civilrättsliga överenskommelser samt riktlinjer, vägledningar, dokumentation och tekniska krav för Infrastrukturen för Svensk e-legitimation,

b) *meddela föreskrifter* inom ramen för den normgivningskompetens som delegeras till nämnden,

c) *upphandla leverantörer* av tekniska tjänster för Infrastrukturen för Svensk e-legitimation,

d) *sluta avtal* med aktörer inom Infrastrukturen för Svensk e-legitimation,

e) *inrätta en Infrastruktur för identifiering* inom ramen för Infrastrukturen för Svensk e-legitimation, och för denna infrastruktur

i. inrätta ett valfrihetssystem för Infrastrukturen för identifiering, och

ii. besluta och avtala om anslutning till Infrastrukturen för identifiering.

1.8 *Identitetsutfärdare* som ansluts till Infrastrukturen för identifiering ska tillhandahålla identitetsintyg åt e-tjänsteleverantörer. Den som lämnar identitetsintyg inom Infrastrukturen för identifiering ska ha ställt ut de e-legitimationer som brukas eller – såvitt är av betydelse för ett lämnat intyg – svara för e-legitimationen och anknytande funktioner som om Identitetsutfärdaren själv hade ställt ut e-legitimationen och tillhandahållit anknytande funktioner.

1.9 *Attributsutfärdare* som anslutits till Infrastrukturen för identifiering ska tillhandahålla uppgifter åt e-tjänsteleverantörer om juridisk behörighet, roll, personnummer eller annat av betydelse för en e-tjänsteleverantör som ska kontrollera uppgifter om användare.

1.10 *Användare* brukar privat e-legitimation eller e-tjänstelegitimation i e-tjänster. Användaren väljer en identitetsutfärdare som nämnden anslutit till Infrastrukturen för identifiering. E-legitimationsnämnden informerar på sin webbplats om vilka identitetsutfärdare som har anslutits.

1.11 *E-tjänsteleverantörer*, anslutna till Infrastrukturen för identifiering, tillhandahåller e-tjänster där det krävs elektronisk legitimering eller elektronisk underskrift.

Register

1.12 E-legitimationsnämnden ska föra register över

a) de identitetsutfärdare och attributsutfärdare som är anslutna till Infrastrukturen för identifiering (*utfärdarregister*), och

b) de e-tjänsteleverantörer som är anslutna till Infrastrukturen för identifiering (*e-tjänsteregister*).

1.13 I dessa register ska finnas uppgifter om

a) elektroniska adresser till anslutna identitets- och attributsutfärdare och e-tjänsteleverantörer,

b) vilka uppgifter en e-tjänsteleverantör behöver för en viss e-tjänst,

c) vilka identitetsuppgifter och attribut som en identitets- eller en attributsutfärdare kan tillhandahålla, och

d) de certifikat och nycklar som en utfärdare av identitets- eller attributsintyg använder för att stämpla intygen och som e-tjänsteleverantörer använder för att kontrollera om mottagna intyg är äkta.

1.14 Uppgifter i utfärdarregistret ska få användas även inom anknytande infrastrukturer för motsvarande tjänster åt företag och andra organisationer, som registreras i e-tjänsteregister som inte är en del av Infrastrukturen för identifiering.

1.15 Utfärdar- och e-tjänsteregistren får inte innehålla personuppgifter såsom information om kommunikation mellan användare och e-tjänsteleverantörer, innehållet i identitets- eller attributintyg eller handlingar som ska skrivas under eller har undertecknats elektroniskt.

1.16 I förordningen (2010:000) om Infrastrukturen för Svensk e-legitimation finns föreskrifter om registrering i utfärdar- och e-tjänsteregistren.

Anvisningstjänst

1.17 E-legitimationsnämnden ska tillhandahålla en tjänst som tillför stöd, dels åt användare när de ska välja e-legitimation i en e-tjänst, dels åt den som tillhandahåller e-tjänsten beträffande vilken utfärdare av e-legitimationer som användaren valt (anvisningstjänst).
E-legitimationsnämnden ska svara gentemot användaren för dessa funktioner.

Signeringstjänst

1.18 E-legitimationsnämnden tillhandahåller inom ramen för Infrastrukturen för Svensk e-legitimation en tjänst som ger stöd för elektronisk underskrift av handlingar (signaturtjänst).

E-legitimationsnämnden ska svara gentemot användaren för signaturtjänsten.

Underleverantörer

1.19 E-legitimationsnämnden får överlämna den tekniska driften och skötseln av register och tjänster till underleverantörer men ska svara för verksamheten som om nämnden hade utfört åtgärderna själv.

E-legitimationer, m.m.

1.20 *E-legitimationer* såsom certifikat, säkerhetsdosor och liknande som ansluts till Infrastrukturen för Svensk e-legitimation utfärdas för användare som *privat e-legitimation* eller – i egenskap av anställd eller uppdragstagare – *som e-tjänstelegitimation*.

1.21 *Användare anskaffar* privat e-legitimation från identitetsutfärdare som är anslutna till Infrastrukturen för Svensk e-legitimation.

1.22 *Myndigheter* och andra organisationer *anskaffar e-tjänstelegitimationer* för sina arbets- och uppdragstagare från identitetsutfärdare som är anslutna till Svensk e-legitimation.

1.23 Svensk e-legitimation och tillhörande identitetsintyg ska utfärdas i enlighet med kraven för tillitsnivå 3 eller högre i tillitsramverket [baserat på Kantara IAF, blivande ISO 29115], *bilaga 9*.

1.24 E-tjänsteleverantören bestämmer vilken tillitsnivå för identifiering, vilket slag av elektronisk underskrift och vilka attribut som ska krävas av användare och dem som användare företräder.

Användning av e-legitimationer m.m.

1.25 En Svensk e-legitimation används vanligtvis på följande sätt mellan enskilda och e-tjänsteleverantörer.

a) *Privat e-legitimation* används av fysiska personer när de kommunicerar för egen räkning.

b) *E-tjänstelegitimation* används av fysiska personer när de kommunicerar i egenskap av anställda eller uppdragstagare.

En användare kan emellertid bruka en privat e-legitimation även i egenskap av företrädare för annan och den som har tilldelats en e-tjänstelegitimation får, om arbets- eller uppdragsgivaren godtar det, bruka e-tjänstelegitimationen också för egen räkning.

1.26 *En användare* som tilldelats en privat e-legitimation eller en e-tjänstelegitimation brukar den för

1) *legitimering* vid

a) *tillträde*, för att elektroniskt få tillgång till uppgifter som får lämnas ut till honom eller henne och för att få skydd

mot att obehöriga får tillgång till uppgifterna under sken av att vara honom eller henne,

b) *uppgiftslämnande*, för att få lämna uppgifter elektroniskt och för att få skydd mot att obehöriga lämnar uppgifter under sken av att vara honom eller henne,

2) *elektronisk underskrift*, för att ställa ut elektroniska handlingar som är skyddade mot förfalskning och förnekande av elektronisk underskrift på liknande sätt som en handling som är undertecknad på traditionellt sätt.

1.27 Genom en *anvisningstjänst* stöds funktioner för att användare ska kunna välja en e-legitimation som har en säkerhetsnivå eller andra egenskaper som är förenliga med de krav som gäller för e-tjänsten.

1.28 En myndighet använder identitetsintyg för att kontrollera

1) *legitimering*,

a) vid *tillträde*, för att kunna ge tillgång till uppgifter elektroniskt så att inte obehöriga får ut uppgifterna,

b) vid *uppgiftslämnande*, för att kontrollera vem som är ansluten när vissa uppgifter lämnas, och

2) *elektronisk underskrift*, för att granska om en handling som har undertecknats elektroniskt är utställd av den som anges som undertecknare.

1.29 En myndighet använder ett attributsintyg för att kontrollera om en person har juridisk behörighet att agera för annans räkning, viss befattning eller annan roll eller egenskap eller på annat sätt är förknippad med något som en attributsutfärdare kan intyga.

4. Regelverkets delar

1.30 Infrastrukturen för Svensk e-legitimation regleras genom detta regelverk, när föreskrifter inte ges i lag eller författning, och i följande avtal.

Avtal efter upphandling av teknisk drift

1.31 E-legitimationsnämnden tecknar *leveransavtal* med den som enligt upphandling rörande Infrastrukturen för Svensk e-legitimation ska sköta teknisk drift av

a) utfärdarregister och e-tjänsteregister,

b) anvisningstjänst, och

c) signeringstjänst.

Avtal efter upphandling av valfrihetssystem

1.32 E-legitimationsnämnden tecknar efter upphandling av valfrihetssystem för Infrastrukturen för Svensk e-legitimation avtal med de

a) identitetsutfärdare som uppfyller de krav som ställs upp inom valfrihetssystemet, och

b) myndigheter som ansluter sig som e-tjänsteleverantörer och uppfyller föreskrivna krav.

c) Dessa avtal ska innehålla de ramar som anges i *bilaga 4 och 5*.

Avtal om e-legitimationer för fysiska personer

1.33 En fysisk person som ansöker om en e-legitimation för att identifiera sig eller skriva under elektroniskt ska sluta avtal med utfärdaren av e-legitimationen.

1.34 Juridiska personer som ansöker om e-tjänstelegitimationer för anställda eller uppdragstagare ska sluta avtal med en utfärdare som är ansluten till Svensk e-legitimation.

5. Anslutning

Anslutning av identitetsutfärdare till Infrastrukturen för identifiering

1.35 Anslutning av identitetsutfärdare till Infrastrukturen för identifiering sker efter *ansökan* hos E-legitimationsnämnden genom att nämnden *tecknar avtal* med utfärdaren.

1.36 Den som uppfyller kraven i ett förfrågningsunderlag enligt lagen (2011:000) om valfrihet för Svensk e-legitimation och godtar de juridiska, tekniska och administrativa villkoren ska ha rätt att bli ansluten till Infrastrukturen för identifiering.

Anslutning av attributsutfärdare till Infrastrukturen för identifiering

1.37 Anslutning av attributsutfärdare till Infrastrukturen för identifiering sker genom

a) *beslut* av E-legitimationsnämnden, efter ansökan av *en myndighet under regeringen*, och

b) *avtal*, efter ansökan av *annan* än myndighet under regeringen.

1.38 En attributsutfärdare får anslutas till Infrastrukturen för identifiering om utfärdaren

a) enligt lag eller författning ska registrera och tillhandahålla de uppgifter som avses lämnas i attributsintygen och uppgifterna är av generell betydelse från kontrollsynpunkt, eller

b) det finns särskilda skäl från kontrollsynpunkt att ett visst slag av attribut från en viss utfärdare ska kunna lämnas inom Infrastrukturen för identifiering.

1.39 Särskilda skäl från kontrollsynpunkt föreligger om det finns ett utbrett behov inom offentlig förvaltning av tillförlitlig åtkomst till uppgiften och den inte finns tillgänglig på fungerande sätt i annan ordning.

1.40 E-legitimationsnämnden får i ett beslut om anslutning som villkor föreskriva att attributsutfärdaren ska följa de juridiska, tekniska och administrativa villkor som nämnden bestämmer.

1.41 E-legitimationsnämnden får ingå avtal om anslutning av en attributsutfärdare endast om utfärdaren accepterar de juridiska, tekniska och administrativa villkoren för anslutning till Infrastrukturen för identifiering.

Anslutning av e-tjänsteleverantörer till Infrastrukturen för identifiering

1.42 Anslutning av e-tjänsteleverantörer till Infrastrukturen för identifiering sker genom

a) beslut av E-legitimationsnämnden, efter ansökan av *en myndighet under regeringen*, och

b) avtal, efter ansökan av *annan* än myndighet under regeringen.

1.43 E-legitimationsnämnden får i ett beslut om anslutning som villkor föreskriva att e-tjänsteleverantören ska följa de juridiska, tekniska och administrativa villkor som nämnden bestämmer.

1.44 E-legitimationsnämnden får ingå avtal om anslutning av en e-tjänsteleverantör endast om utfärdaren accepterar de juridiska, tekniska och administrativa villkoren för anslutning till Infrastrukturen för identifiering.

E-legitimationsnämnden agerar som mellanman vid anslutning till Infrastrukturen för identifiering

1.45 Vid anslutning genom avtal till Infrastrukturen för identifiering beslutar E-legitimationsnämnden om tilldelning av ramavtal och tecknar upphandlingskontrakt för e-tjänsteleverantörernas räkning så att ett kontraktsförhållande uppkommer mellan e-tjänsteleverantören och

varje identitetsutfärdare och attributsutfärdare som genom avtal ansluts till Infrastrukturen för identifiering; jfr 3 § lagen (2011:000) om valfrihet för Svensk e-legitimation.

1.46 Vid anslutning genom beslut av E-legitimationsnämnden gäller de villkor som följer av E-legitimationsnämndens beslut.

Anslutning av e-tjänsteleverantörer till signaturtjänsten

1.47 Anslutning av e-tjänsteleverantörer till signaturtjänsten sker genom

a) beslut av E-legitimationsnämnden, efter ansökan av *en myndighet under regeringen*, och

b) avtal, efter ansökan av *annan* än myndighet under regeringen.

1.48 E-legitimationsnämnden får i ett beslut om anslutning som villkor föreskriva att e-tjänsteleverantören ska följa de juridiska, tekniska och administrativa villkor som nämnden bestämmer.

1.49 E-legitimationsnämnden får ingå avtal om anslutning av en e-tjänsteleverantör endast om utfärdaren accepterar de juridiska, tekniska och administrativa villkoren för anslutning till signaturtjänsten.

Aktivering efter beslut eller avtal om anslutning

1.50 Identitetsutfärdares, attributsutfärdares och e-tjänsteleverantörers anslutningar och funktioner, som samverkar med Infrastrukturen för Svensk e-legitimation, får inte aktiveras förrän de testats och E-legitimationsnämnden funnit att de fungerar på ett tillförlitligt sätt.

6. Utfärdande, m.m.

Tillförlitliga regler och rutiner

1.51 Utfärdare av Svensk e-legitimation, identitetsutfärdare och attributsutfärdare ska tillämpa sådana regler och rutiner att det – utifrån tillämplig tillitsnivå – finns fog för att lita på de e-legitimationer, identitetsintyg och attributsintyg som tillhandahålls. Dessa rutiner regleras från tekniska, administrativa och operativa utgångspunkter i tillitsramverket (bilaga 9).

Svensk e-legitimation

Ansökan, m.m.

1.52 Identitetsutfärdare som är anslutna till Infrastrukturen för Svensk e-legitimation ska utfärda e-legitimation till den som ansöker i enlighet med detta regelverk. [Identitetsutfärdare får dock uppställa särskilda villkor för utfärdande om villkoren är icke-diskriminerande och rör ett berättigat intresse hos identitetsutfärdaren.] Svensk e-legitimation får utfärdas endast efter skriftlig ansökan i traditionell form. Ansökan ska vara undertecknad på traditionellt sätt, med intyg om att lämnade uppgifter är riktiga och fullständiga.

1.53 Om en sökande har legitimerat sig eller skrivit under enligt det förenklade förfarande som anges i 1.60 får en sådan underskrift eller legitimering för uppgiftslämnande ersätta ett förfarande enligt 1.52.

1.54 Vid ansökan om en e-legitimation enligt en lägre tillitsnivå än nivå tre får den sökande identifieras enligt de förenklade förfaranden som anges.

1.55 En ansökan om Svensk e-legitimation ska innehålla de uppgifter som är nödvändiga för att identitetsutfärdaren ska kunna tillhandahålla sådan legitimation och utfärda identitetsintyg.

1.56 Utfärdaren ska i avtal med den som ansöker om Svensk e-

legitimation som villkor föreskriva att användaren ska skydda sin e-legitimation och sin personliga kod enligt 1.93 och när det är tillämpligt välja programvara och utrustning enligt vad som anges i 1.92.

Information om villkor

1.57 Utfärdaren ska informera den som ansöker om Svensk e-legitimation om avtalsvillkorens innehåll. En utfärdare som vill införa villkor som inte finns med i ansökningshandlingen ska tydligt hänvisa till villkoren och utforma rutinerna så att villkoren kommer sökanden tillhanda innan denne undertecknar eller annars ingår avtal med utfärdaren.

1.58 Utfärdaren ska tillhandahålla uppgifter om avtal, villkor, policies, utfärdardeklarationer, regelverk och anknytande uppgifter till anslutna användare, arbets- och uppdragsgivare, e-tjänsteleverantörer och andra som behöver uppgifter i samband med kontroller av legitimeringar eller handlingars äkthet.

Kontroll av sökandens identitet

1.59 Utfärdare av Svensk e-legitimation ska kontrollera den sökandes identitet vid ett personligt besök, på likvärdigt sätt som vid en ansökan om en traditionell identitetshandling.

1.60 Om en sökande redan har identifierats vid ett personligt besök för att få använda bank på Internet eller någon liknande tjänst för ekonomiskt eller rättsligt betydelsefulla mellanhavanden får utfärdaren identifiera den sökande genom denna tjänst i stället för enligt 1.59. En sådan förenklad rutin får dock inte användas om den har spärrats eller om det annars kan antas att den inte fungerar på ett tillförlitligt sätt.

Kontroll av uppgifter och utlämnande av Svensk e-legitimation

1.61 En utfärdare av en e-legitimation ska

1) kontrollera att ansökan om e-legitimation är behörigen undertecknad på papper eller lämnad elektroniskt enligt 1.53 – eller enligt 1.54 om det är förenligt med den aktuella tillitsnivån – och att de uppgifter som den sökande lämnar enligt är fullständiga och stämmer överens med uppgifter som finns registrerade i ett officiellt register, och

2) *tillhandahålla* e-legitimationer på ett säkert sätt.

1.62 Om en utfärdare tillhandahåller en e-legitimation, som användaren ska inneha och en personlig kod som användaren ska bruka för att aktivera legitimationen, ska dessa befordras

1) i separata försändelser och lämnas ut till sökanden vid personligt besök hos utfärdaren eller ett ombud för utfärdaren, eller

2) genom ett elektroniskt förfarande som är förenligt med 6.3 eller 6.4 om detta kan förenas med den tillämpliga tillitsnivån.

Spärrtjänst och spärrkontrolltjänst

1.63 Utfärdare av Svensk e-legitimation ska tillhandahålla en tjänst där användaren kan spärra sin e-legitimation (spärrtjänst). Tjänsten ska ha god tillgänglighet och utfärdaren ska behandla anmälan om spärr skyndsamt.

En myndighet som tillhandahåller en e-tjänst ska också kunna anmäla spärr av en e-legitimation. Identitetsutfärdaren ska spärra e-legitimationen efter en bedömning utifrån angivna skäl [och enligt vissa regler].

Särskilda regler för e-tjänstelegitimationer

1.64 Bestämmelserna om personliga e-legitimationer gäller i tillämpliga delar även för e-tjänstelegitimationer.

1.65 Identitetsutfärdare som är anslutna till Infrastrukturen för Svensk e-legitimation för att utfärda e-tjänstelegitimationer ska utfärda sådan legitimation till den som ansöker i enlighet med detta regelverk. [Identitetsutfärdare får dock uppställa särskilda villkor för utfärdande om villkoren är icke-diskriminerande och rör ett berättigat intresse hos identitetsutfärdaren.]

1.66 En e-tjänstelegitimation får utfärdas endast efter skriftlig ansökan i traditionell form av en arbets- eller uppdragsgivare. Ansökan ska vara undertecknad på traditionellt sätt av arbets- eller uppdragsgivaren. Om denne är en juridisk person ska ansökan vara undertecknad av en behörig företrädare. Utfärdaren ska kontrollera att uppgifterna om behörighet är riktiga.

1.67 Om en arbets- eller uppdragsgivare eller en behörig företrädare för denne har legitimerat sig eller skrivit under enligt förenklade förfarande som anges i 1.60 får en sådan underskrift eller legitimering för uppgiftslämnande ersätta ett förfarande enligt 1.52.

1.68 Den arbets- eller uppdragsgivare som ansöker om en e-tjänstelegitimation

a) bestämmer hur e-tjänstelegitimationen får användas, t.ex. om den får användas även utanför tjänsten, och

b) får spärra e-legitimationen.

1.69 [Närmare regler om uppgiftslämnande vid ansökan och utlämnande, RA-funktion]

1.70 Utfärdaren får lämna ut en e-tjänstelegitimation endast till

a) den som har legitimerat sig med en godkänd legitimationshandling eller på motsvarande sätt [enligt närmare regler på lägre nivå] och visat att han eller hon är behörig att företräda arbets- eller uppdragsgivaren, eller

b) den användare för vilken e-tjänstelegitimationen utfärdats, om arbets- eller uppdragsgivaren skriftligen har godkänt att den lämnas ut direkt till amvändaren.

Vid utelämnandet får förenklade rutiner enligt 1.67 användas.

Identitets- och attributsintyg

1.71 Den som utfärdar identitets- eller attributsintyg inom Infrastrukturen för identifiering ska innan ett intyg lämnas ha utfört kontroller i enlighet med kraven för den aktuella tillitsnivån, vilka anges i tillitsramverket (bilaga 9).

1.72 Utfärdare och e-tjänsteleverantörer ska kontrollera varandras identitet och skydda sin kommunikation mot manipulationer och förfalskningar genom den hantering av certifikat och elektroniska stämplar som ingår i de tekniska och administrativa funktioner som utgör en del av de standardiserade rutinerna inom Infrastrukturen för identifiering.

Utfärdares ansvar

1.73 En utfärdare av Svensk e-legitimation ansvarar gentemot innehavare av Svensk e-legitimation regleras beträffande privat e-legitimation i avtal med användare och för e-tjänstelegitimationer i avtal med arbets- och uppdragsgivare.

1.74 En identitetsutfärdares ansvar gentemot en e-tjänsteleverantör för uppgifter i identitetsintygen regleras i avtal som E-tjänsteleverantören i egenskap av mellanman sluter mellan identitetsutfärdare och e-tjänsteleverantören vid anslutning enligt avsnitt 4 ovan till Infrastrukturen för identifiering.

1.75 Eftersom myndigheter under regeringen utgör samma juridiska person och sådana myndigheter ansluts genom beslut av E-legitimationsnämnden ingås sådant avtal mellan staten och respektive utfärdare av identitetsintyg genom att [ ].

1.76 Attributsutfärdares ansvar för utfärdade intyg följer allmänna regler eftersom Infrastrukturen för Svensk e-legitimation endast tillhandahåller funktioner för att förmedla sådana intyg med stöd av de register och transportmekanismer som hör till Infrastrukturen för identifiering.

1.77 [Genom denna reglering kan rättsliga skillnader när användare betalar för legitimationen – öppet system – respektive e-tjänsteleverantören betalar för förlitandet – slutet system – hanteras].

Utformning av tekniska hjälpmedel

1.78 Om identitetsutfärdaren förser användaren med tekniska hjälpmedel för att hantera e-legitimationen på ett tillförlitligt sätt ska sådana hjälpmedel utformas så att det krävs en aktiv handling för att legitimera sig eller skriva under. Rutinerna bör ta sikte på att likna de omständigheter som användaren ställs inför när han eller hon

1) visar upp en traditionell legitimationshandling för identitetskontroll, eller

2) fattar en penna och skriver under.

1.79 Tekniska hjälpmedel eller tjänster för att granska utkast inför underskrift eller att presentera underskrivna eller stämplade handlingar ska utformas så att de möjliggör

1) en tydlig och begriplig presentation av uppgifterna, och

2) att läsaren av utkast eller färdiga handlingar

b) tydligt kan se all text och om texten är undertecknad respektive stämplad, samt

c) inte ges skäl att förväxla

i. den text som granskas, för att undertecknas eller stämplas, med annan text,

ii. den underskrivna eller stämplade texten med oskyddad text eller med text som hör till andra dokument, eller

iii. elektroniskt bestyrkta handlingar med andra handlingar.

Motsvarande krav gäller för hjälpmedel eller tjänster som identitets- och attribututfärdare tillhandahåller för att presentera identitets- och attributsintyg.

1.80 Om ett tekniskt hjälpmedel för granskning av handlingar stöder hantering av olika versioner eller liknande får underskrifter och stämplar inte presenteras så att det finns risk för att läsaren missförstår vad som har undertecknats eller stämplats.

Bevarande av handlingar

1.81 Utfärdare av Svensk e-legitimation ska bevara

1) ansökningshandlingar och handlingar som rör utlämnande, mottagande eller spärr av e-legitimationer.
2) avtal, policydokument och utfärdardeklarationer, och
3) övriga handlingar och uppgifter som kan behövas för att kontrollera legitimering och elektroniska underskrifter, identifiera personer och hantera insynsskydd.

1.82 Handlingarna ska bevaras och skyddas under den tid som behövs för att tillgodose ändamålen med elektroniska underskrifter m.m. Tiden för bevarande ska inte understiga tio år och material ska kunna tas fram i läsbar form under hela denna tid. Myndigheter och andra organ för vilka arkivlagen (1990:782) gäller får gallra allmänna handlingar endast om åtgärden har stöd i lag eller annan författning eller beslut om gallring.

1.83 Identitetsutfärdare ska lämna ut information om enskilda händelser på begäran av den som behöver kontrollera en legitimering eller en underskrift. Arkiverat material får emellertid inte lämnas ut i strid mot lag eller författning eller avtal med innehavaren av e-legitimationen.

1.84 En utfärdare av Svensk e-legitimation som upphör med

sin verksamhet ska informera sina användare och berörda e-tjänsteleverantörer. Utfärdaren ska hålla arkiverat material tillgängligt.

1.85 E-legitimationsnämnden ska [på motsvarande sätt under den tid som behövs bevara handlingar av betydelse för kontroller av identitet, handlingars äkthet eller annat av betydelse inom Infrastrukturen för Svensk e-legitimation].

7. Regler för användare, m.m.

Användare av Svensk e-legitimationer som sökande och innehavare

Ansökan och avtalsvillkor

1.86 Användare ska ansöka om e-legitimation hos en utfärdare av Svensk e-legitimation och lämna de uppgifter som är nödvändiga. Användaren ska underteckna ansökan i traditionell pappersbaserad form och intyga att lämnade uppgifter är riktiga och fullständiga.

1.87 Om en sökande redan har identifierats vid ett personligt besök för att få använda bank på Internet eller någon liknande tjänst för ekonomiskt eller rättsligt betydelsefulla mellanhavanden får han eller hon använda elektroniska rutiner enligt 1.60.

1.88 Innan ansökan sker ska den sökande ha beretts tillfälle att ta del av och spara utfärdarens villkor och information enligt 1.57 samt tydligt ange om han eller hon till någon del inte godtar villkoren. En innehavares ansvar mot utfärdaren och mot förlitande parter vid fel eller försummelse bör regleras i villkoren.

Identifiering

1.89 En användare som ansöker om e-legitimation ska vidta de åtgärder som behövs för att utfärdaren ska kunna

identifiera den sökande enligt 1.59 och 1.60.

Mottagande och användning av e-legitimation

1.90 Användaren ska behandla sin e-legitimation och sin personliga kod på ett tillförlitligt sätt enligt villkoren i användarens avtal med utfärdaren.

1.91 En användare som väljer sin personliga kod får inte använda en sådan som är enkel att lista ut.

1.92 En användare ska bruka de tekniska hjälpmedel som identitetsutfärdaren tillhandahåller enligt 1.78 – 1.80 så att legitimering och elektronisk underskrift sker med tillförlitliga rutiner.

Skydd för e-legitimationer och personliga koder m.m.

1.93 Användaren ska skydda sin e-legitimation så att ingen annan får tillgång till den och sin personliga kod så att ingen annan kan få reda på den. Dessa åtgärder består bl.a. i att

1) skydda datorer och annan utrustning där e-legitimationen förvaras eller används,

2) välja en personlig kod som inte är lätt att lista ut, och

3) hålla den personliga koden hemlig och inte anteckna koden på ett sätt eller på en plats som gör att den kan kopplas till e-legitimationen.

Anmälan om spärr

1.94 En användare av en e-legitimation ska göra en spärranmälan snarast efter att denne upptäckt att det finns anledning att spärra e-legitimationen.

Användare av e-tjänstelegitimation som innehavare

1.95 En användare av en e-tjänstelegitimation får använda den endast i enlighet med instruktioner från arbets- eller uppdragsgivaren.

Arbets- eller uppdragsgivare som sökande m.m.

1.96 En arbets- eller uppdragsgivare som anskaffar e-tjänstelegitimationer bestämmer inom ramen för sin arbetsledningsrätt hur e-tjänstelegitimationen får brukas av användaren.

1.97 En arbets- eller uppdragstagare ska göra en spärranmälan snarast efter att denne upptäckt att det finns anledning att spärra en e-tjänstelegitimation som denne tilldelat en arbets- eller uppdragstagare. Anledning att spärra kan föreligga bl.a. om arbets- eller uppdragsförhållandet upphört eller en personlig kod kan ha blivit tillgänglig för någon annan.

8. Regler för e-tjänsteleverantörer

E-tjänsteleverantörernas kontroller

1.98 E-tjänsteleverantören hanterar frågor om identitet och attribut med stöd av uppgifter i intyg utfärdade av identitets- och attributsutfärdare som är anslutna till Infrastrukturen för Svensk e-legitimation.

1.99 E-tjänsteleverantörer som är anslutna till Infrastrukturen för Svensk e-legitimation bör normalt godta identitets- och attributsintyg från anslutna utfärdare, om det inte finns skäl för en annan bedömning i ett ärende. E-tjänsteleverantören bedömer vilken tillitsnivå som krävs.

1.100 Om det i det enskilda fallet finns skäl att kontrollera den autentisering som identitetsutfärdaren utfört får myndigheten begära ytterligare uppgifter från identitetsutfärdaren eller begära att användaren ska bekräfta uppgiften om identitet eller den elektroniskt underskrivna handlingen.

Av 10 § tredje stycket förvaltningslagen (1986:223), 44 § tredje stycket förvaltningsprocesslagen (1971:291) och 33 kap. 3 § tredje stycket rättegångsbalken följer att behöriga handläggare från fall till fall får avgöra om en elektroniskt undertecknad eller stämplad handling ska godtas eller om en bekräftelse ska inhämtas.

1.101 Kontroller som e-tjänsteleverantören inte utför automatiserat ska utföras av behöriga handläggare hos e-tjänsteleverantören.

Interna regler för e-tjänsteleverantören

1.102 En e-tjänsteleverantör som är ansluten till Infrastrukturen för Svensk e-legitimation bör ha interna regler om hur identifiering, äkthetskontroll och kontroll av attribut utförs.

Underskrifter och stämplar

1.103 En elektronisk underskrift ska presenteras i anknytning till den text som skrivs under, så att underskriftens innebörd framgår av sammanhanget, på samma sätt som vid underskrift på traditionellt sätt. Behövs skriftlig information om denna innebörd, t.ex. en angivelse av en fullständig firma vid firmateckning enligt 26 § firmalagen (1974:156), bör detta anges i den text som undertecknas.

1.104 Presenteras flera underskrifter på samma sida eller presenteras en underskrift så att det finns risk för att läsaren missförstår vilken text som undertecknats bör åtgärder vidtas för att förenkla och förtydliga läsarens tolkning av det som presenteras. Detsamma gäller om både skyddad och oskyddad text presenteras tillsammans.

Rutiner för att ta emot, expediera, presentera, hantera och långtidslagra elektroniska handlingar

1.105 En myndighet som tar emot eller ställer ut undertecknade elektroniska handlingar ska säkerställa att de krav som de kryptografiska rutinerna för med sig beaktas från arkivsynpunkt. I Riksarkivets föreskrifter finns bestämmelser om framställning, hantering, förvaring och skydd av allmänna handlingar.

1.106 Myndigheter bör tydligt anvisa de mottagningsställen där myndigheten tar emot elektroniska handlingar. [Detta behövs dock inte inom ramen för t.ex. webbformulär och webbtjänster där adresseringen till mottagande myndighet sker automatiskt.]

1.107 Kvittenser bör utfärdas. Kvittenser och andra bekräftelser från myndigheter bör utformas så att det inte finns risk för att mottagaren vilseleds om vad som har undertecknats eller stämplats.

9. Persondataskydd

1.108 Utfärdare av Svensk e-legitimation, identitets- och attributsutfärdare och e-tjänsteleverantörer får inom Infrastrukturen för Svensk e-legitimation inhämta personuppgifter endast direkt från den som uppgifterna avser eller med dennes uttryckliga samtycke och endast i den utsträckning som det är nödvändigt för att utfärda eller upprätthålla funktioner för e-legitimationer och identitets- och attributsintyg. Uppgifterna får inte samlas in eller behandlas för andra ändamål utan uttryckligt samtycke från den som uppgifterna avser.

10. Bevarande, säkerhet och tillsyn

1.109 E-tjänsteleverantörer, identitets- och attributsutfärdare ska tillämpa ett ledningssystem för informationssäkerhet. Detta innefattar bl.a. att

1) upprätta en informationssäkerhetspolicy och andra styrande dokument som behövs för informationssäkerheten,

2) utse en eller flera personer som leder och samordnar arbetet med informationssäkerhet,

3) klassificera sin information med utgångspunkt i krav på sekretess, riktighet, tillgänglighet och spårbarhet,

4) utifrån risk- och sårbarhetsanalyser och inträffade incidenter avgöra hur risker ska hanteras, samt besluta om åtgärder för aktörens informationssäkerhet,

5) dokumentera vidtagna granskningar och säkerhetsåtgärder av större betydelse.

1.110 Ledningen inom en e-tjänsteleverantör, identitets- eller attributsutfärdare ska löpande informera sig om arbetet med informationssäkerhet samt minst en gång per år följa upp och utvärdera detta arbete.

1.111 E-tjänsteleverantör och identitets- och attributsutfärdare ska bedriva sitt arbete enligt 1.109 och 1.110 i former enligt följande etablerade svenska standarder för informationssäkerhet;

1) Ledningssystem för informationssäkerhet – Krav (SS-ISO/IEC 27001: 2006 fastställd 2006-01-19), och

2) Riktlinjer för styrning av informationssäkerhet (SS-ISO/IEC 27002:2005 fastställd 2005-08-12).

1.112 Revision och rapporteringsskyldighet[1].

[1] Utredningen arbetar vidare med att ta fram ett förslag till slutrapporten.

Förslag till riktlinjer för federationsoperatörer

1 Tillämplighet

Dessa förslag till riktlinjer för federationsoperatörer är tillämpliga för aktörer som avser tillhandahålla en identitetsfederation under E-legitimationsnämndens regelverk för identitetsfederationer inom ramen för Infrastrukturen för Svensk e-legitimation.

2 Inledning

En identitetsfederation består av ett antal leverantörer av identitetstjänster (identitetsutfärdare) och förlitande parter (e-tjänsteleverantörer) som samverkar inom ramen för vissa regler, standarder och tekniska lösningar så att identitetsutfärdare kan tillhandahålla trovärdig identitetsinformation till förlitande parter.

Medan en identitetsfederation med några få aktörer kan bygga på att alla deltagare ingår avtal med alla andra som deltar, måste en stor identitetsfederation styras av en federationsoperatör som kan samordna viktiga standarder, tillhandahålla grundläggande tjänster till alla deltagare i federationen och sluta avtal så att avtalsfloran begränsas.

I detta dokument ges förslag till riktlinjer för en federationsoperatör som ska svara för en identitetsfederation för e-legitimationer i Sverige. Begreppet e-legitimation används här som en samlingsbeteckning certifikat, säkerhetsdosor eller andra sådana identifieringslösningar som uppfyller kraven för anslutning till den svenska modellen för legitimering och underskrift i elektronisk miljö.

Federationsoperatören upprätthåller ett ramverk för tillit som deltagarna i federationen är beroende av och ska

- bestämma regler och tekniska standarder för den som är ansluten till federationen, bl.a. för hur

  - e-legitimationer utfärdas och hanteras;
  - användares personliga integritet ska skyddas,
- tillhandahålla regler för certifiering av deltagare i federationen, och
- samla in och tillhandahålla uppgifter som beskriver deltagares tjänster och tillhandahålla information och nycklar för säkert informationsutbyte och identifiering av federationens medlemmar (s.k. metadata).

Utöver dessa grundläggande uppgifter för att skapa tillit till federationen ska federationsoperatören

- tillhandahålla stöd för att lösa frågor när aktörerna inte är eniga (tvistlösning) och att testa överensstämmelse med tekniska normer och förmågan att samverka (s.k. interoperabilitet),
- upphandla och sluta avtal om vissa tjänster som ska vara tillgängliga för anslutna till Svensk e-legitimation.

För att federationsoperatören ska kunna utföra alla dessa uppgifter på ett effektivt sätt måste denna ha resurser, personal och förmåga att ingå de avtal och bestämma de regler för identitetsfederationen som faller inom ramen för federationsoperatörens kompetens.

3 Dokumentation och processer

Identitetsfederationen ska drivas i enlighet med bestämda regler och standarder för anslutning och användning. Hit hör bl.a.

- ett regelverk för identitetsfederationen som ska
  - definiera klasser av anslutna till federationen, såsom identitetsutfärdare, e-tjänsteleverantörer och vissa attributsutfärdare,
  - ange operativa rättigheter och skyldigheter för anslutna,
  - reglera deltagande i och ansvar för federationen,
  - bestämma en process för hur säkerhetsincidenter ska hanteras inom federationen,
- dokument som anger krav eller ger vägledning för anslutna till federationen beträffande de tekniska lösningar och de förfaranden och processer som anslutna ska använda för att delta i federationen; bl.a.

- ett tillitsramverk som anger
  - processer för att kontrollera användares identitet;
  - metoder och faser genom olika stadier av e-legitimationers livscykel för förvaring och skydd av dem,
- en tvistlösningsmekanism för anslutna till federationen,
- krav på informationssäkerhet i anslutna e-tjänste-leverantörers tjänster och skydd för personuppgifter och sekretess,
- tekniska specifikationer av
  - protokoll som ska stödjas vid informationsutbyte inom federationen,
  - attribut som kan ingå i identitets- eller attributsintyg;
  - metadata och åtkomst till sådana,
  - anvisningstjänster för att finna tjänster inom federationen,
- regler och förfaranden för att kontrollera att den som är ansluten till federationen följer de regler, processer och specifikationer som gäller för anslutna,
- avtal för anslutna till Svensk e-legitimation

4 Ansökan om deltagande

Federationsoperatören ska verka inom ramen för regler för att definiera och hantera ansökningar om deltagande i federationen.

5 Tillitsskapande åtgärder

5.1 Tillitsramverk och integritet

Ett grundläggande del i identitetsfederationen är att utarbeta regelverk och tekniska och operativa krav så att anslutna har förtroende för federationen. För identitetsutfärdare innefattar detta krav på identifiering av användare, utfärdande av e-legitimationer, e-legitimationers kvalitet och hantering samt säker lagring och kommunikation av identiteter och annan information. Detta arbete ska säkerställa en korrekt hantering av information och skydd för användares personliga integritet.

5.2 Samordning av regelverk och riktlinjer

Om en identitetsutfärdare som ska anslutas till identitetsfederationen redan har fastställda regler för identitetshantering, kan det dessa regler och hur de förhåller sig till reglerna för federationen kartläggas. Federationsoperatören ska i samverkan med identitetsutfärdaren svara för denna kartläggning.

5.3 Teknisk interoperabilitet och testning

Alla autentiseringsmekanismer och protokoll som används inom identitetsfederationen bör testas för att se till att de fungerar bland dem som är anslutna. Då protokoll som används för att förmedla information om identitet och tillitsnivå är avgörande för federationens funktion bör federationsoperatören definiera hur dessa protokoll ska testas för driftskompatibilitet, inklusive tester för e-tjänsters svar på felaktigt införande av protokoll hos identitetsutfärdare eller i attributstjänster. Även protokoll för distribution av metadata och respons vid felaktiga metadata bör testas.

6 Förhandlingar om avtal

Avtal om deltagande i identitetsfederationen ska ingås mellan federationsoperatören och de som ansluts. Dessa avtal ska vara likvärdiga för alla anslutna.

Behörighetshantering med stöd av attribut

1.1 Funktioner med olika användningsområden

Till den föreslagna Infrastrukturen för identifiering hör också hanteringen av attribut. Medan en beskrivning av Identitetsintyg och hur de används är relativt enkel att göra, i vart fall på ett övergripande plan, blir variationsmöjligheterna många så snart en samordnad infrastruktur för hantering av attribut ska övervägas för hela den offentliga sektorn. Även små myndigheter behöver smidigt kunna integrera, använda och administrera inte bara rena Identitetsintyg utan även intyg med attribut. Härvid uppkommer emellertid en spännvidd i juridiska och tekniska krav som saknar motsvarighet på området för identifiering och som inte kunnat genomlysas i erforderlig omfattning inom ramen för utredningens begränsade uppdrag.

I det följande ska dessa varierande förutsättningar belysas med exempel från Bolagsverkets hantering av registerutdrag och hälso- och sjukvårdens behov av attribut.

1.2 Juridisk behörighet – en granskning i flera led

En juridisk person kan inte agera själv – det krävs att organ såsom styrelse, verkställande direktör, befullmäktigade ombud eller liknande utför rättshandlingar för den juridiska personens räkning. Korrekta bedömningar förutsätter en genomgång i flera led – en slags process – som är allmänt vedertagen i pappersmiljö. Den består normalt av följande led.

1. Vilken *fysisk person* har företagit rättshandlingen?	Här används underskrifter, legitimationshandlingar, m.m. för att knyta en fysisk person till rättshandlingen.
2. Har personen agerat för egen eller *för annans räkning*?	I vems namn har rättshandlingen företagits? Här används t.ex. firmateckning för att klargöra att åtgärden vidtagits i egenskap av företrädare för annan.
3. Är den som agerat som företrädare för annan *behörig* att företa rättshandlingen?	Här används registreringsbevis (utvisande t.ex. firmateckningsrätt), fullmakter o.l.

En fullständig granskning av ovan nämnda omständigheter i varje enskilt fall blir tungrodd. I traditionell miljö har därför *förenklade förfaranden* vuxit fram, t.ex. att för vissa mindre transaktioner

godta en persons uttryckliga eller underförstådda påstående om behörighet.

Med en e-legitimation kan endast första steget i processen kontrolleras; dvs. (1) vilken fysisk person som agerar. Av e-legitimationen framgår inte om innehavaren (2) avser att agera för egen eller för annans räkning eller (3) är behörig att företräda en uppgiven huvudman vid rättshandlingar. Det är vanligt att tvister uppstår beträffande frågan om en viss rättshandling har företagits för *egen* räkning (t.ex. när ett bolag, som alternativt skulle kunna ses som huvudman, har försatts i konkurs) eller som *företrädare* för ett företag (vilket till skillnad från den fysiska personen har förmåga att betala).

1.3 Åtkomstkontroll och inre sekretess – gränsdragningar

Liknande frågor om roller och egenskaper uppkommer inom ett organ. Varje myndighet och varje företag av någon storlek styr numera åtkomsten till och rättigheter i egna informationssystem genom s.k. behörighetskontrollsystem (BKS). Föreskrifter om sådana begränsningar – i vissa sammanhang kallad inre sekretess – finns i patientdatalagen (2008:355; PDL), för vårdgivare. Här är det avgörande om en person är t.ex. läkare eller sjuksköterska och om personen deltar i vården av en viss patient eller av annat skäl behöver uppgifter om patienten för sitt arbete inom hälso- och sjukvården.[1] Begreppet ”behörighet” används emellertid även i det sammanhanget och enligt 4 kap. 2 § PDL ska en vårdgivare bestämma villkor för tilldelning av behörighet för åtkomst till sådana uppgifter om patienter som förs helt eller delvis automatiserat. Härvid föreskrivs att behörigheten ska begränsas till vad som behövs för att den enskilde ska kunna fullgöra sina arbetsuppgifter inom hälso- och sjukvården.

När sådan åtkomstkontroll införs blir det alltså inte fråga om kontroll av om en person *i juridisk mening* är behörig att företrädare ett rättssubjekt (t.ex. ett annat aktiebolag eller en annan myndighet). Det blir istället fråga om att *begränsa åtkomsten* till uppgifter och resurser i informationssystem inom en och samma

[1] Enligt 4 kap. 1 § PDL får den som arbetar hos en vårdgivare ta del av dokumenterade uppgifter om en patient endast om han eller hon deltar i vården av patienten eller av annat skäl behöver uppgifterna för sitt arbete inom hälso- och sjukvården.

vårdgivare.[2] Samtidigt aktualiseras emellertid en slags behörighetskontroll, dels genom att ett landsting eller en kommun som bedriver hälso- och sjukvård genom *flera myndigheter* får ha direktåtkomst till personuppgifter som behandlas av någon annan sådan myndighet i *samma landsting* eller kommun (5 kap. 5 § PDL), dels genom att en vårdgivare under vissa förutsättningar får ha direktåtkomst till personuppgifter som behandlas av *andra vårdgivare* (6 kap. 1 § PDL). Här aktualiseras alltså två olika typer av ”direktåtkomst” – den ena inom en vårdgivare, den andra mellan vårdgivare. För den senare typen av direktåtkomst krävs enligt huvudregeln att patienten lämnat sitt samtycke, att uppgifterna rör en patient som det finns en aktuell patientrelation med och att åtkomsten kan antas ha betydelse för att förebygga, utreda eller behandla sjukdomar och skador hos patienten inom hälso- och sjukvården.

Skillnaden mellan dessa olika typer av kontroller är alltså betydande. Endast några få personer ges *juridisk behörighet* att företräda en juridisk person medan *åtkomstkontroller* införs för alla anställda och uppdragstagare som ska ges åtkomst till informationssystem. En annan skillnad är att juridisk behörighet vanligtvis bestäms *grovmaskigt*; jfr att styrelsen enligt 8 kap. 39 § aktiebolagslagen (2005:551; ABL) får föreskriva att rätten att företräda bolaget och teckna dess firma får utövas endast av två eller flera personer i förening medan *andra inskränkningar* i en firmatecknares rätt att teckna bolagets firma *inte får registreras*. Denna grova avgränsning bör ställas mot åtkomstkontroll till informationssystem där användarnas rätt till åtkomst vanligtvis ges en finmaskig utformning.

Till detta kommer regleringen i patientdatalagen som innehåller en blandning av krav på *åtkomstkontroll* inom respektive mellan myndigheter och andra organ och krav på en slags juridisk behörighetskontroll mellan olika organ. Det finns risk för att dessa variationer i reglering och i hantering av åtkomst- respektive *behörighetskontroller* missförstås när tekniska och administrativa lösningar ska utarbetas för bl.a. Identitets- och Attributsintyg.

System för *åtkomstkontroll* ger alltså – utanför hälso- och sjukvårdsområdet – endast ett inre skydd som, till skillnad från juridisk behörighetskontroll, inte visar om en person äger rätt att

[2] Här finns också föreskrifter om att patienter får motsätta sig att personal vid en annan vårdenhet eller inom en annan vårdprocess hos samma vårdgivare gör personuppgifter som dokumenterats för vårdändamål tillgängliga genom elektronisk åtkomst (4 kap. 4 § PDL).

företräda annan vid rättshandlingar. Attributsintyg bör primärt utformas med tanke på juridiska behörighetskontroller. Det finns emellertid inget hinder mot att dessa Identitets- och Attributsintyg – när det visar sig lämpligt – används även inom en och samma juridiska person, t.ex. en vårdgivare, för att styra anställdas och uppdragstagares åtkomst utifrån relevanta attribut. Dessa användningsområden får emellertid inte blandas samman.

Dessa grundläggande skillnader kan därmed beskrivas så att det

- vid *juridisk behörighetskontroll* ska granskas om en person har sådan rätt att agera (t.ex. är ställföreträdare eller fullmäktig för ett aktiebolag) att *den som företräds* (i detta exempel aktiebolaget) *blir juridiskt bunden*, t.ex. av avtal eller andra åtaganden, men
- vid *åtkomstkontroll* ska granskas om personen *har rätt att få tillgång* till uppgifter eller andra resurser i informationssystem, och
- *inom hälso- och sjukvården* utförs kombinationer av kontroller för vilka en omfattande särreglering införts.

Utvecklingen av en Infrastruktur för Svensk e-legitimation får inte blandas samman med det utvecklingsarbete som utförs i annan ordning, t.ex. inom hälso- och sjukvården för att uppfylla patientdatalagens krav. E-legitimationsnämnden bör visserligen skapa förutsättningar för att de lösningar för identifiering och behörighetskontroller, som redan införts inom t.ex. hälso- och sjukvården, ska kunna tas tillvara även inom en ny Infrastruktur för identifiering. Åtkomstkontroll får härvid inte blandas ihop med juridiska behörighetskontroller. De måste också hållas isär från särskilda kontroller som krävs för att uppfylla patientdatalagens krav.

1.4 Elektroniska registerutdrag

Juridiska behörighetskontroller bör inom Infrastrukturen för identifiering kunna hanteras så att en Användare först legitimerar sig med e-legitimation och att E-tjänsteleverantören – efter att ha granskat identitetsintyget – ställer en attributsintygsfråga till en utfärdare inom Infrastrukturen för identifiering. För att förenkla framställningen utgår vi i det följande från att det är ett aktiebolag

som den identifierade personen påstår sig företräda och att det är Bolagsverket som ska lämna ett utdrag ur aktiebolagsregistret.

Lösningen kan utformas så att *Bolagsverket ställer ut* Attributsintyg med registerutdrag, som skyddas mot förfalskningar och andra angrepp med stöd av de infrastrukturcertifikat som tillgängliggörs i utfärdar- och e-tjänsteregistren för var och en som är ansluten. *E-tjänsteleverantören kontrollerar*, i egenskap av förlitande part, dels att Attributsintyget är äkta, dels att uppgifterna visar att angiven person är behörig att företräda angivet aktiebolag. E-tjänsteleverantörer bör ges möjlighet att tolka behörighetsinformationen såväl automatiserat (i maskinläsbar form) som manuellt (i vanlig läsbar form på t.ex. bildskärm eller i form av en utskrift). Det är emellertid inte Bolagsverkets uppgift att tillhandahålla sådant stöd och behovet av stöd varierar från E-tjänsteleverantör till E-tjänsteleverantör.

En myndighet som behöver göra många kontroller av juridisk behörighet, t.ex. Skatteverket, bör införa en automatiserad funktion för juridisk behörighetskontroll med stöd av Attributsintyg. Ansvars- och riskfördelningen kan bli densamma som idag genom att Bolagsverket endast lämnar registerutdrag. E-tjänsteleverantören (förlitande part) får därefter bedöma om de uppgifter som lämnats i utdraget ger tillräckligt underlag för att Användaren ska anses behörig att logga in eller skriva under i egenskap av företrädare för aktiebolaget. På samma sätt som idag får alltså E-tjänsteleverantören bedöma t.ex. om e-tjänsten endast används för sådant som utgör löpande förvaltningsåtgärder enligt 8 kap. 36 § ABL, så att den verkställande direktören är behörig att agera för bolagets räkning även om denne inte har ensam firmateckningsrätt. Det bör vidare krävas att varje e-tjänst utformas så att Användaren otvetydigt måste ange om tillträde, uppgiftslämnande, underskrift eller andra åtgärder i en e-tjänst utförs för egen eller för annans räkning och vem det är som i så fall företräds.

En lösning för automatiserade kontroller bör förenas med anpassningar för mindre myndigheter, antingen så att intyg kan granskas och bedöms manuellt eller så att de ges ett förenklat innehåll, t.ex. att en kod lämnas utifrån en klassificering som Bolagsverket stöder så att maskinella kontroller kan förenklas. En viss siffra i ett fält kan t.ex. visa att en individ (angiven med personnummer) är behörig att ensam teckna bolagets (angivet med organisationsnummer) firma.

För att inte riskera att rubba dagens ansvarsfördelning mellan Bolagsverket och den som litar på ett registerutdrag (här E-tjänsteleverantören) skulle sådana koder kunna införas enligt specifikationer som tillkommer efter samråd med berörda aktörer och fastläggs av Bolagsverket, t.ex. i en myndighetsföreskrift för tjänsten, där det framgår vad koderna står för och samtidigt klargörs att förlitande part själv får bedöma vilken verkan dessa uppgifter kan anses ha vid en juridisk behörighetskontroll.

En sådan hantering bör kunna utformas så att den blir tekniskt enkel att införa och använda. Den torde inte heller förutsätta några ändringar i lag eller förordning eftersom den endast innebär att Bolagsverket lämnar utdrag ur sina register. Utmaningen blir istället att finna en samsyn kring detaljer så att lösningen kan införas på ett samordnat och enhetligt sätt.

1.5 Behovet av kontroll – olika nivåer

1.5.1 Riskfördelning enligt lag

Att en fysisk person i juridisk mening är behörig att företräda annan innebär som framgått att huvudmannen, t.ex. ett aktiebolag, blir direkt bunden av en rättshandling som företrädaren företar. Det vilar emellertid på förlitande part att kontrollera att behörighet verkligen föreligger. Förlitande part står normalt också risken om det godtas att en person är behörig men detta senare visar sig felaktigt. Här bör nämnas att det av regler i bl.a.

- skuldebrevslagen (SkbrL), framgår att motparten står risken om
  - uppgiven företrädare för en part
    - inte är den han eller hon ger sig ut för att vara (kan kontrolleras med e-legitimation), eller
    - *saknar behörighet* att företräda uppgiven huvudman (kan kontrolleras med registreringsbevis),
  - urkunder, t.ex. skriftliga avtal, registreringsbevis eller fullmakter är falska (kan kontrolleras med e-legitimation om de försetts med elektronisk underskrift),[3]

[3] Enligt 17 § skuldebrevslagen (SkbrL) får förfalskning och bristande behörighet åberopas även mot den som är i god tro och i detta hänseende ger SkbrL uttryck för en allmän förmögenhetsrättslig princip som tillämpas analogt även utanför skuldebrevsrätten. Visserligen avser denna bestämmelse löpande skuldebrev men i lagmotiven har det, med avseende på enkla skuldebrev, uttalats att en gäldenär som regel har att på egen risk pröva

- rättegångsbalken (RB), framgår att resning kan beviljas sedan dom i tvistemål eller brottmål vunnit laga kraft, om en falsk skriftlig handling har åberopats till bevis och handlingen kan antas ha inverkat på utgången och att detsamma torde gälla om talan förts för en juridisk persons räkning där dennes anspråk t.ex. eftergivits helt utan behörighet att agera för denne,[4]
- aktiebolagslagen och aktiebolagsförordningen, framgår att register ska föras av Bolagsverket, att verket ska lämna utdrag men att verkets ansvar i princip är begränsat till att lämnade utdrag som rätt återger innehållet i aktiebolagsregistret – den som mottar och brukar utdrag avgör för vilka kontroller utdragen ska användas, hur kontrollerna ska utföras och står risken om behörighet felaktigt antas föreligga.

Författningsregleringen innebär alltså något förenklat att det är E-tjänsteleverantören (förlitande part) som står risken om det finns brister i behörighetskontrollerna.

1.5.2 Ett balanserat risktagande

Vissa ärenden rör känsliga uppgifter eller stora värden. I sådana fall görs vanligtvis en *fullständig kontroll* av juridisk behörighet, där det på ett tillförlitligt sätt granskas både vem som agerat och om denne var behörig att företa rättshandlingen för angiven huvudmans räkning. I praktiken gör emellertid förlitande parter riskbedömningar utifrån vilka de utformar sina kontroller. Sådana bedömningar kan i många fall leda till att *ingen kontroll* görs av t.ex. registreringsbevis eller fullmakter. Förlitande part utgår från att den som utger sig för att vara behörig företrädare verkligen är det. Skulle påståendet om behörighet vara felaktigt kan den som utgett sig för att ha behörighet bli skadeståndsskyldig mot förlitande part.

Som exempel på uttalanden rörande behovet av balanserade riskbedömningar kan nämnas att justitierådet Henrik Hessler i en äldre monografi ”Obehöriga förfaranden med värdepapper” uttalat att praktiskt taget alla transaktioner enligt sakens natur innebär att aktörerna måste ta vissa risker för att allt inte har gått rätt till och att det knappast är möjligt att helt eliminera dessa risker; ”i allt fall

huruvida den med vilken han har att skaffa är rätt borgenär eller behörig att på dennes vägnar uppbära betalning.

[4] Se 58 kap. 1 och 2 §§ RB.

skulle rigorösa försök i denna riktning sannolikt resultera i att verksamheten blev orimligt tungrodd". Hessler tillade bl.a. följande, som torde anses vara en självklarhet i pappersmiljö:

> I åtskilliga situationer kan dock (banken) blott genom utvisande av skälig aktsamhet och sålunda utan någon krävande försiktighetsapparat skydda sig mot förlustrisk. Ett klarläggande så långt möjligt av i vilka lägen en sådan aktsamhet är på sin plats samt kanske fram för allt vad den bör gå ut på och hur långt den behöver sträckas torde därför vara av praktiskt värde till underlättande av verksamhetens bedrivande; det förekommer väl icke blott att erforderlig aktsamhet eftersätts utan ej sällan också att man i brist på säker kännedom om rättsläget drivs att iakttaga en större försiktighet än nöden i själva verket kräver, vilket blir en onödig belastning på rörelsen.

Detta uttalande passar väl in på dagens hantering av kontroller i elektronisk miljö. E-tjänsteleverantörerna, som ska ställa upp de krav som en e-tjänst ska uppfylla bl.a. beträffande kontroll av behörighet, tenderar att ställa synnerligen höga krav så snart IT-stöd införs. En orsak kan vara en sammanblandning av de behov som finns av juridisk prövning av bl.a. identitet och behörighet med behov från informationssäkerhetssynpunkt av att skydda E-tjänsteleverantörens IT-miljö.[5]

Myndigheter kan emellertid i många fall – i vart fall initialt – förväntas införa e-tjänster utifrån enklare lösningar med manuella inslag. Här bör resonemang från pappersmiljön ofta kunna återanvändas så att förenklingar anses möjliga. I många fall bör en identifiering med t.ex. e-legitimation kunna räcka, utifrån enkla, närmast självklara resonemang. Som exempel kan nämnas att ärenden där t.ex. telefaxmeddelanden eller kanske till och med uppgiftslämnande per telefon godtas utan några behörighetskontroller knappast kan anses kräva fullständiga behörighetskontroller bara för att hanteringen har överförts till elektronisk miljö.

Begränsningar av behörighetskontroller godtas också enligt lag. Varken i förvaltningslagen (1986:223) eller lagen (1996:242) om domstolsärenden föreskrivs att en myndighet som handlägger ett ärende måste begära in och granska registreringsbevis eller fullmakt för ett ombud.[6] Däremot *får* myndigheten begära in behörighetshandlingar om myndigheten finner skäl för en sådan kontroll.

[5] En del i detta kan antas vara att automatiseringen medför att det saknas motsvarighet till den sociala kontroll som finns i pappersmiljö, så att handläggare reagerar om något verkar misstänkt. Vidare tar sig informationssäkerhetsarbetet ofta sådana uttryck att det inte görs några jämförelser med motsvarande riskbedömningar i pappersmiljö.

[6] Motsatsen gäller emellertid i tvistemål och brottmål enligt rättegångsbalken.

Visserligen innebär det ett risktagande när en myndighet använder sig av möjligheten att begränsa behörighetskontrollerna. Det har emellertid i praktiken visat sig fungera i pappersmiljö. På motsvarande sätt godtar företag ofta beställningar av varor per telefon, telefax o.l. – utan någon identitets- eller behörighetskontroll. Samma synsätt bör kunna tillämpas för e-tjänster. Har Användaren identifierats med stöd av e-legitimation och detta kontrollerats med hjälp av Identitetsintyg torde dessa åtgärder ofta räcka. Här bör motsvarande praktiska synsätt kunna tillämpas som i traditionell miljö – med de anpassningar som behövs till särskilda risker som IT kan föra med sig.

I traditionell miljö är det som framgått vanligt att identitets- och behörighetskontroller inte görs. För dessa fall skulle ett förenklat förfarande för IT-miljö där identifiering sker med Identitetsintyg men registerutdrag från Bolagsverket inte krävs innebära en noggrannare kontroll än den som görs i traditionell miljö när underskrifter godtas utan kontroller. Därmed bör det i många fall – i kombination med det skadeståndsansvar som följer av felaktiga påståenden om behörighet – räcka att den som agerar identifieras med stöd av Identitetsintyg samt att e-tjänsten utformas så att det otvetydigt framgår

- om personen agerar för egen eller för annans räkning, och
- för vem ett agerande för annans räkning sker.

I andra sammanhang kan en fullständig behörighetskontroll framstå som självklar, jfr de kontroller som görs av en ansökan om lagfart, i rättegång eller när betalning beordras av betydande belopp från ett konto i en bank. Vanligtvis finns inga särskilda regler om vilken dokumentation av behörighet som ska finnas och vilka kontroller som ska göra.[7] Det blir då upp till E-tjänsteleverantören att, utifrån det skyddsvärde som respektive e-tjänst anses ha, bedöma vilka krav som ska ställas på behörighetskontroller. Hanteringen av Attributsintyg får utformas utifrån dessa förutsättningar.

[7] Jfr dock rättegångsbalkens krav på bl.a. registreringsbevis och fullmakter och den redovisade särregleringen i patientdatalagen.

1.6 Processen för granskning och samverkan

När juridisk behörighet ska kontrolleras i elektronisk miljö bör hanteringen kunna förenklas med stöd av den föreslagna Infrastrukturen för identifiering. Denna hantering kan, som en följd av den *automatisering* som sker i IT-system, beskrivas som ett handlings- eller transaktionsmönster – i IT-sammanhang kallat en *process* (jfr avsnitt 1.1). Denna process kan beskrivas som ett antal steg där berörda aktörer har att

1. bedöma om registreringsbevis eller liknande behövs,
2. beställa registreringsbevis,
3. sända en beställning till rätt aktör,
4. motta beställningen,
5. se vilket intyg som ska lämnas enligt beställningen,
6. upprätta intyg,
7. sända intyget till rätt aktör,
8. motta intyget,
9. kontrollera att intyget är äkta, och
10. bedöma om intygets innehåll ska anses visa att behörighet föreligger.

När en person i traditionell miljö utger sig för att företräda att aktiebolag används vanligtvis registreringsbevis från Bolagsverket för en manuell granskning och bedömning. Bolagsverket tillhandahåller emellertid redan idag tjänster där elektroniska bevis med utdrag ur aktiebolagsregistret lämnas i XML-format. En förlitande part som mottagit ett sådant elektroniskt utdrag kan behandla det automatiserat enligt programmerade rutiner genom vilka det avgörs om behörighet anses föreligga för att t.ex. logga in i en e-tjänst, få del av uppgifter där eller lämna och skriva under uppgifter.

Skatteverket använder sig redan av denna elektroniska tjänst som fungerar som en del i den process som krävs för en helt automatiserad hantering; jfr processtegen i följande figur.

Skatteverket har också utformat en egen automatiserad procedur för att avgöra om uppgifterna i ett XML-baserat registreringsbevis visar att personen är behörig att företräda det aktuella bolaget.

Utformning och användning av vissa processteg i figuren bestäms i princip av respektive E-tjänsteleverantör, utifrån det skyddsvärde som leverantören anser att e-tjänsten har; se de steg som ligger utanför det röda fältet i följande figur. Däremot tar Bolagsverket emot beställningarna, ser vilka intyg som ska utfärdas samt upprättar och sänder dem.

Eftersom den föreslagna Infrastrukturen för identifiering avses användas, för dessa beställningar och svar, berörs även E-legitimationsnämnden som i denna del, i enlighet med sin instruktion, ska utveckla specifikationer och liknande krav som ska vara gemensamma för myndigheter under regeringen. Utformningen av juridiska behörighetskontroller med stöd av Attributsintyg kräver alltså samverkan mellan (A) E-legitimationsnämnden (som svarar för Infrastrukturen för identifiering via vilken begäran om intyg och utfärdade intyg distribueras), (B) Bolagsverket (som svarar för angivna delar i processen för att utfärda Attributsintyg) och de (C) E-tjänsteleverantörer som ansluts till Infrastrukturen för

identifiering och som ska kunna beställa, motta och använda Attributsintyg.

En del i denna samverkan är att utarbeta samordnade lösningar som är tillräckligt enkla och avgränsade för att kunna införas på bred front, så att även mindre aktörer, inom offentlig sektor kan nyttja dem. Målet bör vara en fullständig automatisering. Här behöver emellertid beaktas att myndigheter i många fall – i vart fall initialt – kan antas införa e-tjänster utifrån enklare lösningar med manuella inslag. I sådana fall bör resonemang från pappersmiljö ofta kunna återanvändas och förenklingar vara möjliga utifrån närmast självklara resonemang som var och en bör kunna förstå. Här kan som exempel nämnas ärenden där t.ex. telefaxmeddelanden eller kanske till och med uppgiftslämnande per telefon godtas. När samma ärenden handläggs i elektronisk miljö kan fullständiga behörighetskontroller knappast krävas, med e-legitimationer och attributsintyg, bara för att IT-stöd införts.

Här behöver också beaktas att kontroller av juridisk behörighet kan bli komplicerade i enskilda fall. Behörighetsfrågan behöver då – om en fullständig kontroll ska göras – bedömas manuellt. I undantagsfall kan rättsutredningar och bedömningar av expertis behövas. Sådana komplicerade juridiska bedömningar kan inte automatiseras eftersom de inte kan styras av på förhand programmerade lösningar.

Väljer den förlitande parten att ta en medveten risk kan automatisering dock ske även i sådana fall. Tolkningssvårigheterna uppdagas då inte förrän i ett senare skede när transaktionen redan utförts. Ett skäl för att godta sådana förenklingar kan vara ett en uppgiven företrädare har ett strängt personligt skadeståndsansvar gentemot den förlitande parten: Enkelt uttryckt, blir organisationen inte bunden av beställningen kan användaren av e-legitimationen bli skyldig att ersätta den skada som därmed drabbar den förlitande parten. Dessa regler gäller även för elektronisk miljö så länge inte annat föreskrivs.

Den infrastruktur som E-legitimationsnämnden inför för juridiska behörighetskontroller bör tillhandahålla de funktioner och kontrollnivåer som e-tjänstelevererande myndigheter och företag efterfrågar. Det får därefter bli upp till respektive E-tjänsteleverantör att utifrån beskrivna flöden avgöra vilket stöd för behörighetskontroller som ska införas i en e-tjänst. Denna infrastruktur får som framgått inte blandas samman med åtkomstkontroller inom en organisation eller de kombinationer av

kontroller för vilka särskild reglering har införts i patientdatalagen m.fl. författningar.

1.7 En samordnad hantering av Attributsintyg

1.7.1 Bolagsverkets nuvarande tjänster

Bolagsverket har dels en *myndighetsutövande funktion*, till vilken hör att registrera företag (bl.a. aktiebolag som här används som exempel), dels en *servicefunktion* som innefattar att *tillhandahålla företagsinformation* från verkets register (bl.a. Aktiebolagsregistret). Informationen tillhandahålls på flera olika sätt till förlitande parter, som t.ex. kan beställa ett traditionellt registreringsbevis på papper och få det översänt med vanlig post.[8] Den som behöver information om företag kan emellertid också söka fram samma uppgifter i verkets Näringslivsregister och ladda ned e-registreringsbevis i ett format som var och en kan läsa. Det är också möjligt att beställa eller ladda ned ett fullständigt eller tidsbegränsat historiskt bevis där alla ändringar, respektive de ändringar som skett under viss tid redovisas.

Den som inte nöjer sig med att få reda på vilka uppgifter som redan har registrerats i Aktiebolagsregistret kan beställa diariebevis eller ärendebevis, där det i det första fallet framgår om en handling som rör ett visst bolag har kommit in och i det andra fallet dessutom framgår vilket slags ärende som inkommen handling avser. Till detta kommer Bolagsverkets särskilda beställningsverksamhet där uppgifter lämnas ur register förpackade i enlighet med en beställares önskemål.

1.7.2 XML-paket

Leveranser i elektronisk miljö

Bolagsverket har även infört tjänster där s.k. XML-paket levereras. En av dessa produkter, betecknad ”FunktionarerFirmateckning-Vakanser”, visar bl.a. firmateckning; dvs. samtliga företrädare som är registrerade. Dessa XML-paket kan levereras även med historik. Automatiserade frågor efter sådana paket ställs med organisations-

[8] Beviset innehåller bl.a. företagets namn, registreringsdatum, verksamhet, firmatecknare, styrelse, företrädare samt adressen till företaget och till styrelsen.

nummer som sökbegrepp. Den som mottar XML-paket avses kunna låta egna datorprogram bearbeta och visa uppgifter i egna gränssnitt.

Dessa tjänster tar liksom de som beskrivits i avsnitt 1.6.1 s*in utgångspunkt* i det aktuella *aktiebolaget*. Bolagets organisationsnummer används som sökbegrepp. E-tjänsteleverantören avses därefter utifrån mottagna uppgifter om bolaget kunna sortera fram de uppgifter som rör den individ som legitimerat sig i e-tjänsten och att utifrån dem bedöma om denne är behörig att företräda aktuellt bolag.

Visserligen tillhandahåller verket också bevis om funktioner som tar sin utgångspunkt i en viss individ och visar vilka uppdrag denne har i olika företag eller föreningar. Dessa bevis utvisar emellertid inte i vilken mån individen är behörig firmatecknare i dessa företag och föreningar.

Mottagarens hantering

Den som beställt och mottagit XML-paket för behörighetskontroller måste emellertid sortera och tolka informationen. Eftersom XML-paketen tar sin utgångspunkt i företaget – inte i den individ som besöker en e-tjänst – blir informationen omfattande. Samtliga uppgifter om firmateckningsrätt finns med och en mängd andra uppgifter.

Materialet har visserligen försetts med koder, avsedda att förenkla en automatisering, men komplexiteten blir betydande och det behövs juridisk kompetens för att kravställa funktioner för kontroller. Det har visat sig svårt för E-tjänsteleverantörer att *sortera* sådan omfattande information och att göra de tolkningar och det utvecklingsarbete som krävs för att införa en automatiserad kontrollrutin i en e-tjänst.

Bolagsverket ska leverera utdrag – inte tolka innehållet

Till bakgrunden vid Bolagsverkets utveckling av dessa lösningar hör att verket inom ramen för sin servicefunktion endast ska lämna uppgifter ur registret – registerutdrag. Bolagsverket ska naturligtvis inte göra tolkningar av innehållet åt förlitande parter. E-tjänsteleverantörerna ska alltså själva granska och juridiskt bedöma om

den som använder e-tjänsten är behörig – alternativt välja att ta en viss risk.

I praktiken synes denna närmast självklara utgångspunkt emellertid ha lett till en alltför begränsad syn på vad som är ett registerutdrag till skillnad från en tolkning av registrets innehåll. Av regleringen i lag och förordning framgår nämligen endast följande. Enligt 8 kap. 43 § första stycket 3 ABL ska varje aktiebolag för registrering anmäla av vilka och hur bolagets firma tecknas. I paragrafens andra stycke sägs att anmälan ska innehålla uppgift om bl.a. postadress för de personer som anges i första stycket 3 och de angivna personernas personnummer. På liknande sätt föreskrivs i 1 kap. 3 § aktiebolagsförordningen (2005:559; ABF) att en anmälan för registrering enligt 2 kap. 22 § ABL ska innehålla uppgift om hur bolagets firma tecknas. I 2 kap. 14 § ABF sägs vidare att de uppgifter som avses i 8 kap. 43 § ABL ska antecknas när ett aktiebolag registreras. Cirkeln är därmed sluten och det finns inte några myndighetsföreskrifter på området

Kraven i författning på registreringens utformning går alltså inte längre än att det ska noteras ”av vilka och hur bolagets firma tecknas”. Dessa uppgifter registreras i maskinläsbar form. Varje presentation för vanlig läsning av en människa kräver alltså omvandling av digitala data till text på t.ex. papper eller bildskärm. Redan detta innefattar en tolkning från ett maskinspråk till ett uppfattbart språk. Dessutom görs vissa urval redan idag genom att fullständiga registerutdrag är ovanliga och att de begränsade utdragen innefattar viss sortering.

Även om det inte finns någon knivskarp gräns för samtliga fall mellan vad som utgör en juridisk tolkning av registrets innehåll, till skillnad från ett rent utdrag som begränsats till en delmängd av uppgifter, bör avgränsningar kunna ske så att även en träffsäkert begränsad mängd uppgifter ur t.ex. aktiebolagsregistret kan betraktas som utdrag ur registret; inte en juridisk tolkning.

1.7.3 Automatiserade tolkningar

Begränsade, kodade uppgifter i förfinade registerutdrag

Det har visat sig komplicerat för E-tjänsteleverantörer att tolka komplex information från Bolagsverket, särskilt när den ska användas automatiserat. Genom dessa utdrag överförs som fram-

gått betydligt mer information än E-tjänsteleverantören behöver. Informationen måste därför sorteras och tolkas. Den förlitande parten (E-tjänsteleverantören) har själv haft att sortera fram de uppgifter som behövs och har dessutom haft att utveckla ett automatiserat stöd för kontroller. Hittills synes endast Skatteverket ha infört en teknisk lösning för kontroller där det automatiserat bedöms om en person är behörig att företa en viss rättshandling. Dessutom är denna funktion begränsad till att ange om en person är behörig att ensam teckna firman.

Bolagsverket har därför inlett ett utvecklingsarbete för att förenkla hanteringen. Tanken är att Bolagsverket ska kunna lämna förfinade registerutdrag ur t.ex. aktiebolagsregistret, med endast *delmängder* av de uppgifter som idag lämnas i XML-paket. Utvecklingsarbetet är knutet till utredningens förslag om att införa en Infrastruktur för identifiering, där Identitetsintyg ska kunna kompletteras med Attributsintyg som tar sin *utgångspunkt i en individ* som t.ex. loggar in i en e-tjänst.

Från Bolagsverkets utgångspunkter blir frågan hur förfinade utdrag ska kunna utformas så att de endast blir att anse som registerutdrag – inte som juridiska tolkningar åt förlitande parter av om en viss individ är behörig företrädare för en juridisk person. Sådana intyg avses underlätta och förbättra verkets servicefunktion genom att E-tjänsteleverantörer enkelt, säkert och automatiserat ska kunna begära och få ut registrerade uppgifter samt utföra erforderliga kontroller. För E-tjänsteleverantörerna blir frågan istället hur de ska kunna hantera intyg för automatiserade bedömningar av juridisk behörighet.

Till nämndens uppgifter hör att skapa enighet och samordning mellan dessa aktörer inom ramen för en balanserad lösning. För att en sådan samordning ska kunna etableras måste, som ett första steg, ett förslag till en praktisk lösning tas fram. Här har Bolagsverket redan gjort ett omfattande arbete för att införa koder i sina register, bl.a. i Aktiebolagsregistret. Dessa koder finns redan med i de registerutdrag som lämnas i form av XML-paket. Tanken har varit att E-tjänsteleverantörer ska kunna programmera sina e-tjänster att godta de Användare som har kod(er) som visar att de är behöriga firmatecknare. Redan i denna del har emellertid vissa frågor aktualiserats. Koden ”FAVE” (= firman tecknas ensam av) kan enkelt förstås när den knyts till ett *personnummer* och en automatiserad tolkning av detta kan enkelt programmeras. När koden knyts till ”le” (=ledamöter) måste emellertid den automatiserade

granskningen kopplas till de fält där bolagets ledamöter anges. Eftersom ett utdrag ur Aktiebolagsregistret utgör en ögonblicksbild av registrets innehåll, även vid användning av XML-paket, kan det knappast hävdas att en angivelse av FAVE och le skulle utgöra ett registerutdrag, medan en användning av FAVE-koden så att den knyts till personnumret för varje ledamot som har ensam firmateckningsrätt skulle utgöra en tolkning. Uppgifterna kan inte missförstås utan utgör endast två olika språkliga sätt att säga samma sak.

Dessa exempel tydliggör den typ av frågor som behöver lösas.

Frågor för att få förfinade registerutdrag

När Bolagsverket funnit lämpliga lösningar rörande innehållet i förfinade registerutdrag behöver det klarläggas hur den standardiserade lösningen (SAML) ska kunna användas för att ställa frågor om juridisk behörighet. Denna standard används vanligtvis för att få svar rörande egenskaper som avser ett enda subjekt. En preliminär genomgång har emellertid visat att de avgränsningar som krävs till visst företag – är x firmatecknare i bolaget y – bör kunna ske genom att frågan innehåller t.ex. individens personnummer och företagets organisationsnummer.

Det behöver härvid genomlysas hur olika strukturer av svar ska kunna lämnas i Attributsintyg så att kontroller kan göras automatiskt i e-tjänsten. Även här aktualiseras frågor om roller. Lösningarna ska utformas så att E-tjänsteleverantörer eller andra inte kan få uppfattningen att Bolagsverket eller E-legitimationsnämnden utför juridiska tolkningar åt E-tjänsteleverantörer. Bolagsverket ska inte göra någon bedömning av en individs rätt att företa en viss rättshandling utan endast, genom den Infrastruktur för identifiering som E-legitimationen avses svara för, lämna svar elektroniskt med ett registerutdrag som avgränsats till uppgifter om den individ som agerat.

Stöd för automatiserade kontroller

För att en sådan lösning ska kunna få spridning behövs också funktioner för att E-tjänsteleverantörer ska kunna ta emot och tolka informationen. Denna samordning bör kunna ske inom

ramen för E-legitimationens uppdrag enligt myndighetens instruktion – att utveckla specifikationer och liknande krav som ska vara gemensamma för myndigheter under regeringen i deras användning av e-legitimationer.

Till denna användning hör inte bara e-legitimationerna utan även de Identitets- och Attributsintyg som behövs för att infrastrukturen ska fungera. I praktiken behöver någon programvara eller tjänst utvecklas, så att varje E-tjänsteleverantör enkelt kan automatisera kontroller av juridisk behörighet med stöd av Attributsintyg från Bolagsverket. Detta stöd bör kunna utvecklas i samverkan mellan Bolagsverket, E-legitimationsnämnden, Tillväxtverket, Skatteverket och Försäkringskassan m.fl. myndigheter som kommit långt i införandet av E-tjänster. Motsvarande lösningar bör i annan ordning tas fram för privat sektor.

Regleringen

Utvecklingstakten är hög. Det kan därför med kort varsel behövas anpassningar till nya behov eller risker. Till detta kommer att detaljeringsgraden kan bli hög. Regler i lag eller förordning är därför knappast ett lämpligt styrmedel. En reglering genom myndighetsföreskrifter kan däremot visa sig önskvärd, särskilt som avtal i många fall inte kan ingås mellan berörda aktörer eftersom de utgör en del av samma juridiska person (myndigheter under regeringen). En naturlig utgångspunkt för en fördelning av regelområdet finns också genom att

- Bolagsverket meddelar föreskrifter om vilka uppgifter som lämnas i förfinade registerutdrag och hur dessa uppgifter används (så att verket inte anses ha gjort tolkningar för annan), och
- E-legitimationsnämnden meddelar föreskrifter om Attributsintyg och deras funktioner och användning inom Infrastrukturen för Svensk e-legitimation.

En sådan normgivningskompetens för E-legitimationsnämnden ges enligt 40 § förslag till förordning om infrastrukturen för Svensk e-legitimation.

1.8 Kommuner

Samma användning i kommuners e-tjänster

Den beskrivna lösningen för *juridiska* behörighetskontroller har tagits fram med tanke främst på statliga myndigheter som behöver kontrollera om en fysisk person som uppger sig företräda en juridisk person är behörig att företräda denne, t.ex. ett aktiebolag eller någon annan organisation för vilken ett register förs enligt författning där uppgifter finns om firmatecknare.

Samma lösning bör fungera för kommuner som tillhandahåller sådana e-tjänster där användares juridiska behörighet att företräda en viss juridisk person måste kontrolleras. Här kan de kommunala myndigheternas behov av kontroll vara desamma som för statliga myndigheter – i den mån en fullständig behörighetskontroll verkligen behövs vid användning av den aktuella e-tjänsten.

Till detta kommer de samordnade lösningar som avses skapas för att även små myndigheter smidig ska kunna integrera, använda och administrera funktioner för Identitets- och Attributsintyg. Detta stöd kan antas bli betydelsefullt även inom kommunal sektor.

Publika register finns inte över behöriga handläggare

Kommunernas användning av registreringsbevis från Bolagsverket för att kontrollera juridisk behörighet att företräda t.ex. aktiebolag får emellertid inte förväxlas med kontroller av om en person är behörig handläggare hos *en myndighet* så att kontakter med en annan myndighet – t.ex. användning av en annan myndighets e-tjänst – sker behörigen. Skulle en sådan tjänst, för att kommunicera mellan myndigheter, anses kräva en fullständig kontroll av att den person som utger sig för att agera för en annan myndighets räkning verkligen är behörig att handlägga ärendet, kan den ovan beskrivna lösningen inte användas. Detta beror inte på att den tekniska lösningen skulle sakna tillräckliga funktioner utan på att det inte finns några *författningsreglerade register* över vilka handläggare vid kommuner eller andra myndigheter som är behöriga att handlägga en fråga. Det pågår emellertid ett arbete för att skapa sådana register och kataloger internt hos flera kommuner, där det tydligt och uppdaterat ska framgå vilka som är behöriga att handlägga olika kategorier av ärenden.

E-legitimationsnämnden bör i sitt fortsatta arbete agera för att myndigheter ska strukturera sina delegationsordningar m.m. på visst sätt och tillhandahålla dessa uppgifter elektroniskt så att det framgår vilka som är behöriga handläggare av olika kategorier av ärenden. Det är emellertid viktigt att hålla isär dessa behov av kontroller från de juridiska behörighetskontroller för vilka t.ex. Bolagsverket tillhandahåller registerutdrag.

1.9 Landsting

Landsting kan också tillhandahålla e-tjänster för företag och behöva kontrollera att den som loggar in är juridiskt behörig att agera för företagets, t.ex. ett aktiebolags räkning. Även här bör lösningen med Attributsintyg från Bolagsverket passa, förutsatt att landstingen kan godta den tekniska hanteringen inom den nationella Infrastrukturen för identifiering. I denna del torde det i praktiken kunna bli enkelt eftersom källan till den efterfrågade informationen finns på *ett enda ställe* för hela riket – hos Bolagsverket – och att den grundläggande hanteringen av dessa uppgifter är *reglerad* i lag och förordning utifrån syftet att sprida uppgifterna (s.k. publicitetsregister).

Inom kommunala och landstingskommunala myndigheter finns däremot som framgått inga lagreglerade publicitetsregister över vilka anställda och uppdragstagare som har olika behörigheter. På det område som regleras av patientdatalagen behövs uppgifter från olika register. Dessa register är inte publika och det finns inte någon sådan reglering av registerinnehåll och ansvar gentemot andra för registeruppgifter som vid användning av t.ex. aktiebolagsregistret eller fastighetsregistret.

Regleringen i patientdatalagen leder dessutom till blandade krav på dels *åtkomstkontroll* inom respektive mellan myndigheter och andra organ, dels en slags juridisk *behörighetskontroll* inom och mellan olika organ när åtgärder får vidtas endast av personer som har vissa roller. Det är nödvändigt att beakta dessa skillnader i reglering och hantering av *juridiska behörighetskontroller* av det slag som Bolagsverket avses stödja genom registerutdrag i form av Attributsintyg, respektive *blandade kontroller* enligt patientdatalagen av åtkomst och behörighet, inom respektive mellan myndigheter.

För hanteringen av Attributsintyg gäller olika juridiska förutsättningar vid behörighetskontroller med stöd av ett elektroniskt registerutdrag (Attributsintyg) från Bolagsverket och motsvarande intyg som lämnas inom det område som regleras av patientdatalagen. På det senare området tillkommer de roller och egenskaper inom ett organ, t.ex. ett landsting, som ska kunna kontrolleras enligt reglerna om inre sekretess och de register över ”behörigheter” som ska finnas och administreras hos varje vårdgivare.

1.10 En samordning kräver fortsatta analyser

De berörda särskilda reglerna för hälso- och sjukvårdsområdet och den hantering av attribut som krävs där får inte sammanblandas med generella kontroller av juridisk behörighet. Det är också viktigt att skilja frågan om vilka e-legitimationer ska få användas som Svensk e-legitimation från frågor om vilka attribut och Attributsutfärdare som ska finnas inom ramen för den Infrastruktur för identifiering (vilken även ska innefatta attributshantering) som E-legitimationsnämnden ska etablera. Exempelvis bör de e-tjänstelegitimationer som landstingen och flera kommuner infört och som uppfyller de högt ställda krav på identifiering kunna användas inom hela Infrastrukturen för Svensk e-legitimation medan all attributshantering för vilken sådana e-tjänstelegitimationer används kanske inte hör hemma inom den infrastruktur som E-legitimationsnämnden etablerar. En sortering behöver därför göras av vad som ska ingå i den Infrastruktur för identifiering som E-legitimationsnämnden enligt sin instruktion har att etablera och vad som bör utformas som särlösningar för t.ex. hälso- och sjukvårdsområdet.

Detta innebär naturligtvis inte att E-legitimationsnämnden ska bortse från behoven inom kommuner och landsting. Dessa behov bör så långt möjligt tillgodoses genom samordnade lösningar. Däremot bör lösningar som tillgodoser speciella krav, t.ex. inom hälso- och sjukvården, och som skulle föra med sig hinder eller begränsningar om de genomförs generellt, inte införas på områden där de inte behövs.

Genom att i det fortsatta arbetet närmare klargöra dessa skillnader och hur de bör hanteras kan sammanblandningar och missförstånd undvikas. Samtidigt kan de lösningar som E-legitima-

tionsnämnden respektive landstingen utvecklar tydligt avgränsas så att kravställning och samordning kan förenklas. En fråga i detta sammanhang är om det kan vara så att brister i samsyn som framträtt i det tekniska utvecklingsarbetet inte längre gör sig gällande om sammanblandningar med särlösningar för enskilda områden kan undgås. Här bör nämnas hur de förslag som utredningen tagit fram innebär att Användaren först legitimerar sig och att ett Identitetsintyg lämnas till E-tjänsteleverantören, som därefter beställer och får ett Attributsintyg från t.ex. Bolagsverket, medan det förslag som diskuterats inom hälso- och sjukvårdsområdet går ut på att i ett och samma intyg lämna uppgifter om såväl identitet som attribut, efter att Användaren legitimerat sig och systemet för utfärdande av intyg hämtat attribut från tillgängliga kataloger.

Det bör således genomlysas om skillnader i teknisk och administrativ syn på hur standarden (SAML) ska användas kan överbryggas när skilda förutsättningarna på dessa områden har klargjorts och beaktats. Den komplexa hanteringen av en mängd kataloger inom hälso- och sjukvårdsområdet och de särskilda kraven på tilldelade finmaskiga behörigheter för intern och extern åtkomst saknar motsvarighet vid de juridiska behörighetskontroller som görs med stöd av uppgifter ur t.ex. aktiebolagsregistret. Till detta kommer att attribut inom hälso- och sjukvårdsområdet styrs även utifrån användares angivelser av i vilken egenskap (uppdrag) de agerar i det enskilda fallet. Samma person kan ha flera uppdrag inom hälso- och sjukvården, vilket normalt inte blir fallet vid grovmaskiga juridiska behörighetskontroller där individen antingen är firmatecknare/fullmäktig eller saknar behörighet.

Härvid får sammanblandningar inte ske med kraven på t.ex. e-tjänstelegitimationer. Den Infrastruktur för Svensk e-legitimation som E-legitimationsnämnden ska införa bör harmoniera med existerande lösningar inom såväl hälso- och sjukvårdsområdets som andra kommunala redan existerande federationslösningar. Här kan olika tekniska och administrativa lösningar diskuteras för att säkerställa samverkande lösningar. En pusselbit för att åstadkomma en sådan samordning skulle kunna vara en genomtänkt anvisningstjänst som ger stöd även för användares val av uppdrag eller roll. En sådan angivelse skulle kunna läggas till grund för val av olika attributskällor, vilket blir intressant vid legitimering med bl.a. e-tjänstelegitimationer. I fall där en e-tjänst kräver intyg, som utöver identitet även behöver ange vilka rättigheter Användaren har i den

aktuella e-tjänsten, kan en på så sätt vidareutvecklad anvisningstjänst möjlige underlätta för fall där det redan finns attributskällor etablerade, t.ex. inom vård och omsorg. Dessa frågor behöver emellertid genomlysas närmare.

Genom att uppmärksamma och genomlysa dessa skillnader mellan rättsfrågor som har sin grund i patientdatalagens (finmaskiga) särreglering respektive generella regler om kontroller av en (grovmaskig) rätt att teckna en juridisk persons firma och tekniska val som görs för att tillgodose patientdatalagens särreglering respektive kontroller av juridisk behörighet, bör det alltså bli möjligt att finna en samsyn även kring tekniska frågor. Samtidigt bör missförstånd kunna undvikas.

Tillitsramverk

1 Tillitsramverk för e-legitimering

Detta tillitsramverk avses utgöra en central del i det regelverk som ska vara styrande för Infrastrukturen för identifiering. Utredningens arbete har emellertid inte nått så långt att det i alla delar kunnat bestämmas hur regelhierarkin ska se ut och på vilka nivåer i denna hierarki som närmare regler och krav ska finnas. I denna bilaga ges därför en första sammanställning och anpassning av de krav som kan ställas på utfärdare av Svensk e-legitimation. Infrastrukturen för identifiering bör ta sin utgångspunkt i ett tillitsramverk byggt på internationell standard och medge den flexibilitet som den föreslagna Infrastrukturen för Svensk e-legitimation och internationell samverkan kräver. Det måste emellertid säkerställas att dessa standarder är tillämpbara på och förenliga med svenska förhållanden.

Bilagan bör läsas som en vägledning inför en anpassning av Svensk e-legitimation till internationell standard, och de mer konkreta och detaljerade krav som en sådan anpassning kan komma att kräva.

För att konkretisera den diskussion som måste föras om ett tillitsramverks närmare utformning, har detta första utkast till en sammanfattning av de krav som kan förväntas ställas på Svensk e-legitimation tagits fram. Utkastet bör läsas som en vägledning inför en anpassning av Svensk e-legitimation till internationell standard, och de mer konkreta och detaljerade krav som en sådan anpassning kan komma att kräva.

De flesta av de internationella ansträngningar som gjorts för att definiera nivåer av tillit vid användning av e-legitimationer har sin grund i en publikation (SP 800-63) från det amerikanska National Institute of Standards and Technology (NIST). De riktlinjer som beskrivs där är emellertid relativt allmänt hållna. Fördjupande arbeten har därför bedrivits inom bl.a. Europeiska unionen, där det storskaliga s.k. STORK-projektet utgjort en viktig del[1].

[1] EU-kommissionen har tagit fram en handlingsplan som ska underlätta för medlemsstaterna att införa ömsesidigt godkända och kompatibla system för e-signaturer och e-legitimationer i syfte att göra det lättare att tillhandahålla elektroniska offentliga tjänster över gränserna [KOM(2008) 798]. Arbetet för ömsesidigt erkännande av elektronisk identifiering inom EU genomförs inom STORK-projektet.

Ett betydelsefullt arbete för att utarbeta ett internationellt tillitsramverk bedrivs nu också inom International Organization for Standardization och International Electrotechnical Commission (ISO/IEC). Det kommande resultatet av detta arbete, ISO/IEC 29115, som förväntas bli internationell norm på området, bygger på dokument som publicerats inom det s.k. Kantara Initiative Identity Assurance Framework (Kantara IAF).

Under förutsättning att det fortsatta arbetet inom ISO/IEC leder till resultat som är förenliga med behoven inom den föreslagna Infrastrukturen för identifiering bör Sverige följa denna internationella standard. E-legitimationsnämnden bör därför, liksom E-delegationen, verka för att resultatet av standardiseringsarbetet blir förenligt med svenska intressen på området.

I avvaktan på detta resultat bör ett tillitsramverk införas som har sin förankring i de tidigare nämnda publikationerna. De har alla gemensamt att de definierar fyra tillitsnivåer (AL)[2] för e-legitimering, i syfte att möta olika nivåer av risk och olika krav på användbarhet. Dessa tillitsnivåer svarar mot olika grader av teknisk och operationell säkerhet hos utfärdaren och olika grader av kontroll av att en person som tilldelas en elektronisk identitet verkligen är den han eller hon utger sig för att vara.

Något förenklat kan tillitsnivåerna beskrivas som en måttstock, där en lägre indikering på skalan motsvarar enklare användning och utgivning, lägre kostnader, men också en lägre skyddsnivå. Högre klassificering medför högre kostnader för såväl utgivande som användande, men leder till att en högre grad av tillit kan fästas vid identifieringen.

1.1 Svensk e-legitimation

Vid en tillämpning av dessa internationella normer har det, såvitt hittills framkommit, visat sig ändamålsenligt att för Svensk e-legitimation kräva en tillitsnivå som motsvarar nivå 3 (AL3) eller högre. Detta innebär att utgivare av Svensk e-legitimation ska ha dokumenterade och fungerande ledningssystem för informationssäkerhet i enlighet med erkända standarder, att innehavares identiteter verifieras på ett ändamålsenligt sätt, att metoden för

[2] AL är en förkortning av den internationella termen för tillitsnivå, ”Assurance Level”, som används såväl i Kantara IAF som i STORK-projektet.

legitimering baseras på starka kryptografiska mekanismer och utgivaren ska kunna påvisa att de når upp till och efterlever kraven enligt AL3.

Tillitsnivå 3 är också den nivå som ligger närmast de av ramavtalsleverantörerna idag utgivna e-legitimationerna. Den öppnar emellertid även nya typer av e-legitimationer som inte är certifikatbaserade. Detta förväntas kunna leda till en högre användbarhet och större spridning inom fler samhällsgrupper. Om det visar sig att en betydande del av de redan utgivna e-legitimationerna inte uppfyller kraven för nivå 3 i tillitsramverket kan det komma att bli nödvändigt att etablera övergångsregler så att dessa kan godtas inom infrastrukturen för Svensk e-legitimation till dess att en anpassning skett. Kvalificerade certifikat utgivna i enlighet med lagen (2000:832) om kvalificerade elektroniska signaturer kan, bland annat beroende på metod för utgivning, komma att uppfylla kraven för nivå 2, 3 eller 4, och därmed också användas inom infrastrukturen för Svensk e-legitimation. Då kraven i tillitsramverket är väsentligt mer specifikt framställda än de som återfinns i 4 kap. signaturlagen, följer att kvalificerade certifikat inte med automatik uppfyller någon tillitsnivå högre än 2.

En förutsättning för att en Svensk e-legitimation ska få utfärdas föreslås dessutom vara att användaren har svenskt person- eller samordningsnummer. En e-tjänsteleverantör kan därför, när Svensk e-legitimation använts, veta att det finns möjlighet att få sådan information, i ett identitetsintyg eller efter en manuell förfrågan om en sådan påkallas från persondataskyddssynpunkt. Dessa krav införs liksom regleringen i övrigt genom avtal mellan E-legitimationsnämnden och utfärdare för anslutning till Infrastrukturen för Svensk e-legitimation, i den mån detta inte följer av författningsreglering.

E-legitimationsnämnden ska utöva tillsyn över utfärdare av Svensk e-legitimation så att tillgänglighet, kvalitet och informationssäkerhet blir säkerställda i enlighet med ett regelverk för Infrastrukturen för Svensk e-legitimation. I enlighet med regelverket ska nämnden också kunna ingripa mot missförhållanden – ytterst avveckla en utfärdare om omständigheterna är sådana att de riskerar att leda till oacceptabla konsekvenser för användare, e-tjänsteleverantörer eller andra, eller i stort rubba förtroendet för Infrastrukturen för Svensk e-legitimation.

1.2 Internationell samverkan

Vid samverkan över nationsgränserna kan andra länders E-legitimationer översättas till AL1 eller AL2 i tillitsramverket. Om en utländsk E-legitimation erhållit klassificering enligt STORK-projektets modell, kan Nivå 2 eller högre översättas till AL2. Vid de fall det råder tveksamhet under vilka premisser en utländsk E-legitimation utfärdas, ska dessa istället översättas till AL1.

1.3 Tillitsnivåer

Fyra tillitsnivåer (AL1—AL4) definieras. Nivåerna indikerar hur stor tilltro man bör fästa vid en elektronisk identitet, och beskrivs enligt nedanstående skala:

AL1: ingen eller liten tilltro till identiteten
AL2: viss tilltro till identiteten
AL3: hög tilltro till identiteten
AL4: mycket hög tilltro till identiteten

För att kunna fastställa lägsta acceptabla tillitsnivå för en e-tjänst, bör de risker och konsekvenser som en felaktig identifiering kan medföra inom följande områden beaktas:

- Obehag, oro eller ryktesskada
- Finansiell skada
- Skada för myndighetens rykte
- Civilt- eller straffrättsligt brott
- Personsäkerhet

För höga krav på identifieringen kan medföra högre kostnader för e-tjänsten, men också resultera i mindre flexibilitet och användbarhet för användaren. Den högre kostnaden för identifiering uppstår på grund av att det vanligen är dyrare att utfärda och underhålla en identitet med en högre tillitsnivå än en med en lägre. Den minskade flexibiliteten för användaren visar sig t.ex. genom att användaren enbart kan använda viss utrustning eller viss programvara för att nå e-tjänsten, eller att identiteten i praktiken enbart kan utfärdas till och användas av vissa kategorier av befolkningen.

Som grundregel bör därför en e-tjänst kräva en lägsta tillitsnivå som står i proportion till de identifierade riskerna enligt ovan.

1.3.1 Nivå 1 (AL1)

På Tillitsnivå 1 finns ingen eller liten tilltro till angiven identitet. Användning av denna nivå är lämplig när resultat av en felaktig identifiering endast förväntas leda till marginella negativa konsekvenser, samtidigt som identifieringsmetoden ger viss tillit och underlättar för användaren och/eller e-tjänsten.

Felaktig identifiering i en e-tjänst som kräver denna nivå kan t.ex. innebära:

- små monetära förluster
- liten skada på rykte

Exempel: Uppgiftslämnande via en e-tjänst kan använda sig av AL1 i de fall när information endast flödar från individen till e-tjänsten, inga känsliga uppgifter delges uppgiftslämnaren och inga av de övriga kraven för högre tillitsnivåer blir tillämpliga.

Ett flertal olika tekniker för identifiering kan användas, t.ex. lösenord eller PIN-kod. Denna nivå kräver inte heller starkt kryptografiskt skydd av identiteten.

1.3.2 Nivå 2 (AL2)

På Tillitsnivå 2 finns viss tilltro till angiven identitet. Användning av denna nivå är lämplig när man kan se vissa negativa konsekvenser som resultat av en felaktig identifieringen.

Användning av starkt lösenord över öppet nätverk är en acceptabel identifieringsmekanism på denna nivå. AL2 kräver skydd mot avlyssning, återuppspelning och gissning av lösenord.

Fastställandet av sökandens identitet kan ske utan traditionell legitimering vid personligt besök, och istället baseras på metoder liknande de för utgivning av kreditkort.

Felaktig identifiering i en e-tjänst som kräver denna nivå kan t.ex. innebära:

- medelhöga monetära förluster

- att delvis känslig information kommer i orätta händer
- viss skada på rykte

Exempel: E-tjänster som tar emot och lämnar ut delvis känslig information, men där uppgifterna i sig kan verifieras eller inhämtas på annat sätt, kan använda sig av AL2 förutsatt att inga av de övriga kraven för högre tillitsnivåer blir tillämpliga.

1.3.3 Nivå 3 (AL3)

På tillitsnivå 3 finns hög tilltro till angiven identitet. Användning av denna nivå är lämplig när man kan se substantiella konsekvenser som resultat av en felaktig identifiering.

Denna nivå kräver flerfaktorsidentifiering som styrker både kännedom om personlig kod samt kontroll över e-legitimationshandling som baserats på starka kryptografiska mekanismer. Både mjuka och hårda e-legitimationshandlingar är tillåtna, inklusive metoder för att framställa engångslösenord.

Kraven på kontroll av den ursprungliga identifieringen är starkare än på AL2, och kräver att användaren legitimerat sig vid ett personligt besök hos utfärdaren eller utfärdarens ombud.

Felaktig identifiering i en e-tjänst som kräver denna nivå kan t.ex. innebära:

- viss skada på allmänna intressen
- substantiella monetära förluster
- att känslig information kommer i orätta händer
- substantiell skada på rykte

Exempel: Inhämtande och utlämnande av känsliga uppgifter som traditionellt kräver identifiering med godkänd fotolegitimation, kan använda sig av AL3.

1.3.4 Nivå 4 (AL4)

På tillitsnivå 4 finns mycket hög tilltro till angiven identitet. Användning av denna nivå är lämplig när man kan se mycket stora konsekvenser som resultat av en felaktig identifiering.

Denna nivå kräver starkast möjliga identifieringsmekanismer, och måste baseras på kryptografiska metoder som bevisar tillgång till nyckelmaterial lagrat i hårda bärare under innehavarens direkta kontroll.

Hög kryptografisk och fysisk säkerhet krävs för samtliga ingående komponenter som hanterar nyckelmaterial. All data-överföring måste skyddas och skyddet måste vara kryptografiskt kopplat till det nyckelmaterial som används vid identifieringen.

Felaktig identifiering i en e-tjänst som kräver denna nivå kan t.ex. innebära:

- hög fara för annans liv
- stor skada på allmänna intressen
- stora monetära förluster (> 10 M EUR)
- att mycket känslig information kommer i orätta händer
- stor skada på rykte

2 Kriterier för utfärdande av Svensk e-legitimation

2.1 Organisation och styrning

1.1 Utfärdare av Svensk e-legitimation ska drivas som ett registrerat svenskt aktiebolag eller motsvarande utländska företag inom Europeiska ekonomiska samarbetsområdet.

1.2 Utfärdare ska ha en etablerad verksamhet, vara fullt operationell i alla delar som berörs i detta dokument, och vara väl insatt i de regulatoriska, avtalsmässiga och juridiska krav som ställs på denne som utfärdare av Svensk e-legitimation.

1.3 Utfärdare ska förfoga över tillräckliga ekonomiska medel för att kunna bedriva verksamheten i minst 1 år och bära risken för skadeståndsskyldighet.

2.2 Information om villkor

2.1 Utfärdaren ska tillhandahålla uppgifter om avtal, villkor samt anknytande uppgifter och eventuella begränsningar i användandet av tjänsten till anslutna användare, arbets- och uppdragsgivare, e-tjänsteleverantörer och andra som kan komma att förlita sig på utfärdarens tjänst.

2.2 En utfärdare som vill införa villkor som inte finns med i ansökningshandlingen ska tydligt hänvisa till villkoren och utforma rutinerna så att villkoren kommer sökanden tillhanda innan denne undertecknar eller annars ingår avtal med utfärdaren.

2.3 Utfärdaren ska tillhandahålla en utfärdardeklaration som bl.a. innefattar:

a) bolagets identitet och kontaktuppgifter,

b) ägarstruktur och vilka principer för bolagsstyrning som tillämpas,

c) villkor förknippade med den tillhandahållna tjänsten (inklusive metod för utgivning, spärr och avveckling),

d) metod att ändra villkoren för den tillhandahållna tjänsten,

e) utfärdarens skyldigheter, utfästa garantier, utlovad tillgänglighet och finansiellt ansvar,

f) användarens skyldigheter att skydda sin elektroniska identitet,

g) information om insamling, registrering, lagring, bearbetning, och spridning eller samkörning av personuppgifter, och i vilken mån detta sker.

2.4 Utfärdare av Svensk e-legitimation ska inhämta användarens samtycke vid nyteckning eller ändring av tjänsten, samt regelbundet var 5:e år.

2.5 Utfärdare av Svensk e-legitimation ska tillhandahålla en tjänst där användaren kan ändra tilläggsinformation knuten till den elektroniska identiteten (t.ex. e-postadress) samt spärra sin e-legitimation (spärrtjänst). Tjänsten ska ha god tillgänglighet och utfärdaren ska behandla anmälan om spärr skyndsamt.

2.6 Den arbets- eller uppdragsgivare som ansöker om en Svensk e-legitimation knuten till organisationstillhörighet (e-tjänst-elegitimation)

a) får bestämma hur e-tjänstelegitimationen får användas, t.ex. om den får användas även utanför tjänsten, och

b) får spärra e-legitimationen.

2.3 Identifiering och registrering

3.1 Utfärdare ska, beaktat reglerna för persondataskydd, föra register över anslutna användare och de tilldelade elektroniska identitetshandlingarna, och hålla detta register aktuellt.

3.2 Svensk e-legitimation får utfärdas endast efter skriftlig ansökan i traditionell form. Ansökan ska vara undertecknad på traditionellt sätt, med intyg om att lämnade uppgifter är riktiga och fullständiga.

3.3 Om en sökande redan har identifierats vid ett personligt besök (i enlighet med 3.8) för ekonomiskt eller rättsligt betydelsefulla mellanhavanden, och sökanden kan identifieras på annat tillförlitligt sätt som är likvärdigt med kraven för Svensk e-legitimation, får utfärdaren identifiera och ta emot ansökan genom denna tjänst i stället för enligt 3.2.

3.4 En ansökan om Svensk e-legitimation ska innehålla personnummer eller samordningsnummer, samt de uppgifter som i övrigt är nödvändiga för att identitetsutfärdaren ska kunna tillhandahålla sådan e-legitimation och utfärda identitetsintyg.

3.5 En Svensk e-legitimation knuten till organisationstillhörighet (e-tjänstelegitimation) får utfärdas endast efter skriftlig ansökan i traditionell form av en arbets- eller uppdragsgivare. Ansökan ska vara undertecknad på traditionellt sätt av arbets- eller uppdragsgivaren. Om denne är en juridisk person ska ansökan vara undertecknad av en behörig företrädare.

3.6 Om en arbets- eller uppdragsgivare eller en behörig företrädare för denne har legitimerat sig eller skrivit under med Svensk e-legitimation, eller enligt det förenklade förfarande som anges i 3.3, får en sådan underskrift eller legitimering för uppgiftslämnande ersätta ett förfarande enligt 3.5.

3.7 Utfärdare ska skyndsamt och på ett säkert sätt behandla och effektuera spärrbegäran och vidta sådana åtgärder för att förhindra missbruk av spärrtjänsten (eller andra handlingar som leder till spärr av en elektronisk identitetshandling) att användares e-legitimationer är tillgängliga när de behövs.

2.3.1 Fastställande av sökandens identitet

3.8 Utfärdare av Svensk e-legitimation ska kontrollera den sökandes identitet vid ett personligt besök, på likvärdigt sätt som vid en ansökan om en traditionell identitetshandling.

3.9 Utfärdare av en e-legitimation ska kontrollera att ansökan om e-legitimation är behörigen undertecknad på papper eller lämnad elektroniskt enligt 3.3, och att de uppgifter som den

sökande lämnat är fullständiga och stämmer överens med uppgifter som finns registrerade i ett officiellt register.

3.10 Utfärdare av en e-legitimation knuten till organisationstillhörighet (e-tjänstelegitimation) ska kontrollera att ansökan om e-legitimation är behörigen undertecknad på papper eller lämnad elektroniskt enligt 3.6, och att de uppgifter som den sökande lämnat är fullständiga och stämmer överens med uppgifter som finns registrerade i ett officiellt register.

2.3.2 Utfärdande av e-legitimation

3.11 Utfärdare av Svensk e-legitimation ska säkerställa att alla sökande tilldelas en unik elektronisk identitet och att de utfärdade elektroniska identitetshandlingarna är utformade så att de för användaren tydligt kan hänföras till den aktuella tjänsten.

3.12 Utfärdare av Svensk e-legitimation ska tillhandahålla den tilldelade elektroniska identitetshandlingen till sökanden på ett säkert sätt, och säkerställa att identitetshandlingen blir entydigt kopplad till sökandens elektroniska identitet.

3.13 En utfärdare som vid personligt besök eller via elektroniskt förfarande som är förenligt med 3.3, tillhandahåller både den elektroniska legitimationshandlingen som användaren ska inneha och personlig kod som användaren ska bruka för att aktivera e-legitimationen, ska bekräfta brevledes till sökandens folkbokföringsadress att överlämning av sådan e-legitimation skett.

3.14 Sökanden ska bekräfta att denne mottagit e-legitimationen innan den blir giltig.

2.3.3 Utformning av tekniska hjälpmedel

3.15 Tekniska hjälpmedel för identifiering genom Svensk e-legitimation ska utformas enligt sådan tvåfaktorsprincip att en del består i den elektroniska identitetshandlingen som användaren ska inneha, och en del i det som användaren ska bruka för att aktivera e-legitimationen (personlig kod).

3.16 Aktiveringsmekanismen och den personliga koden ska utformas så att det är osannolikt att en utomstående kan forcera aktiveringsskyddet, ens på maskinell väg.

3.17 Användare av Svensk e-legitimation ska på egen hand kunna byta personlig kod, och få hjälp att välja den personliga koden så att kraven i 3.16 upprätthålls.

2.3.4 Identitetsintyg

3.18 Utfärdare av Svensk e-legitimation ska tillhandahålla tjänst för utgivning av identitetsintyg till förlitande e-tjänster, enligt de tekniska specifikationer som E-legitimationsnämnden från tid till annan föreskriver. Utlämnande av identitetsintyg ska föregås av en tillförlitlig kontroll av den angivna elektroniska identiteten och den elektroniska identitetshandlingens giltighet.

3.19 Lämnade identitetsintyg ska vara giltiga endast så länge som det krävs för att användaren ska få tillgång till den efterfrågade e-tjänsten, samt skyddas så att informationen är läsbar endast för den avsedda mottagaren och att den som tar emot intyget kan kontrollera att mottagna intyg är äkta.

2.4 Operationella krav

4.1 Utfärdare ska ha ett ledningssystem för informationssäkerhet (LIS) som i tillämpliga delar baseras på ISO/IEC 27001 eller motsvarande erkända och vedertagna standarder, omfattande bl.a. organisation, resurser samt tekniska respektive administrativa säkerhetsåtgärder och utgöra en kvalitetsprocess som kontinuerligt ska utvärderas och anpassas till aktuella verksamhets- och omvärldskrav:

a) Samtliga säkerhetskritiska administrativa och tekniska processer ska dokumenteras och vila på en formell grund, där roller, ansvar och befogenheter finns tydligt definierade.

b) Utfärdare ska säkerställa att denne vid var tid har tillräckliga personella resurser till förfogande för att uppfylla sina åtaganden.

c) Utfärdare ska inrätta en process för riskhantering som på ett ändåmålsenligt sätt, kontinuerligt eller minst var sjätte månad, analyserar hot och sårbarheter i verksamheten, och som genom införande av säkerhetsåtgärder balanserar riskerna till acceptabla nivåer.
d) Utfärdare ska inrätta en process för incidenthantering som systematiskt säkerställer kvaliteten i tjänsten, former för vidarerapportering och att lämpliga reaktiva och preventiva åtgärder vidtas för att lindra eller förhindra skada vid händelser som lett till eller kunnat leda till en incident.
e) Utfärdare ska upprätta och testa en kontinuitetsplan som tillgodoser verksamhetens tillgänglighetskrav genom en förmåga att återställa kritiska processer vid händelse av katastrof eller allvarliga incidenter.

4.2 Ledningssystemet för informationssäkerhet och efterlevnaden av de krav som ställs på utfärdare av Svensk e-legitimation ska årligen vara föremål för internrevision, utförd av oberoende intern kontrollfunktion, såvida inte organisationens storlek eller annan försvarbar orsak motiverar annat.

4.3 Ledningssystemet för informationssäkerhet och efterlevnaden av de krav som ställs på utfärdare av Svensk e-legitimation ska vara föremål för extern revision minst var 24:e månad, och utföras av opartisk och självständig revisor med dokumenterad erfarenhet av IT-revisioner och kontrolltestning. Resultatet av revisionen ska redovisas i en revisionsrapport, och som på begäran ska ges in till E-legitimationsnämnden.

4.4 En utfärdare som på annan part har lagt ut utförandet av en eller flera säkerhetskritiska processer, ska genom avtal definiera vilka kritiska processer som underleverantören är ansvarig för och vilka krav som är tillämpliga på dessa, samt tydliggöra avtalsförhållandet i utfärdardeklarationen så att underleverantörens uppfyllelse av kraven för Svensk e-legitimation kan verifieras oberoende av huvudmannen.

2.5 Fysisk, administrativ och personorienterad säkerhet

5.1 Verksamhetens centrala delar ska skyddas fysiskt mot skada som följd av miljörelaterade händelser, otillåten åtkomst eller andra yttre störningar. Tillträdeskontroll ska tillämpas så att åtkomst till känsliga utrymmen är begränsad till behörig personal, att flyttbart datamedia och pappersdokument förvaras på ett säkert sätt, och att dessa utrymmen kontinuerligt övervakas för obehörigt tillträde.

5.2 Innan en person antar någon av de roller som identifierats i enlighet med 4.1a, och som är av särskild betydelse för säkerheten, ska utfärdaren ha genomfört bakgrundskontroll i syfte att förvissa sig att personen kan anses vara pålitlig samt att personen har de kvalifikationer och den utbildning som krävs för att utföra de arbetsuppgifter som följer av rollen på ett tillfredställande, korrekt och säkert sätt.

5.3 Utfärdare av Svensk e-legitimation ska bevara

a) ansökningshandlingar och handlingar som rör utlämnande, mottagande eller spärr av e-legitimationer.

b) avtal, policydokument och utfärdardeklarationer, och

c) övrig dokumentation som stöder efterlevnaden av de krav som ställs på utfärdare av Svensk e-legitimation, och som visar att de säkerhetskritiska processerna fungerar.

5.4 Tiden för bevarande ska inte understiga tio år och material ska kunna tas fram i läsbar form under hela denna tid, såvida inte krav på gallring påkallas från integritetssynpunkt och har stöd i lag eller annan författning.

5.5 En utfärdare av Svensk e-legitimation som upphör med sin verksamhet ska informera sina användare och E-legitimationsnämnden. Utfärdaren ska hålla arkiverat material tillgängligt.

2.6 Teknisk säkerhet

6.1 Utfärdare ska kunna visa att de tekniska kontroller som finns införda är tillräckliga för att uppnå den skyddsnivå som bestämts genom riskanalysen, och att dessa kontroller fungerar och är effektiva.

6.2 Kommunikation mellan systemkomponenter över allmänna telekommunikationsnät eller andra kommunikationslänkar som inte är fysiskt skyddade i enlighet med 5.1, ska begränsas och ömsesidigt identifieras med en styrka som minst motsvarar kraven för Svensk e-legitimation, samt skyddas mot insyn, manipulation och återuppspelning.

6.3 Känsligt kryptografiskt nyckelmaterial ska skyddas så att:

a) åtkomst begränsas, logiskt och fysiskt, till de roller och de tillämpningar som oundgängligen kräver det,

b) nyckelmaterialet aldrig lagras i klartext på beständigt lagringsmedia,

c) aktiveringsdata för skydd av nyckelmaterial hanteras genom flerpersonkontroll,

d) nyckelmaterialet skyddas när det inte är under användning, direkt eller indirekt, via kryptografisk hårdvarumodul med aktiva säkerhetsmekanismer mot både fysiska och logiska försök att röja nyckelmaterialet,

e) säkerhetsmekanismerna för skydd av nyckelmaterial är genomlysta och baserade på erkända och väletablerade standarder.

6.4 Utfärdaren ska kunna påvisa att tekniska säkerhetskontroller införts vid identifiering av användare och utfärdande av identitetsintyg, så att det är osannolikt att utomstående genom gissning, avlyssning, återuppspelning eller manipulation av kommunikation kan forcera skyddsmekanismerna.

6.5 Utfärdaren ska ha en dokumenterad och fungerande process for styrning och ändring av IT-system i enlighet med vedertagna principer, och som innefattar kontinuerlig omvärldsbevakning av de produkter och teknologier som används i tjänsten samt ändåmålsenlig beredskap för förändrade risknivåer.

Kvalificerade certifikat

Analys av konsekvenser om identitetsleverantörer tvingas tillhandahålla endast kvalificerade certifikat.

1 Sammanfattande slutsatser

Ett krav på att endast kvalificerade certifikat är godkända som e-legitimationer i Sverige garanterar inte en högre säkerhetsnivå än om även icke kvalificerade certifikat accepteras.

Ett krav på kvalificerade certifikat skapar stora övergångsproblem för såväl dagens utfärdare av e-legitimationer som utfärdare av tjänstelegitimationer och tvingar nuvarande e-legitimationsutfärdare att stå utanför federationen om de inte helt ändrar sin affärsmodell och avtalsstruktur.

Ett krav på kvalificerade certifikat strider mot normer som utarbetats inom EU projektet STORK om det inte kombineras med ett krav på hårda nyckelbärare (Smarta Kort).

Ett krav på kvalificerade certifikat utesluter alternativa tekniker som anses vara acceptabla inom EU projektet STORK, ex användning av koddosor och kan medföra mer långtgående krav än vad som ofta behövs i praktiken.

2 Uteslutning av e-legitimationslösningar

Ett krav på att e-legitimationer ska baseras på kvalificerade certifikat reducerar drastiskt mängden godkända e-legitimationer.

I Sverige finns bara en aktör som är registrerad som utfärdare av kvalificerade certifikat. Detta krav utesluter därför bl.a. följande övriga aktörer:

- Samtliga ramavtalsleverantörer i infratjänsten, d.v.s. e-legitimationer från BankID, Nordea, SEB, Telia, Posten och Steria. Därmed utesluts i stort sett samtliga e-legitimationer som idag accepteras av svenska myndigheter.
- Befintliga tjänstelegitimationer som ex SITHS och enskilda myndigheters e-tjänstekort (Skatteverket, Polisen m.m.)

Vidare utesluts även alternativa tekniker så som koddosor, kodkort och diverse mobiltelefonbaserade e-legitimeringslösningar som inte

är certifikatbaserade eller som av andra skäl inte knyts till ett kvalificerat certifikat.

3 Hur svårt är det att konvertera

Av lagen (2000:832) om kvalificerade elektroniska signaturer (signaturlagen) följer att kvalificerade elektroniska signaturer skapas med certifikat som ska ges ut till allmänheten (s.k. öppna system). Innebörden av detta kan sammanfattas enligt följande:

> För slutna system ska parternas avtalsfrihet respekteras i den utsträckning det är förenligt med övrig lagstiftning. Vissa svårigheter finns dock att avgöra vad som utgör slutna respektive öppna system. *Storleken på den grupp till vilken ett certifikat har erbjudits anses inte vara avgörande*. I stället kan det, enligt lagmotiven, vara rimligt att som huvudregel utgå från att *det rör sig om utfärdande till allmänheten när certifikaten avses användas vid kommunikation med andra än utfärdaren, alltså en tredje part, och det inte föreligger något kontraktsförhållande mellan utfärdaren och denne tredje part.* Anger en certifikatutfärdare att certifikaten är kvalificerade, utan att i certifikaten begränsa kretsen av möjliga mottagare på ett mer precist sätt, kan det finnas anledning att anse att certifikatutfärdaren omfattas av lagens tillämpningsområde. Den närmare tolkningen av begreppet "till allmänheten" har överlämnats till rättstillämpningen (prop. 1999/2000:117 s. 35–36).

Nuvarande e-legitimationsutfärdare är i dag bundna till en affärsmodell där man tar betalt för spärrkontroll. Detta förutsätter ett kontraktsförhållande med förlitande part och får till följd att spärrinformation inte kan tillhandahållas öppet till andra förlitande parter som inte omfattas av sådant kontraktsförhållande.

Dagens e-legitimationsutfärdares tjänster kan därför inte uppfylla kraven på att vara kvalificerade med mindre än att nuvarande affärsmodell och kontraktsförhållande med förlitande parter ändras och systemet öppnas för allmän användning.

Av 6 § signaturlagen följer vidare att ett certifikat – för att få kallas kvalificerat – ska innehålla uppgift om att det utfärdats som ett kvalificerat certifikat. Det är inte tillräckligt att certifikatutfärdaren anger detta i sin marknadsföring eller på annat sätt; det måste framgå av själva certifikatet (prop. 1999/2000:117 s. 71).

Detta innebär att även om man överger sin nuvarande affärsmodell och registrerar sig som utfärdare av kvalificerade certifikat, så kommer inte de certifikat som redan utfärdats att räknas som kvalificerade. Endast nya certifikat som innehåller uppgift om att de utfärdats som kvalificerade certifikat uppfyller rekvisiten för att vara kvalificerade.

Här finns en övergångsperiod där alla nuvarande innehavare av e-legitimationer aktivt måste ansöka om nya certifikat efter det att man övergett sin gamla affärsmodell.

Dessa problem drabbar inte bara nuvarande utfärdare av privata e-legitimationer utan drabbar lika hårt dagens tjänstekort. De certifikat som finns utfärdade på tjänstekort blir inte kvalificerade bara för att utfärdaren blir registrerad som utfärdare av kvalificerade certifikat. Innan tjänstekorten kan användas måste nya tjänstekort utfärdas alternativt förses med nya certifikat.

Sammantaget blir en konvertering av befintliga e-legitimationssystem till utfärdande av kvalificerade certifikat mycket kostsam. Detta är en kostnad som sannolikt kommer att drabba svenska myndigheter som i slutändan ska betala för användningen av dessa e-legitimationer.

4 Övergångsproblem

Det är inte rimligt att anta att alla myndigheter byter e-legitimationssystem samtidigt. Under en övergångstid tvingas dagens e-legitimationsutfärdare därför att kvarstå som utfärdare av icke kvalificerade certifikat tills alla e-tjänster har konverterat till den nya federativa infrastrukturen. Först då kan man börja om och ge ut kvalificerade certifikat. Under denna tid måste tjänsteleverantörer vara anslutna till båda systemen samtidigt.

I teorin kan e-legitimationsutfärdaren erbjuda alternativ till användarna,

1. kvalificerade certifikat för legitimering mot myndigheter som är anslutna till federationen, och/eller
2. icke kvalificerade certifikat för legitimering mot myndigheter som är anslutna till nuvarande infratjänst.

I praktiken är en sådan uppdelning mindre hållbar eftersom det blir svårt för användare att välja både vilken e-legitimation de ska skaffa och vilken e-legitimation de ska använda för legitimering mot en viss e-tjänst.

En annan övergångsmöjlighet är att godkänna icke kvalificerade certifikat under en övergångsperiod som är så lång att samtliga myndigheter och utfärdare av e-legitimationer har kunnat konvertera till att använda identitetsfederationen samt att samtliga användare har bytt ut sina e-legitimationer mot nya.

Detta är dock inte helt okomplicerat om det innebär att e-legitimationerna därmed byter tillitsnivå.

Problem uppstår även om någon av dagens utfärdare inte anser att det är tillräckligt lönsamt att registrera sig som utfärdare av kvalificerade certifikat eller om e-tjänster inte kan acceptera kostnaden för den ändrade tillitsnivån.

5 Säkerhetsvinster med kvalificerade certifikat

Identitetsfederationens hanterar kvalitetskrav på identifiering genom att definiera olika tillitsnivåer. Varje tillitsnivå definieras av en rad ingående faktorer så som krav på registrering och verifiering av användares identiteter, legitimeringstekniker och krav på nyckelbärare. De säkerhetskrav som ställs för utfärdare av kvalificerade certifikat i signaturlagen är dock allmänt hållna:

> 9 § En certifikatutfärdare som utfärdar kvalificerade certifikat till allmänheten ska bedriva verksamheten tillförlitligt och
>
> 1. ha personal med tillräcklig kompetens och erfarenhet för verksamheten, särskilt vad avser ledning, teknik och säkerhetsrutiner,
> 2. använda sådana rutiner för administration och ledning som uppfyller erkända standarder,
> 3. använda pålitliga system och produkter som är skyddade mot ändringar och se till att teknisk och kryptografisk säkerhet upprätthålls,
> 4. förfoga över tillräckliga ekonomiska medel för att kunna bedriva verksamheten enligt denna lag och bära risken för skadeståndsskyldighet,

5. ha säkra rutiner för identitetskontroll av de undertecknare som kvalificerade certifikat utfärdas till,

6. förfoga över ett snabbt och säkert system för registrering och omedelbar återkallelse av kvalificerade certifikat, och

7. vidta åtgärder mot förfalskning av kvalificerade certifikat och i förekommande fall se till att framställandet av signaturframställningsdata sker konfidentiellt.

Kraven i första stycket 3 ska anses uppfyllda för sådan maskin- eller programvara som överensstämmer med sådana standarder för produkter för elektroniska signaturer som Europeiska gemenskapernas kommission fastställt och offentliggjort referensnummer till i Europeiska gemenskapernas officiella tidning.

10 § En certifikatutfärdare som utfärdar kvalificerade certifikat till allmänheten ska

1. omedelbart återkalla ett certifikat när undertecknaren begär det eller när det annars finns anledning till det,

2. säkerställa att exakt tidpunkt kan anges för utfärdande och återkallelse av certifikat, och

3. säkerställa att av utfärdaren framställda signaturframställningsdata och signaturverifieringsdata kan användas som komplement till varandra.

Det finns inget som hindrar att identitetsfederationen ställer krav på utfärdare av e-legitimationer som motsvarar dessa krav utan att för den sakens skull kräva att e-legitimationen baseras på ett kvalificerat certifikat i lagens mening.

Därmed kan man inte förutsätta att en e-legitimation som baseras på ett kvalificerat certifikat är säkrare bara på grundval av att det är kvalificerat. Förtroendenivå avgörs av den definierade tillitsnivån.

I tillitsramverket kan federationen ställa olika krav på säkerhetsnivåer som både är högre och lägre än kvalificerade certifikat, vilket också är fallet i EU projektet STORK (se nedan under internationell samverkan). Tillitsramverket är vidare mycket mer detaljerat än lagens krav på utfärdare av kvalificerade certifikat.

En annan viktig aspekt som avgör graden av tillförlitlighet är kvaliteten på den nyckelbärare som certifikatet är kopplat till. Kravställningarna runt kvalificerade certifikat ställer inga specifika krav på nyckelbärarens kvalitet. En e-legitimation utgiven av en bank med smart kort som nyckelbärare kan anses vara mer tillförlitlig än ett kvalificerat certifikat med mjuk nyckelbärare

utfärdat av en identitetsutfärdare som inte har en tidigare relation med e-legitimationsinnehavaren.

6 Internationell samverkan

Internationell samverkan runt identifiering baseras inom ramen för dagens aktiviteter inom Europa på federationsteknik och dess ramverk för tillitsnivåer.

Inom ramen för STORK-projektet har ett ramverk definierats för tillitsnivåer med 4 nivåer som i stora drag är kompatibelt med det internationella ramverket ”Kantara Identity Asurance Framework” som även ligger till grund för de tillitsnivåer som vi avser definiera i Sverige.

Nivå 4 av STORK-projektets tillitsnivåer förutsätter kvalificerade certifikat samt hårda nyckelbärare. Nivå 3 och lägre förutsätter inte att kvalificerade certifikat används och tillåter mjuka nyckelbärare.

Det är värt att notera att det inte räcker med att ett certifikat är kvalificerat för att uppnå STORK tillitsnivå 4. Även om dagens leverantörer av e-legitimationer konverterar och ger ut kvalificerade certifikat så uppnås därmed inga fördelar inom ramen för internationell samverkan med mindre än att man även kräver att alla nyckelbärare ska vara hårda (ex smarta kort).

Enligt STORK uppfyller såväl certifikat med mjuk nyckelbärare som koddosor utan certifikat kraven för nivå 3. Även om vi i Sverige kräver kvalificerade certifikat men tillåter mjuka nyckelbärare, samtidigt som vi inte tillåter icke kvalificerade certifikat eller icke certifikatbaserade lösningar, så är vi därmed i klar disharmoni med det Europeiska ramverket eftersom vi har dragit en linje rakt igenom tillitsnivå 3.

Om Sverige vill harmonisera med STORK-ramverket så ska nivå 4 kräva kvalificerade certifikat och hårda nyckelbärare medan nivå 3 ska tillåta icke kvalificerade certifikat och alternativa autentiseringsmetoder med motsvarande säkerhetsnivå.

Om vi i Sverige inte avser kväva nivå 4 för alla e-tjänster (vilket torde vara orimligt) så måste även icke kvalificerade certifikat tillåtas i federationen om Sveriges tillitsramverk (för nivå 3) ska harmonisera med övriga Europa.

7 Juridiska frågor om säkerhetsnivå

I ett beslut den 16 oktober 2009 av Europeiska kommissionen (2009/767/EG) om åtgärder för att underlätta användningen av förfaranden på elektronisk väg genom gemensamma kontaktpunkter har kommissionen uttalat sig bl.a. angående användande av elektroniska signaturer (artikel 1). Där framgår att medlemsstaterna ska kräva att en användning av avancerad elektronisk signatur baserad på ett kvalificerat certifikat, endast om det är motiverat på grundval av en ändamålsenlig bedömning av berörda risker.

En identitetsfederation har ingen direkt koppling till elektroniska underskrifter eftersom den är till för identifiering. Krav på elektroniska underskrifter kan hanteras i en separat signeringstjänst.

Det kan därför vara mindre lämpligt att motverka eller utmönstra identifiering med alternativa metoder.

Till saken hör också att det inte någonstans i svensk lagstiftning eller författningsreglering krävs en kvalificerad elektronisk signatur (se 2 § signaturlagen där ”kvalificerad elektronisk signatur” definieras som en avancerad elektronisk signatur som är baserad på ett kvalificerat certifikat och som är skapad av en säker anordning för signaturframställning).

Hur lätt det är att blanda samman dessa begrepp framgår emellertid av bl.a. Karnovkommentaren till lagen (2005:807) om ersättning för viss mervärdesskatt för kommuner och landsting. Där sägs följande i not 15 till 9 §:

> Bestämmelsen är utformad efter mönster av 10 kap. 26 § skattebetalningslagen (1997:483) och 4 kap. 4 § lagen (2001:1227) om självdeklarationer och kontrolluppgifter, se prop. 2005/06:7, s. 29 f. Att kravet på underskrift får uppfyllas med elektroniska medel innebär att det finns en kvalificerad elektronisk signatur (kursiverat här). Detta följer av 17 § lagen (2000:832) om kvalificerade elektroniska signaturer. De aktuella blanketterna finns normalt endast som ifyllnadsbara pdf-blanketter på Skatteverkets hemsida.

Ett studium av regeringens proposition 2005/06:7 Vissa kommunalekonomiska frågor visar på samma missförstånd. Där sägs följande:

> I andra stycket anges vad som är ett elektroniskt dokument. Att kravet på underskrift ska anses som uppfyllt med elektroniska medel innebär att det finns en kvalificerad elektronisk signatur. Detta följer av 17 § lagen (2000:832) om kvalificerade elektroniska signaturer.

Påståendena är felaktiga. I 9 § andra stycket nämnda lag föreskrivs nämligen att med ett elektroniskt dokument avses en upptagning som har gjorts med hjälp av automatiserad databehandling och vars innehåll och utställare kan verifieras genom ett visst tekniskt förfarande. Denna definition kräver inte att den elektroniska signaturen ska vara kvalificerad; jfr motsvarande misstag i prop. 2001/02:25 s. 172.

En näraliggande slutsats – från juridiska och praktiska utgångspunkter – är därmed att det kan vara lämpligt att undvika en begreppsapparat som missförståtts av så många och som bygger på en teknikstyrd terminologi som genererar ständiga diskussioner och behov av klargöranden. Ett praktiskt alternativ är att bygga på sådana tillitsnivåer och anslutning till en identitetsfederation som övervägs inom detta projekt.

8 Ekonomi Affärsmodell

Identitetsutfärdare kommer att klassas i enlighet med den tillitsnivå de erbjuder och varje tjänstetyp för varje e-tjänsteleverantör kommer att deklarera vilken tillitsnivå de kräver. Det är därför väldigt enkelt att hantera flera tillitsnivåer i federationen.

Inom ramen för den fördelning av pengar som sker till identitetsutfärdare borde det finnas utrymme för olika ersättningsnivåer beroende på vilken tillitsnivå man tillhandahåller, alternativt viktad mot vilken tillitsnivå som e-tjänsten krävt.

9 Realistiska alternativ

Ett realistiskt alternativ till att kräva kvalificerade certifikat för medlemskap i federationen är att vi i Sverige definierar tillitsnivåer som harmoniserar med internationella standarder och Europeiska normer med eventuella tillägg för Svenska förhållanden inom ramen för de internationella ramverken.

Nivå 3 kan då inte kräva kvalificerade certifikat medan nivå 4 troligen gör detta i kombination med krav på hårda nyckelbärare.

Inom ramen för den upphandlingsmodell för identifieringstjänster som tas fram bör man vidare ha möjlighet att anpassa ersättningsnivå till identitetsutfärdare beroende på vilken tillitsnivå de tillhandahåller.

Teknisk sammanfattning av infrastrukturen för Svensk e-legitimation

1 Sammanfattning

Denna sammanfattning av Infrastrukturen för Svensk e-legitimation är riktad till läsare som är bekanta med federationsteknik enligt SAML 2.0 och de tekniker som i övrigt ligger till grund för utfärdande och användning av e-legitimationer för identifiering och signering.

2 Grundstruktur och skillnader mot dagens infrastruktur

Infrastrukturen för identifiering inom ramen för Svensk e-legitimation bygger på en federativ modell enligt protokollet SAML 2.0.

Detta innebär inga skillnader för utfärdande och utformning i förhållande till dagens e-legitimationer. Samma e-legitimationer som används inom nuvarande infrastruktur kommer att kunna användas inom ramen för en federativ modell.

Den stora skillnaden är att ”Service Providers” SP (i utredningen kallade E-tjänsteleverantörer) inte kommer i direkt kontakt med användarnas e-legitimationer utan istället får ett identitetsintyg i form av en SAML assertion från e-legitimationsutfärdarens Identity Provider (IdP).

I en traditionell SAML-relation innebär detta att myndigheters e-tjänster intar rollen som service provider (SP) och att e-legitimationsutfärdarna intar rollen som Identity Provider (IdP) och därmed den part för vilken användaren identifierar sig, oavsett vilken e-tjänst som användaren avser att logga in på.

Övergången från att hantera e-legitimationer direkt till att konsumera Identitetsintyg i form av SAML assertions innebär även

att de identitetsuppgifter som förmedlas till e-tjänsten kan anpassas efter e-tjänstens behov. När e-tjänsten kräver personnummer ska denna information ingå i identitetsintyget men om e-tjänsten istället kräver andra uppgifter som exempelvis organisationsnummer och ID inom organisationen kan informationen i identitetsintyget anpassas till e-tjänstens behov oavsett vilken e-legitimation som användaren använt för att legitimera sig.

För de fall där e-tjänsten behöver mer information om användaren som loggar in, exempelvis uppgift om juridisk behörighet kan en fråga ställas till en Attribute Authority – AA (I utredningen benämnd Attributsutfärdare) som genom en attribute query (attributsförfrågan) kan erhålla nödvändig kompletterande information.

Härvid kan teoretiskt sett alla typer av e-legitimationer, även de som inte innehåller några specifika personuppgifter så som koddosor för generering av engångslösenord, användas för inloggning mot en myndighet som kräver såväl personnummer som ytterligare information om juridisk behörighet.

3 Tillitsramverk och Säkerhetsnivåer

Grunden för vilken säkerhetsnivå som tillämpas när en användare legitimerar sig är den tillitsnivå som e-tjänsten kräver. För att dessa säkerhetsnivåer ska kunna vara jämförbara inom ramen för federationen definieras fyra tillitsnivåer (assurance levels) för federationen genom ett tillitsramverk. Alla IdP som utfärdar Identitetsintyg till anslutna e-tjänster måste visa att hela den process som ligger till grund för utfärdandet av identitetsintyg uppfyller kraven i den efterfrågade tillitsnivån, detta innefattar bl.a.

- Krav på utfärdandeprocessen.
- Krav på själva e-legitimationen och dess användning.
- Krav på utfärdaren av e-legitimationen.

Mer information om tillitsramverket tillhandahålls i *Bilaga 9*.

4 Metadata

För att infrastrukturen ska kunna erbjuda identifiering med hög säkerhetsnivå måste bl.a. Identitetsintyg med identitetsuppgifter signeras och krypteras från IdP till e-tjänst. Detta kräver att parterna har tillgång till varandras publika nycklar dels för verifiering av signaturer och dels för kryptering av data.

Vidare behöver e-tjänsters krav på attribut och tillitsnivåer finnas tillgängliga så att en IdP kan leverera ett identitetsintyg med lämplig information om användare till e-tjänsterna.

För att underlätta spridning av denna information på ett tillförlitligt sätt lagras sådan information i ett centralt register med s.k. metadata. Dessa metadata hålls tillgänglig för de aktörer som behöver den. Varje IdP måste ha tillgång till information om alla e-tjänster och e-tjänsterna behöver information om varje IdP och attributstjänst. Metadatainformationen tillhandahålls i signerad form, signerad av den federationsoperatör som administrerar federationen och dess tillhörande registeruppgifter.

5 Discovery service

5.1 Grundläggande syfte och funktion

Genom federationens metadata vet varje e-tjänst vilken IdP som ska identifiera en användare med en specifik typ av e-legitimation och som ska utfärda ett Identitetsintyg för användaren.

För att detta ska kunna ske måste dock e-tjänsten veta vilken e-legitimation som användaren kan och vill använda. E-tjänsten kan så som sker idag låta en användare välja vilken av alla tillgängliga e-legitimationer som användaren vill använda men detta blir opraktiskt i takt med att antalet alternativ ökar.

En discovery service (i utredningen benämnd Anvisningstjänst) kan i samarbete med varje användare komma ihåg vilken e-legitimation som användaren använt tidigare mot andra e-tjänster och därmed skapa förenklade dialoger där användarens tidigare val av e-legitimation kommer upp som förval.

Utredningen förordar att en discovery service ska erbjudas i två versioner, en där användaren omdirigeras till discovery service

enligt standardiserat SAML protokoll och ett där en dynamisk webbsida från e-tjänsten kan anpassas till användarens förval genom s.k. AJAX anrop till discoverytjänsten. Dessa alternativ finns närmare beskrivna i *bilaga 16*.

5.2 Förhållande mellan IdP och utfärdare av e-legitimation

Det är viktigt att användarens val av e-legitimation blir begriplig för användaren. Detta innebär att användaren endast ska behöva välja typ av e-legitimation för att e-tjänsten ska kunna hänvisa användaren till rätt IdP för identifiering.

Samtidigt är det viktigt att användaren inom ramen för Infrastrukturen för svensk e-legitimation känner igen sig vid varje identifieringstillfälle. Det är därför betydelsefullt att användaren alltid identifierar sig för samma IdP oberoende av vilken e-tjänst inom infrastrukturen som kräver legitimering.

Varje typ av e-legitimation från en specifik utfärdare måste vidare kopplas till ett namn på e-legitimationen som användaren känner igen och kan relatera till i det gränssnitt för val av e-legitimationer som skapas i samverkan med infrastrukturens discovery service. Detta namn återfinns även i federationens metadata för respektive IdP. Det är dessa metadata som utgör grunden för att såväl skapa val-gränssnitt för användare som att koppla användarens val till en viss IdP.

För att garantera att varje typ av e-legitimation representeras av ett för användaren begripligt namn och att detta endast kopplas samman med en IdP, är e-legitimationsutfärdaren ansvarig för definition av namn för dennes olika typer av e-legitimationer samt att specificera en och endast en godkänd IdP för vare typ av e-legitimation.

6 Integration i e-tjänster

Hantering av SAML Assertions är i dag väldigt enkelt då de stöds av en lång rad färdiga produkter och i allt större utsträckning stöds som standard i olika miljöer och verktyg för att införa webb-tjänster.

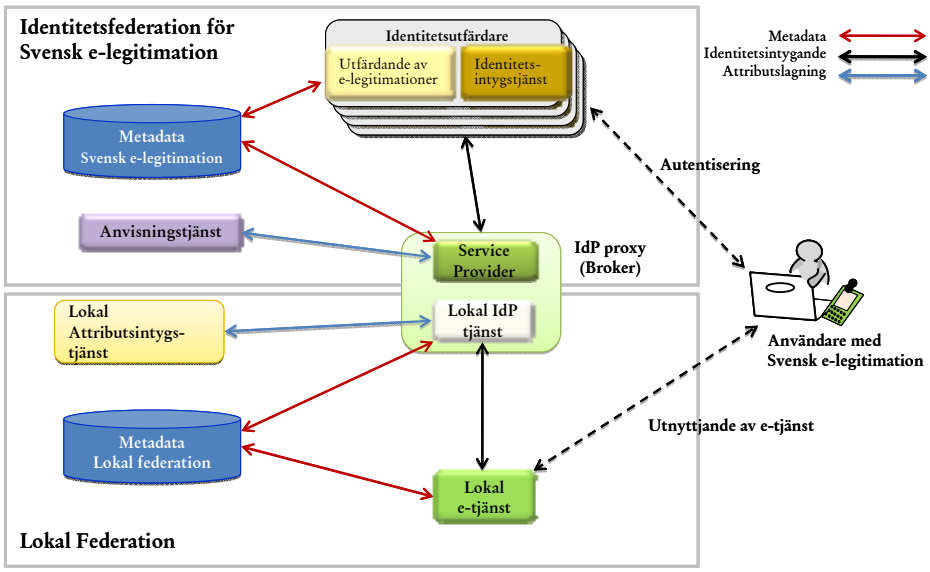
Eftersom Identitetsintyg följer ett standardiserat format behöver e-tjänster i den federativa modellen inte anpassas ytterligare om nya aktörer i egenskap av identitetsutfärdare tecknar avtal med federationsoperatören (E-legitimationsnämnden).

Integrationen av färdiga e-tjänster mot den nya infrastrukturen är därför förhållandevis enkel. För de parter som avser att skapa en ny e-tjänst, utgör integration med den federative infrastrukturen en generellt sett försumbar kostnad i jämförelse med vad det kostar att skapa själva e-tjänsten.

6.1 Integration med lokala federationer

Idag existerar många befintliga identitetsfederationer som är uppbyggda på liknande sätt som identitetsfederationen för Svensk e-legitimation. En sådan "lokal" identitetsfederation kan innefatta e-tjänster som nyttjar en IdP inom den lokala federationen för att erhålla identitetsintyg som följer lokala konventioner, men där denna e-tjänst likväl vill tillåta att användare ska kunna identifiera sig via identitetsfederationen för Svensk e-legitimering.

Detta kan enkelt lösas genom att den lokala IdP:n i den lokala federationen uppträder som en IdP Proxy enligt följande modell:



En IdP Proxy agerar som en IdP inom en lokal federation mot e-tjänster i den lokala federationen men utgör samtidigt en registrerad Service Provider (e-tjänst) i federationen för Svensk e-legitimation. En användare med Svensk e-legitimation som loggar in på en e-tjänst som är ansluten till den lokala federationen överförs till IdP Proxy som i enlighet med lokala konventioner konstaterar att användaren ska identifieras genom federationen för Svensk e-legitimation. Användaren anvisas till och identifieras av den IdP som är kopplad till användarens e-legitimation och ett identitetsintyg returneras till IdP Proxy. IdP Proxy aggregerar vid behov ytterligare information om användaren och returnerar sedan ett lokalt identitetsintyg till e-tjänsten i den lokala federationen.

För att underlätta discovery i den lokala federationen så att användaren kan ges en korrekt uppsättning val av e-legitimationer för inloggning som även inkluderar e-legitimationer som bara hanteras inom federationen för Svensk e-legitimation, kan lämplig metadata om IdP tjänster i federationen för Svensk e-legitimation inkluderas i den lokala federationens metadataregister.

7 Signering

I nuvarande infrastruktur sker signeringen i användarens klient av den information som skickas från e-tjänsten. Detta kräver dels att e-tjänsten kan skicka information som ska signeras på ett sätt som är anpassat till användarens lokala klientprogramvara och e-legitimation, dels att användarens e-legitimation är certifikatbaserad och kan användas för att skapa en elektronisk signatur enligt gällande standards.

Elektroniska signaturer som skapas i dagens modell kan endast verifieras av parter som har avtal med e-legitimationsutfärdaren för åtkomst till spärrinformation. Detta omöjliggör i praktiken för utländska myndigheter att verifiera en signatur skapad med en svensk e-legitimation.

I en ny modell där det kan förekomma e-legitimationer som inte kan användas för signering krävs en annan lösning som

- inte kräver att e-tjänsten inför anpassningar mot varje typ av e-legitimation och klientprogramvara, och
- gör det möjligt

- för alla användare att signera, även de som innehar en icke certifikatbaserade e-legitimationer, och
- för utländska aktörer att verifiera en signatur som är skapad med stöd av en svensk e-legitimation.

Utredningen har föreslagit att en central signeringstjänst ska övervägas för att tillgodose dessa behov. Olika förslag på lösningar presenteras i *Bilaga 17*.

Tekniskt ramverk

Teknisk beskrivning av infrastrukturen för Svensk e-legitimation

1 Introduktion

Det tekniska ramverket beskriver hur identitetsfederationen implementeras tekniskt. Identitetsfederationen är baserad på den internationella standarden SAML v2.0 specificerad i [SAML2Core].

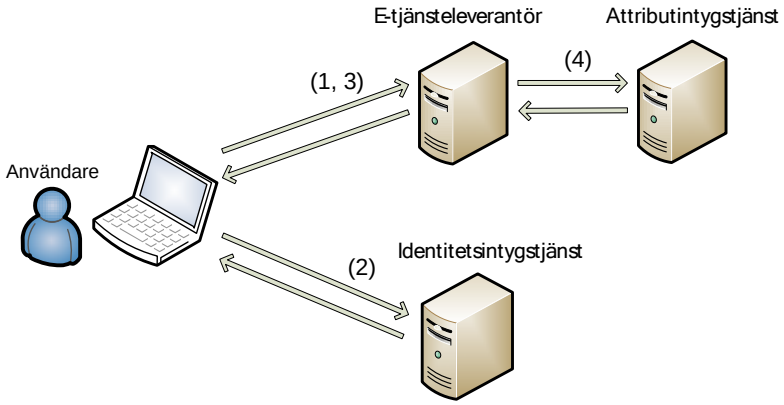
SAML är en flexibel standard som inte reglerar implementationen av aktuella identitetsfederationer på detaljnivå. För att kunna federera med SAML på ett effektivt sätt behöver ett antal vägval göras och dokumenteras. Den tekniska dokumentationen utgörs av dessa vägval och närmare reglering av hur standarden används.

Grundtanken vid framtagandet av det tekniska ramverket har varit att i så stor utsträckning som möjligt använda internationellt vedertagna tekniska profiler för federering och SAML.

2 Teknisk bakgrund

2.1 Elektroniska intyg

Det är viktigt att noggrant specificera format och innehåll för de elektroniska intyg som kommuniceras mellan identitetsintygstjänst (IdP), e-tjänsteleverantör (SP), och attributintygstjänst. Syftet är att förenkla kommunikationen mellan parter i identitetsfederationen utan att skapa onödiga begränsningar. Som bakgrund presenteras nedan det tänkta informationsflödet vid en inloggning till en webbtjänst i identitetsfederationen.



1. Användaren ansluter till e-tjänsten.

2. E-tjänsteleverantören skickar användaren vidare till ett inloggningsformulär hos identitetsintygstjänsten med hjälp av en identitetsförfrågan.

3. Efter framgångsrik autentisering utfärdas ett identitetsintyg som skickas tillbaka till e-tjänsteleverantören. Detta intyg beskrivs ingående i avsnitt 2 i attributspecifikation [AttrSpec].

4. Om e-tjänsteleverantören behöver ytterligare information om användaren kan denna hämtas från en attributintygstjänst via en attributförfrågan. Denna process beskrivs närmare i avsnitt 3 i attributspecifikationen.

Attributintyg används för att e-tjänsteleverantörer ska kunna hämta användarattribut som inte är kända för identitetsintygstjänsten. Exempel på sådana attribut kan vara organisationstillhörighet, roll, behörighetsinformation etc.

Det finns ingen teoretisk begränsning i vilken information som kan kommuniceras via attribut. Det är dock viktigt att påpeka att en attributsförfrågan skiljer sig från en auktorisationsfråga.

En attributsförfrågan besvarar frågan: ”Vilka egenskaper har detta subjekt?”

En auktorisationsförfrågan besvarar frågor av typen: ”Får detta subjekt genomföra åtgärd X”.

Rena auktorisationsfrågor kan inte besvaras med ett attributsintyg.

2.2 Tillit och metadata

Identitetsfederering via SAML är baserat på att identitetsintygsgivarna och e-tjänsteleverantörerna litar på varandra och därmed kan verifiera de signaturer som används i SAML-kommunikationen. Rent tekniskt så baseras denna tillit på att respektive parter litar på varandras URL:er och tillhörande servercertifikat.

Tillitsprocessen automatiseras via användning av SAML metadata [SAML2Meta]. Specifikationen av metadata är framtagen av OASIS för att underlätta administration av större federationer. Federationen definieras då av ett register i XML-format som är signerat med federationsoperatörens certifikat. Filen innehåller information om identitetsfederationens medlemmar inklusive deras servercertifikat. Eftersom metadatafilen är signerad räcker det med att jämföra ett servercertifikat med dess motsvarighet i metadatat.

En infrastruktur baserad på ett centralt federationsregister förutsätter att registret uppdateras kontinuerligt samt att federationsmedlemmarna alltid använder den senaste versionen av filen.

För att kunna använda metadata krävs en central aggregator som kontinuerligt hämtar lokal metadata från federationsdeltagarna och uppdaterar och signerar federationsregistret. Mjukvarukrav på hantering av lokal metadata beskrivs i federationens implementationsprofil [ImpProf].

2.3 Federationsregister

Inom identitetsfederationen används federationsregister definierade av metadatafiler publicerade av federationsoperatören. Registren kommer att innehålla följande typer av information:

- Information om identitetsintygsgivare och attributintygsgivare
- Information om e-tjänsteleverantörer, såväl offentliga som kommersiella från näringslivet.

Hantering och innehåll i metadata specificeras i [MetaSpec].

2.4 Användning av SAML

Svensk eID-federation använder SAML, version 2.0 eller högre. SAML v2.0 är en mycket omfattande standard som definierar ett antal så kallade användningsprofiler. Av de tillgängliga profilerna används följande.

- *SAML Web Browser SSO Profile* definierad i [SAML2Prof]. Profilen används för federerad autentisering mot e-tjänster.
- *SAML Assertion Query/Response Profile* definierad i [SAML2Core] och [SAML2Prof]. Profilen används för attributförfrågningar och attributsintyg.
- *IdP Discovery Profile* definierad i [IdPDisco].

Profilerna är relativt generellt hållna och lämnar många beslut öppna till de faktiska implementationerna.

3 Normativ dokumentation

Dokumenten listade i detta avsnitt reglerar normativt hur förloppen beskrivna i kapitel 1 och 2 realiseras inom svensk eID-federation. Samtliga dokument förutom SAML2Int är framtagna som del av utredningens arbete.

3.1 SAML2Int

SAML2Int är en samling av större akademiska identitetsfederationer vilka tillsammans tagit fram en profil [SAML2Int] som reglerar typisk användning av *Web Browser SSO Profile*. Istället för att göra om deras arbete väljer vi att istället peka på denna profil som riktlinje för användning av *Web Browser SSO.*

3.2 Attributspecifikation

Det är nödvändigt att specificera format och innehåll på de elektroniska intyg som skickas mellan identitetsintygstjänst, e-tjänsteleverantörer och attributintygstjänst. Detta regleras i attributspecifikationen [AttrSpec].

Attributspecifikationen pekar tillbaka på *Web Browser SSO* för hantering av identitetsintyg och *Assertion Query/Response Profile* för attributsintyg.

3.3 Specifikation av metadata

Federationen hålls samman av tre stycken federationsregister. Innehåll, uppdatering och publicering av dessa register beskrivs i specifikation av metadata [MetaSpec].

3.4 Anvisningstjänst

En anvisningstjänst tillhandahåller en tjänst till e-tjänsteleverantörer som underlättar processen att fastställa vilken identitetsintygstjänst som ska autentisera en användare. Anvisningstjänsten beskrivs närmare i [AnvTj].

3.5 Krav på mjukvara

Mjukvara som ska användas inom Infrastrukturen för Svensk e-legitimation förväntas leva upp till kraven i implementationsprofilen [ImpProf].

4 Referenser

[AnvTj] Utredningen kring bildandet av en ny e-legitimationsnämnd FI 2010:05, ”Anvisningstjänst”, 2010

[AttrSpec] Utredningen kring bildandet av en ny e-legitimationsnämnd FI 2010:05, ”Attributspecifikation”, 2010

[IdPDisco] OASIS Committee Specification, ”Identity Provider Discovery Service Protocol and Profile”, March 2008.

[ImpProf] Utredningen kring bildandet av en ny e-legitimationsnämnd FI 2010:05, ”Implementation Profile”, 2010

[MetaSpec] Utredningen kring bildandet av en ny e-legitimationsnämnd FI 2010:05, ”Specifikation av metadata”, 2010

[SAML2Core] OASIS Standard, “Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0”, March 2005.

[SAML2Int] SAML2Int, ”Interoperable SAML 2.0 Profile”, <http://saml2int.org/profile/current>

[SAML2Prof] OASIS Standard, “Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0”, March 2005

Attributspecifikation

Specifikation av innehåll och format på identitets- och attributsintyg

1 Identitetsintyg

Varje deltagande identitetsintygstjänst eller e-tjänsteleverantör i identitetsfederationen måste uppfylla de identitetsprofiler som presenteras i denna specifikation. Det står identitetsintygstjänst fritt att kommunicera ytterligare information i intygen förutsatt att intygen följer det i detta dokument fastlagda formatet.

1.1 Användningsfall

Inom infrastruktur för Svensk e-legitimation hanteras tre olika identitetsprofiler eller användningsscenarier; personlig, anonymiserad samt organisationsanknuten identitet. Nedan följer exempel på användar-fall som motsvaras av de tre identitetstyperna. Närmare specifikation av attributen ges i avsnitt 1.4.

1.1.1 Personlig identitet

Personlig identitet används när en medborgare behöver identifiera sig mot en e-tjänst med personnummer. Detta kan liknas vid inloggning med certifikatsbaserad e-legitimation innehållande personnummer.

Obligatoriska attribut: pseudonym, personnummer, namn
Valfria attribut: tillitsnivå, adress, telefonnummer, e-post

1.1.2 Organisationsidentitet

För vissa tillämpningar är det intressant att basera användarens identitet på organisationstillhörighet. Information om identitet hos den aktuella organisationen kan även kompletteras med personlig identitet (personnummer).

Obligatoriska attribut: pseudonym, organisationstillhörighet(er) och namn
Valfria attribut: personnummer, adress, telefonnummer, e-post

Flera samtidiga organisationstillhörigheter representeras i intyget som en sekvens av attribut av samma typ.

1.1.3 Pseudonym identitet

En pseudonymiserad identitet används för att skydda den personliga integriteten. En sådan identitet kan användas närhelst en e-tjänst inte kräver koppling av användaren till en specifik fysisk individ. Många enklare webbtjänster som används idag utanför offentlig sektor lämpar sig för denna typ av inloggning.

Obligatoriska attribut: pseudonym
Valfria attribut: adress, telefonnummer, e-post

1.2 Identitetsintyg

Format och hantering av identitetsintyg beskrivs i [SAML2Core].

Inom identitetsfederationen måste alla identitetsintyg av säkerhets- och anonymitetskäl skickas i krypterad form. Det är valfritt för e-tjänsteleverantörerna att signera identitetsförfrågningar men obligatoriskt att signera attributförfrågningar. Kryptering och signering sker med respektive parts publika nyckel vilken publicerats i metadata.

1.2.1 Format på identitetsintyget

Regler för utgivande av identitetsintyg ges nedan.

1. Om identitetsintygstjänsten önskar returnera ett fel ska svaret <saml2p:Response> inte innehålla någon <Assertion>.
2. Om autentiseringen är lyckad ska identitetsintyget innehålla åtminstone:

- Utfärdaren av identitetsintyget som elementet <Issuer>.
- En <Assertion> innehållande exakt en <AuthnStatement> som innehåller ett <NameId> med en persistent pseudonym. Intyget innehåller även ett flertal attribut i enlighet med avsnitt 2.1.
- Tillitsnivå kommuniceras som del av <AuthnContext> enligt specifikation i [IdAssurProf] och [AuthCtx]. Faktiska tillitsnivåer och namnrymd är definierade i tillitsramverket [TillRamverk].

Det är valfritt men rekommenderat att utöver tillitsnivå även kommunicera använd autentiseringsmetod som del av <AuthnContext>.

1.2.2 Kodning av attribut

- XML-attributet `NameFormat` på elementet `Attribute` måste vara `urn:oasis:names:tc:SAML:2.0:attrname-format:uri`
- Attributnamn måste vara en URI som beskrivet ovan.
- XML-attributet `FriendlyName` är valfritt.
- Alla attribut måste ha en OID och ska använda denna som namn.
- Alla attributvärden måste vara av typen "`xs:string`".

Ett exempelattribut formaterat enligt ovanstående regler ges nedan:

```
<saml:AttributeNameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
        Name="urn:oid:2.5.4.4" FriendlyName="displayName">
        <saml:AttributeValue xsi:type="xs:string">John
Smith</saml:AttributeValue>
</saml:Attribute>
```

1.3 Pseudonymisering

Pseudonymisering består i att ersätta identifierbar data såsom personnummer med en artificiell identifierare. Av anonymitetskäl är den unika användaridentifieraren i identitetsintyget en pseudonym.

Pseudonymen genereras av IdP baserat på EntityID för IdP, SP samt en unik användaridentifierare endast känd av IdP:n. Det är viktigt att pseudonymen är genererad på ett sådant sätt att den inte kan användas för att härleda användarens identitet.

I samtliga användarfall beskrivna i avsnitt 2.1 kommuniceras pseudonymen som SAML `NameID` i identitetsintyget.

1.4 Attributdefinitioner

Endast attribut med befintlig allokerad OID (objektidentifierare se [RFC3061]) är tillåtna. Följande obligatoriska attribut hanteras som del av identitetsintyg inom federationen.

Beskrivning	Attributnamn	OID
Personnummer*	personalIdentityNumber	1.2.752.29.4.13
Org-identifierare	orgAffiliation	Allokeras av nämnden
Namn**	displayName	2.16.840.1.113730.3.1.241
Namn (alternativ)	Sn	2.5.4.4
	givenName	2.5.4.42
Nåbarhetsadress	postalAddress	2.5.4.16
Folkbokföringsadress	Street	2.5.4.9
	postOfficeBox	2.5.4.18
	postalCode	2.5.4.17
	l	2.5.4.7
	c	2.5.4.6
Telefon	telephoneNumber	2.5.4.20
Mobil	Mobile	0.9.2342.19200300.100.1.41
Epost	Mail	0.9.2342.19200300.100.1.3

*Attributet används även för samordningsnummer [Samord].

** Fördelen med displayName är att attributet är av ”single value” typ.

1.4.1 Organisationsidentifierare

Identifieraren ska identifiera en organisation (svenskt organisationsnummer) med möjlighet att specificeras en inom organisationen lokal identifierare, t.ex. anställningsnummer eller användarnamn. Roll inom organisationen specificeras inte genom denna identifierare. Syntax:

http://id.gov.se/org/< se-org-no > [/< local-part >]

Exempel på organisationsidentifierare för en organisation med organisationsnummer 123456-7890 skulle kunna vara:

http://id.gov.se/org/123456-7890
http://id.gov.se/org/123456-7890/svensvensson
http://id.gov.se/org/123456-7890/9823

1.4.2 Egendefinierade attribut

Inom infrastrukturen för identifiering kan det uppstå behov attribut som endast några få deltagare i infrastrukturen behöver känna till. Om en attributstjänst exempelvis tillhandahåller ett attribut som är anpassat till en viss tjänst, så är det bara användare av den tjänsten som behöver känna till hur detta attribut ska hanteras.

Definition av attribut som används inom ramen för svensk e-legitimation kan därför hanteras olika beroende på attributets användningsområde:

Attribut som måste kunna hanteras av alla deltagare i infrastrukturen – Information om dessa attribut införs i infrastrukturens attributspecifikation

Attribut som är av allmänt intresse – Information om dessa attribut kan ingå i infrastrukturens attributsspecifikation men kan även definieras i separata dokument som godkänns och publiceras av e-legitimationsnämnden.

Privata attribut som bara behöver förstås av några få aktörer inom ramen för ett avgränsat användningsområde - Definition av dessa attribut kan göras oberoende av e-legitimationsnämnden. Om ett sådant attribut listas i något av federationens register (metadata) så måste dock

attributets definition godkännas och publiceras av e-legitimationsnämnden.

En aktör som behöver definiera ett nytt attribut med begränsat användningsområde kan göra så och fritt förmedla information om detta attribut till berörda parter utan att ansöka om tillstånd.

2 Attributsintyg

2.1 Användningsfall

Ett exempel på en tjänst som begagnar attributsförfrågan skulle kunna vara att Skatteverket vill låta privatpersoner se skattekonton för de företag respektive person företräder. För att ta reda på denna information gör Skatteverket en attributförfrågan till Bolagsverket.

2.2 Format på attributsintyg

Attributsintyg använder SAML-profilen *Attribute Query / Response* definierad i [SAML2Prof] och [SAML2Core].

Attributsförfrågningar använder en så kallad `<saml2p:AttributeQuery>` och attributsintyget kommuniceras inom ramen för ett `<saml2p:Response>`.

Attributförfrågningar autentiseras mot attributintygstjänsten med e-tjänsteleverantörens certifikat (enligt metadata) som klientcertifikat.

2.3 Attributdefinitioner

I denna specifikation görs ingen reglering av vilken information som får eller måste kommuniceras inom attributsintyg inom federationen.

Däremot ges i följande tabell rekommendationer för vilka faktiska attribut som bör användas för att representera vissa vanliga egenskaper. Nedanstående tabell kompletterar attributdefinitionerna i avsnitt 1.4.

Beskrivning	Attributnamn	OID
Organisationsnamn	organization	2.5.6.4
Organisationsenhet	organizationalUnit	2.5.6.5

3 Referenser

[AuthCtx] OASIS Standard, "Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0", mars 2005.

[IdAssurProf] OASIS Standard, "SAML V2.0 Identity Assurance Profiles Version 1.0", juli 2010.

[RFC3061] RFC 3061, "A URN Namespace of Object Identifiers", IETF Proposed Standard, februari 2001.

[Samord] Samordningsnummer, SKV 707, utgåva 2, Skatteverket, oktober 2006

[SAML2Core] OASIS Standard, "Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0", mars 2005.

[SAML2Prof] OASIS Standard, "Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0", mars 2005.

[TillRamverk] Utredningen kring bildandet av en ny e-legitimationsnämnd FI 2010:05, *Tillitsramverk, 2010*

Specifikation av metadata

Användning av SAML metadata för svensk eID-federation

1 Introduktion

Hanteringen av federationsregister och förtroende inom identitetsfederationen ska följa *OASIS Metadata Interoperability Profile* [MetaIOP]. Profilen är framtagen för att standardisera upprättande av förtroende via metadata. Federationsregister signeras av federationsoperatören.

1.1 Gemensamma regleringar

Attribut refererade i metadata identifieras unikt av sin OID. Obligatoriska attribut och hantering av aktörerna egendefinierade attribut beskrivs i attributspecifikationen [AttrSpec].

Såväl identitets- som attributsintyg ska både krypteras och signeras. Ingen reglering görs av identitetsförfrågningar medan attributsförfrågningar måste signeras.

För att på ett enkelt sätt garantera global unicitet för `EntityID` rekommenderas federationsaktörerna använda ett URI-baserat format involverande den egna organisationen.

1.2 Identitets- och attributintygsgivare

Utöver `EntityID` förväntas Identitetsintygsgivare kommunicera följande information via metadata i enlighet med [MetaIOP]:

- Läsbart namn som unikt identifierar e-legitimationsutfärdaren. Lämpligt attribut är `orgFriendlyName`.
- URL till tjänsten
- certifikat för SAML-kommunikation
- tillgängliga tillitsnivåer, se avsnitt 1.3.1.

Ovanstående kan kompletteras med tillgängliga attribut representerat som en sekvens av `<saml:Attribute>` element.

Attributintygsgivare behöver endast kommunicera URL samt certifikat.

1.3 E-tjänsteleverantörer

E-tjänsteleverantörer förväntas kommunicera följande information via metadata i enlighet med [MetaIOP] och [SAML2Meta]:

- Namn på e-tjänsten
- URL till tjänsten
- certifikat för SAML-kommunikation
- efterfrågade användarattribut som en sekvens av `<RequestedAttribute>` element.
- efterfrågad tillitsnivå, se avsnitt 2.3.

En e-tjänsteleverantör kan tillhandahålla flera e-tjänster förutsatt att tjänsterna har unika URL:er.

1.4 Utvidgningar av metadata

I och med att metadata används i praktiken har det uppstått ett behov av att kunna lägga in godtyckliga attribut. Detta regleras i *SAML V2.0 Metadata Extension for Entity Attributes* [MetaAttr].

1.4.1 Tillitsnivå

Nedan ges ett exempel på hur man lägger till en tillitsnivå för antingen en identitetsintygsgivare eller en e-tjänsteleverantör.

```
<EntityAttributes xmlns="urn:oasis:names:tc:SAML:metadata:attribute">
  <saml:Attribute Name="urn:oasis:names:tc:SAML:attribute:assurance-certification">
  <saml:AttributeValue>http://id.gov.se/AL_X.pdf</saml:AttributeValue>
  </saml:Attribute>
 </EntityAttributes>
```

Attributnamnet `Name` ska som i exemplet ovan vara:
urn:oasis:names:tc:SAML:attribute:assurance-certification

1.4.2 Gränssnitt

För att göra det möjligt för identitetsintygsgivare att kontrollera sin grafiska representation hos anvisningstjänsten är det möjligt att använda metadata UI extensions beskrivna i [MetaUI]. Användningen av gränssnittsutvidgningen är frivillig inom federationen.

2 Centralt register

Federationens tre register sammanställs, signeras och publiceras av federationsoperatören. Federationsoperatören ansvarar för att innehållet i respektive register är korrekt. Medlemsinformation kan inhämtas till registret med valfri metod förutsatt att äktheten kan garanteras.

För att garantera en god tillgänglighet till anvisningstjänsten rekommenderas e-tjänsteleverantörer att lagra en lokal kopia av federationsregistret för identitetsintygsgivare.

3 Referenser

[AttrSpec] Utredningen kring bildandet av en ny e-legitimationsnämnd FI 2010:05, ”Attributspecifikation”, 2010

[MetaAttr] OASIS Committee Specification, ”SAML V2.0 Metadata Extension for Entity Attributes Version 1.0”, August 2009.

[MetaIOP] OASIS Committee Specification, “SAML V2.0 Metadata Interoperability Profile Version 1.0”, August 2009.

[MetaUI] OASIS Committee Specification, “SAML V2.0 Metadata Extensions for Login and Discovery User Interface Version 1.0”, September 2010.

[SAML2Core] OASIS Standard, “Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0”, March 2005.

[SAML2Meta] OASIS Standard, “Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0”, March 2005

Implementation Profile

Software requirements for the Swedish Infrastructure for eID

This document is directly based on the InCommon implementation profile for SAML interoperability [InCommon]. Some modifications and additions have been made to adjust to special requirements of the Swedish Infrastructure for eID. The major adjustments relate to the use of pseudonyms and attribute queries.

1 Implementation profile

This profile specifies behavior and options that implementations of the SAML v2 Web Browser SSO Profile and Assertions Query/Request Profile [SAML2Prof] are required to support for use within the Swedish eID-federation. The requirements specified are in addition to the requirements of the original profiles, and readers should be familiar with all relevant reference documents. Any such requirements are not repeated here except where deemed necessary to highlight a point of discussion or draw attention to an issue addressed in errata, but remain implied.

SAML leaves substantial latitude to implementations with regard to how software is architected and combined with authentication and application infrastructure. Where the terms "Identity Provider" and "Service Provider" are used, they should be understood to include the total software footprint intended to provide the desired functionality; no specific assumptions are made as to how the required features are exposed to deployers, only that there is some method for doing so.

2 Metadata and Trust Management

Identity Provider, Service Provider, and Discovery Service implementtations MUST support the use of SAML v2.0 Metadata [SAML2Meta] in conjunction with their support of the SAML V2.0 Web Browser SSO Profile [SAML2Prof]. Additional expectations around the use of particular metadata elements related to profile behavior may be encountered in subsequent sections.

Implementations MUST support the SAML V2.0 Metadata Interoperability Profile Version 1.0 [MetaIOP]. It is OPTIONAL for implementations to support the generation, publication, or exportation of metadata, but implementations MUST support the following mechanisms for the importation of metadata:

- local file
- remote resource at fixed location accessible via HTTP 1.1 [RFC2616] or HTTP 1.1 over TLS/SSL [RFC2818]

In the case of HTTP resolution, implementations MUST support use of the "ETag" header for cache management; other cache control support is OPTIONAL. Implementations SHOULD support the use of more than one fixed location for the importation of metadata, but MAY leave their behavior unspecified if a single entity's metadata is present in more than one source.

In accordance with [MetaIOP], importation of multiple entities' metadata contained within an <*md:EntitiesDescriptor*> element MUST be supported.

Verification of metadata MUST include XML signature verification at least at the root element level, and SHOULD support the following mechanisms for signature key trust establishment:

- direct comparison against known keys
- some form of path-based certificate validation against one or more trusted root certificates and certificate revocation lists

The latter mechanism does not impose a particular profile for certificate validation, as no such profile has wide enough adoption across tools and libraries to warrant such a requirement, but should be understood as being consistent with the "usual" practices encountered in the implementation of certificate validation. Where possible, implementations SHOULD document known limitations of the mechanisms they employ.

Implementations SHOULD support the SAML V2.0 Metadata Extension for Entity Attributes Version 1.0 [MetaAttr] and provide policy controls on the basis of SAML attributes supplied via this extension mechanism.

Finally, implementations SHOULD allow for the automated updating/reimportation of metadata without substantial disruption of services.

3 Identity Provider Discovery

Service Provider and Discovery Service implementations MUST support the Identity Provider Discovery Service Protocol Profile in conformance with section 2.4.1 of [IdPDisco].

4 Pseudonyms

Identity Provider and Service Provider implementations MUST support the following SAML V2.0 name identifier formats, in accordance with the normative obligations associated with them by [SAML2Core]:

- urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
- urn:oasis:names:tc:SAML:2.0:nameid-format:transient

Support for other formats is OPTIONAL.

5 Attributes

Identity Provider and Service Provider implementations MUST support the generation and consumption of <*saml2:Attribute*> elements that conform to the MACE-Dir Attribute Profile for SAML 2.0 [MACEAttr], with the exception that the ability to support <*saml2:AttributeValue*> elements whose values are not simple strings (e.g., <*saml2:NameID*>, or other XML values) is OPTIONAL.

As a non-normative summary, this requirement primarily implies the capability to ensure the use of particular *Name* and *NameFormat* values when generating and consuming <*saml2:Attribute*> elements, rather than relying on hard-wired assumptions or proprietary sets of attribute identifiers.

6 Authentication Requests

6.1 Binding and Security Requirements

Identity Provider and Service Provider implementations MUST support the use of the HTTP-Redirect binding [SAML2Bind] for the transmission of <*saml2p:AuthnRequest*> messages, including the generation or verification of signatures in conjunction with this binding.

Because verification of signatures by Identity Providers cannot be guaranteed in deployments, Service Provider implementations MUST NOT rely on the integrity of a signed request for the enforcement of requirements derived from options such as the *ForceAuthn* attribute or the <*saml2p:RequestedAuthnContext*> element. Rather, Service Providers MUST enforce such requirements based on the content of the <*saml2p:Response*> messages they receive.

Support for other bindings is OPTIONAL.

6.2 Message Content

In addition to standard core- and profile-driven requirements, Service Provider implementations MUST support the inclusion of at least the following <*saml2p:AuthnRequest*> child elements and attributes (when appropriate):

- AssertionConsumerServiceURL
- ProtocolBinding
- ForceAuthn
- IsPassive
- AttributeConsumingServiceIndex
- <saml2p:RequestedAuthnContext>
- <saml2p:NameIDPolicy>

Identity Provider implementations MUST support all <*saml2p:AuthnRequest*> child elements and attributes defined by [SAML2Core], but MAY provide that support in the form of returning appropriate errors when confronted by particular request options. However, implementations SHOULD fully support the options enumerated above. Implementations MAY limit their support of the <*saml2p:RequestedAuthnContext*> element to the value "exact" for the Comparison attribute.

7 Authentication Responses

7.1 Binding and Security Requirements

Identity Provider and Service Provider implementations MUST support the use of the HTTP-POST binding [SAML2Bind] for the transmission of <*saml2p:Response*> messages.

Support for other bindings is OPTIONAL.

Identity Provider and Service Provider implementations MUST support the signing of <*saml2:Assertion*> elements in responses; support for signing of the <*saml2p:Response*> element is OPTIONAL.

Identity Provider and Service Provider implementations MUST support the use of XML Encryption via the <*saml2:EncryptedAssertion*> element; support for the <*saml2:EncryptedID*> and <*saml2:EncryptedAttribute*> elements is OPTIONAL.

7.2 Message Content

The Web Browser SSO Profile allows responses to contain any number of assertions and statements. Identity Provider implementations MUST allow the number of <*saml2:Assertion*>, <*saml2:AuthnStatement*>, and <*saml2:AttributeStatement*> elements in the <*saml2p:Response*> message to be limited to one.

In turn, Service Provider implementations MAY limit support to a single instance of those elements when processing <*saml2p:Response*> messages.

It is OPTIONAL for Identity Provider implementations to support the inclusion of a Consent attribute in <*saml2p:Response*> messages.

Service Provider implementations that provide some form of session semantics MUST support the <*saml2:AuthnStatement*> element's *SessionNotOnOrAfter* attribute.

8 Attribute Queries

Identity Provider and Service Provider implementations MUST support the Assertion Query/Request Profile as defined in [SAML2Prof] and [SAML2Core].

8.1 Binding and Security Requirements

Identity Provider and Service Provider implementations MUST support the use of the SOAP binding [SAML2Bind] for the transmission of attribute query and response messages.

8.2 Message Content

Identity Provider and Service Provider implementations MUST support <*saml2p:AttributeQuery*> requests with accompanying <*saml2p:Response*> and corresponding responses.

Support for other assertion request types is OPTIONAL.

9 Referenser

[RFC2616] RFC 2616, “Hypertext Transfer Protocol – HTTP/1.1”, June 1999.

[RFC2818] RFC 2818, “HTTP Over TLS”, May 2000

[IdPDisco] OASIS Committee Specification, Identity Provider Discovery Service Protocol and Profile, March 2008.

[InCommon] “InCommon Federation SAML 2.0 Profiles”, InCommon Federation Technical Advisory Committee. February 2010

[MACEAttr] MACE-Dir Working Group Publication, ”MACE-Dir SAML Attribute Profiles”, April 2008.

[MetaAttr] OASIS Committee Specification, ”SAML V2.0 Metadata Extension for Entity Attributes Version 1.0”, August 2009.

[MetaIOP] OASIS Committee Specification, “SAML V2.0 Metadata Interoperability Profile Version 1.0”, August 2009.

[SAML2Core] OASIS Standard, “Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0”, March 2005.

[SAML2Meta] OASIS Standard, “Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0”, March 2005.

[SAML2Bind] OASIS Standard, “Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0”, March 2005.

[SAML2Prof] OASIS Standard, “Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0”, March 2005.

Anvisningstjänst

Teknisk specifikation för anvisningstjänst inom infrastukturen för Svensk e-legitimation

1 Sammanfattning

Detta dokument utgör teknisk specifikation för en anvisningstjänst (Discovery Service) som upprättas inom ramen för infrastukturen för Svensk e-legitimation.

Anvisningstjänstens funktion är att underlätta användarens val av e-legitimation vid utnyttjande av en e-tjänst.

Genom anvisningstjänsten ges användaren en möjlighet att informera om vilken e-legitimation användaren brukar använda så att ett förenklat gränssnitt, där användarens tidigare använda e-legitimation kommer upp som förvalsalternativ, kan skapas vid legitimering. Användarens tidigare val av e-legitimationer kommuniceras inte med e-tjänsten utan hanteras uteslutande mellan användaren och anvisningstjänsten genom en s.k. ”cookie” som lagras i användarens webbläsare. Denna cookie innehåller ingen information om användarens aktiviteter eller identitet och anvisningstjänsten har ingen information om vilken individ som utnyttjar tjänsten för att välja e-legitimation. Genom att lagra senaste val lokalt hos användaren genom denna metod behöver inte anvisningstjänsten lagra någon information om användares senaste val i anvisningstjänsten mellan användarens nyttjande av e-tjänster.

Anvisningstjänsten tillhandahålls i två utförande. I det ena utförandet överförs användaren till anvisningstjänsten som tillhandahåller gränssnitt för användarens val av e-legitimation. I det andra utförandet tillhandahåller e-tjänsten ett eget gränssnitt mot användaren genom en dynamisk webbsida som automatiskt anpassas till tidigare val av e-legitimation genom kommunikation med anvisningstjänsten.

I detta utförande är inte tillgång till anvisningstjänsten kritisk. Om anvisningstjänsten inte är tillgänglig innebär detta bara att användaren inte får upp sin e-legitimation som förval. En e-tjänst som tillämpar det första utförandet är dock beroende av att

anvisningstjänsten är tillgänglig för användaren för att en legitimering ska kunna genomföras.

I inget utförande är det kritiskt att användaren accepterar en cookie från anvisningstjänsten. En användare som inte accepterar att lagra en cookie, eller av andra orsaker inte har en cookie med förvalsinformation lagrad, får göra ett förnyat val.

E-tjänster måste inte använda anvisningstjänsten. Ett tredje alternativ för e-tjänsten är att skapa en helt egen dialog med användaren för val av e-legitimation genom att hämta nödvändig information från federationens metadata (federationsregistret). Detta alternativ kan även kombineras med alternativ 2 så att gränssnittet fungerar även om anvisningstjänsten av någon anledning inte är tillgänglig. Det är rekommenderat att alltid använda anvisningstjänsten i någon form där detta är möjligt för att kunna erbjuda användarna ett förenklat gränssnitt.

2 Definitioner och förkortningar

Följande begrepp används som synonymer

Begrepp	Synonymer
Anvisningstjänst	Discovery Service
E-tjänst	E-tjänsteleverantör
Identitetsutfärdare	Identity Provider

Förkortningar

Förkortning	Betydelse
DS	Discovery Service (Anvisningstjänst)
SP	Service Provider (E-tjänst)
IdP	Identity Provider (Identitetsutfärdare)

3 Förutsättningar

Denna specifikation är uteslutande definierad för Anvisningstjänst inom ramen för Infrastukturen för Svensk e-legitimation. Anvisningstjänstens funktion förutsätter att varje typ av e-legitimation som representeras av ett unikt namn i användargränssnitt för val av e-legitimation representeras av en specifik IdP och att denna unika relation mellan e-legitimation och IdP är dokumenterad i federationens metadata (federationsregistret).

Anvisningstjänsten måste kunna identifiera en och endast en Identitetsutfärdare utifrån det val av e-legitimation som användaren gör. Detta innebär att användaren aldrig först ska behöva välja e-legitimation för att sedan behöva göra ytterligare att val av vilken Identitetsutfärdare som ska utföra autentisering.

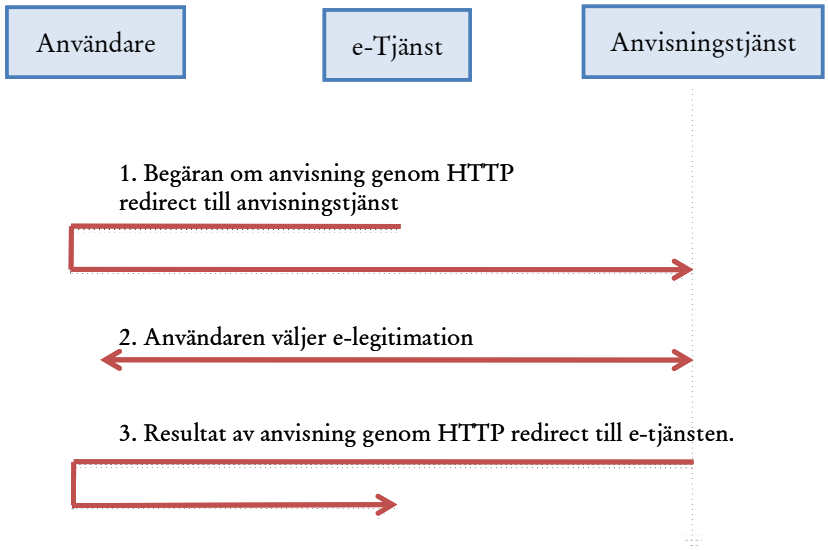
4 Utförandealternativ

Anvisningstjänst som upprättas enligt denna specifikation ska tillhandahålla tjänst till e-tjänster som underlättar processen att fastställa vilken Identitetsutfärdare som ska autentisera en användare. Anvisningstjänsten ska erbjuda tjänsten i två utförande avsedda för

1. E-tjänster som inte tillhandahåller eget gränssnitt för användarens val av e-legitimation, och
2. E-tjänster som själva tillhandahåller att gränssnitt för användarens val av e-legitimation.

5 Utförande 1 – e-tjänst utan gränssnitt för val av e-legitimation

Detta utförande av Avisningstjänsten ska implementeras enligt SAML ”Identity Provider Discovery Service Protocol and Profile” [SAML-Discovery].



Enligt detta utförande sker anvisning av Identitetsutfärdare enligt följande förfarande:

1. E-tjänsten skickar en begäran om anvisning som en HTTP Get request enligt [SAML-Discovery] till Anvisningstjänsten i en HTTP redirect.
2. Anvisningstjänsten (DS) returnerar en webbsida där användaren ges möjlighet att välja e-legitimation. Anvisningstjänsten använder federationens metadata för att fastställa vilken Identitetsutfärdare som användarens e-legitimation är kopplad till i federationen.
3. Anvisningstjänsten returnerar uppgift om Identitetsutfärdare (IdP) som en HTTP Get request enligt [SAML-Discovery] till e-tjänsten i en HTTP redirect.

Utformning av webbgränssnitt där användaren väljer e-legitimation är inte specificerad.

Avisningstjänsten bör erbjuda användarens klient en cookie enligt [rfc2965] för att spara användarens val av e-legitimation för att underlätta framtida val av e-legitimation. Denna cookie ska vara identisk med den cookie som användaren erbjuds i utförande 2 (se avsnitt 6)

Följande avgränsningar gäller för implementering av [SAML-Discovery]

Parameter	Avgränsning
isPassive	Måste vara satt till ”false” i alla request till anvisningstjänsten
returnIDParam	Ska utelämnas från request till anvisningstjänsten (Anvisningstjänsten returnerar ett ”entityID”)
return	Denna parameter ska alltid medfölja en request till anvisningstjänsten och ska identifiera den URL som anvisningstjänsten ska returnera användaren till efter val av e-legitimation.

Om anvisningstjänsten erhåller en request som bryter mot någon av reglerna ovan, eller om anvisningstjänsten av annan anledning inte kan fastställa vilken Identitetsutfärdare som användaren ska anvisas till för autentisering, så ska anvisningstjänsten returnera användaren till e-tjänsten till den URL som anges i returnIDParam, men utan att returnera någon entityID för Identitetsutfärdare.

5.1 Krav på kontroll av mottagande e-tjänst

För att förhindra att någon som inte är en registrerad e-tjänst kan vidarebefordra användaren till anvisningstjänsten för att utröna användarens val av e-legitimation så måste anvisningstjänsten kontrollera att e-tjänstens internetadress som specificeras av ”return” parametern överensstämmer med en internetadress för en legitim e-tjänst i metadataregistret.

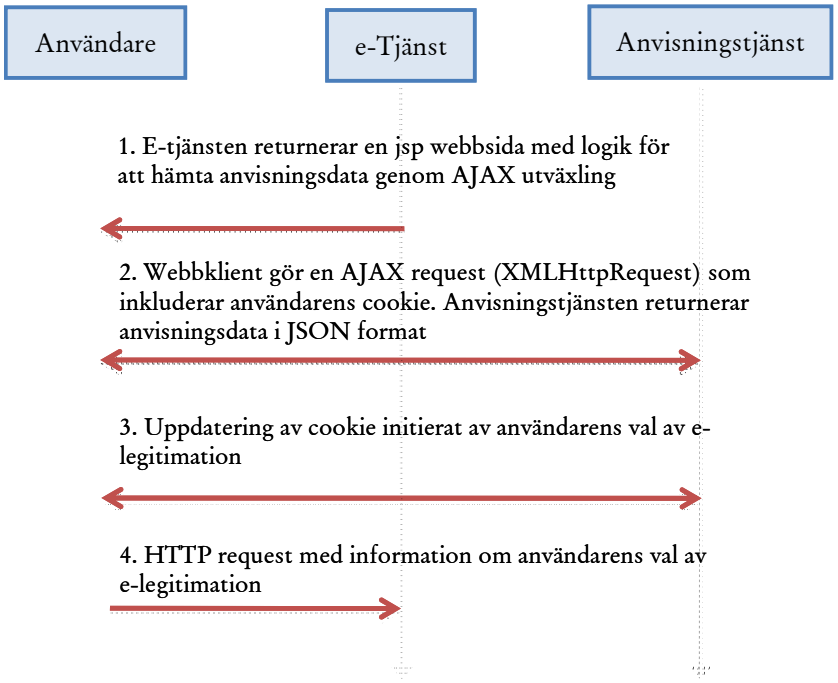
6 Utförande 2 – e-tjänst med eget gränssnitt för val av e-legitimation

Det saknas i dag någon standardiserad lösning för en Anvisningstjänst som tillhandahålls till e-tjänster som själv implementerar gränssnittet för val av e-legitimation. Den lösning som presenteras i detta avsnitt utgör ett grundförslag som beskriver en av många möjliga lösningar.

I detta utförande tillhandahåller e-tjänsten en dynamisk webbsida (Java Server Pages) för val av e-legitimation som implementerar AJAX (Asynchronous JavaScript and XML) kommunikation med anvisningstjänsten för att hämta hem anvisningsinformation i JSON (JavaScript Object Notation) format.

Då användarens webbsida hämtar JSON informationen genom AJAX anrop så skickas även användarens cookie med förvalsinformation till anvisningstjänsten som därmed anpassar den returnerade JSON informationen efter användarens förval.

Java script i den dynamiska webbsidan anpassar användarens gränssnitt för val av e-legitimation baserat på JSON informationen från anvisningstjänsten.



Enligt detta utförande sker anvisning av Identitetsutfärdare enligt följande förfarande:

1. E-tjänsten tillhandahåller en dynamisk webbsida (Java Server Pages) med AJAX instruktioner

2. Användarens webbläsare gör ett AJAX anrop (XMLHttpRequest) för att hämta ett JSON objekt med anvisningsdata. Användarens cookie med information om användarens preferenser (om sådan finns) medföljer anropet. JSON objektet anpassas av anvisningstjänsten utifrån användarens preferenser. Användarens gränssnitt skapas utifrån mottagen information från anvisningstjänsten.
3. Användarens val initierar uppdatering av användarens cookie med information om användarens senaste val.
4. Ett HTTP request skickas till e-tjänsten med information om vilken Identitetsutfärdare som ska legitimera användaren.

6.1 Cookie format och användning

Cookie med information om användarens preferenser konsumeras endast av anvisningstjänsten. Det är upptill anvisningstjänsten att utforma cookie så att den tillhandahåller nödvändig information men ska utformas i enlighet med RFC 2965 [rfc2965].

För det fall en användare använder flera e-legitimationer, eller samma webbläsare används av flera användare med olika e-legitimationer, ska en cookie kunna lagra information om flera valda e-legitimationer.

Livslängd för cookie ska sättas så att den består mellan en typisk användares utnyttjande av e-tjänster. Detta bör inte överstiga en tid av tre månader.

En cookie bör innehålla information om tidpunkt för senaste val av respektive e-legitimation så att ett förval kan tas bort om denna e-legitimation inte används mer men att cookien ändå förnyas regelbundet genom val av annan e-legitimation.

6.2 Format för JSON data

Format för JSON data måste följa ett väl definierat format så att e-tjänsters dynamiska webbsidor kan tolka informationen från anvisningstjänsten och dynamiskt uppdatera användarens gränssnitt.

Detta format bör utarbetas och vid behov uppdateras av e-legitimationsnämnden i samråd med federationens e-tjänster.

7 Referenser

[SAML-Discovery]	Identity Provider Discovery Service Protocol and Profile, OASIS Committee Specification 01, 27 March 2008
[HTTP]	RFC 2616, ”Hypertext Transfer Protocol -- HTTP/1.1”, IETF Draft Standard, June 1999.
[TLS]	RFC 5246, ”The Transport Layer Security (TLS) Protocol Version 1.2”, IETF Proposed standard, August 2008.
[RFC2965]	RFC 2965, ”HTTP State Management Mechanism”, IETF Proposed Standard, October 2000.

Central signeringstjänst

Central signering för myndigheters e-tjänster med stöd av identitetsfederationen för svensk e-legitimation

1 Sammanfattning

Detta dokument beskriver en möjlig utformning av en svensk central signeringstjänst som kan användas av svenska myndigheter och offentlig sektor för att låta användare av Svensk e-legitimation signera elektroniska handlingar.

Den lösning som beskrivs är avsedd att om möjligt skapa kvalificerade elektroniska signaturer enligt svensk lag (2000:832) om kvalificerade elektroniska signaturer. Syftet är inte att ta ställning till om detta är ett nödvändigt krav för svenska myndigheter, utan för att beskriva vad som krävs för att detta ska kunna realiseras.

Materialet i detta dokument har som syfte att fungera dels som beslutsunderlag men även som arkitekturförslag för ett implementeringsprojekt. Ytterligare tekniska specifikationer krävs för en komplett specificerad lösning.

En viktig slutsats är att de krav som identifierats för en signeringstjänst inte kan uppfyllas av en och samma utförande av signeringstjänsten. Därför beskrivs två alternativa utföranden med respektive fördelar och nackdelar. Ytterligare utredning av myndigheters och offentlig verksamhets behov krävs för att besluta om inget, ett eller båda dessa alternativa utföranden ska implementeras.

Som ytterligare del i ett sådant beslutsunderlag bör tillfogas myndigheters och offentlig verksamhets behov av elektroniska signaturfunktioner där detta ställs mot alternativa lösningar, som exempelvis att en användare godkänner information enbart genom legitimering, utan att signera informationen.

För det fall att inget av de föreslagna alternativen bedöms vara genomförbara förs en diskussion om möjliga övriga alternativ med begränsad funktionalitet som kan realiseras inom ramen för en federativ infrastruktur för identifiering.

Denna tekniska del av utredningen av en signeringstjänst tar inte ställning till hur många signeringstjänster som ska kunna finnas, affärsmodeller eller olika konkurrensaspekter.

2 Terminologi

2.1 Synonymer

Följande termer används med gemensam innebörd:

- elektronisk underskrift, underskrift, elektronisk signatur, signatur och avancerad elektronisk signatur
- dokument, handling och information

2.2 Begrepp

I detta dokument används följande begrepp:

Begrepp	Betydelse
Hash	Även ofta benämnt ”fingeravtryck” är en kontrollsekvens av data som beräknas från ett dokument med hjälp av en hashalgoritm. Hashalgoritmer är så beskaffade att ett varje dokument har ett unikt hash. När ett dokument signeras så är det dokumentets hash som signeras och inte själva dokumentet.
Elektronisk signatur	Data, knutet till ett elektroniskt dokument som kan användas för att verifiera vem som signerat dokumentet och att dokumentet inte förvanskats. **Not:** Det generella begreppet ”elektronisk signatur” används i detta dokument ekvivalent med begreppet ”avancerad elektronisk signatur” enligt signaturlagen [Sig].
Certifikat	Data som utfärdats till en användare och signerats av en certifikatutfärdare vars användningsområde i detta dokument är begränsat till att verifiera en användares signaturer. Certifikatet innehåller information om användarens identitet, nyckel för att verifiera användarens signaturer samt information om certifikatets användningsområde. **Not:** Det finns certifikat som har andra användningsområden än signaturverifiering men i detta

	dokument diskuteras endast certifikat som används för att verifiera innehavarens elektroniska signaturer.
Kvalificerat certifikat	Ett certifikat som utfärdats som kvalificerat certifikat i enlighet med signaturlagen [Sig]. Kvalificerade certifikat ställer särskilda krav på utfärdare och dess ansvar för utfärdade certifikat
Säker signeringsfunktion	En kryptografisk modul för skapande av elektroniska signaturer som uppfyller signaturlagens [Sig] krav på en ”säker anordning för signaturframställning”.
Kvalificerad elektronisk signatur	En elektronisk signatur enlig definition ovan som framställts av en säker signeringsfunktion och som kan verifieras med ett kvalificerat certifikat
Tidsstämpel	Kryptografiska data knutet till ett elektroniskt dokument som intygar att ett dokument existerade i ett specifikt utförande vid en specificerad tidpunkt. **Not:** Det dokument som tidsstämplas innefattar vanligtvis även en elektronisk signatur. På så sätt intygar tidsstämpeln såväl att dokument som dess signatur existerade vid den specificerade tidpunkten.

3 Nulägesanalys

I dagsläget kan myndigheter låta en användare signera elektroniska handlingar med sin e-legitimation. Vid detta förfarande signerar användaren den elektroniska handlingen lokalt i sin dator med hjälp av sin egen e-legitimation. E-tjänsteleverantören ombesörjer kommunikation med klienten som resulterar i att användaren accepterar och signerar en elektronisk handling.

Inom den så kallade ”Infratjänsten” tillhandahålls ett gemensamt gränssnitt OSIF (Offentligt Sammanhållen Identifierings Funktion) mot e-legitimationsutfärdarna för att underlätta legitimering och signering med användarnas e-legitimation. Vid tillämpning av OSIF-protokollet för signering skickas den information som ska signeras först till OSIF-servern för att anpassas till respektive typ av klientprogramvara som ombesörjer signering i användarens dator. Om denna OSIF-server tillhandahålls av en extern infratjänst så innebär detta att alla dokument som signeras passerar en central tjänst. I ett senare led av signeringen verifierar samma OSIF-server att användarens signatur överensstämmer med den information som e-tjänsten begärde få signerad.

Även om OSIF-protokollet är gemensamt för samtliga aktuella utfärdare av e-legitimationer så skickas olika data i skilda dataformat beroende på vilken klientprogramvara som installerats i användarens dator. Detta innebär att dagens tillämpning av OSIF-protokollet är direkt knuten till den funktionalitet och de dataformat som nuvarande klientprogramvaror kräver.

Elektronisk signering enligt denna modell innebär sammanfattningsvis följande:

- Signeringen sker i användarens dator
- Endast de e-legitimationer som är certifikatbaserade kan användas för signering. Andra former av e-legitimationer, ex kryptografiska kod-dosor, kan inte användas.
- Användare måste ladda hem en särskild programvara som ombesörjer signering av information som skickas från e-tjänsten, en s.k. klientprogramvara. Nuvarande protokoll för att understödja e-tjänsters hantering av legitimering och signering är knuten till nuvarande klientprogramvaror.
- Verifiering av användares elektroniska signatur förutsätter teknisk anpassning mot samt avtal med e-legitimationsutfärdarna. Den information om spärrning av certifikat som krävs för en oberoende verifiering av signatur, är inte öppet tillgänglig. Detta innebär exempelvis att signaturer inte kan verifieras av utländska aktörer som saknar avtal med e-legitimationsutfärdarna.
- Vid tillämpning av OSIF-protokollet mot en central OSIF-server så görs handlingen som ska signeras tillgänglig för en central tjänst.

I en framtida infrastruktur för Svensk e-legitimation som bygger på en SAML baserad federativ modell, innebär detta en rad problem:

- Den nuvarande modellen för signering är i grunden knuten till dagens leverantörer av e-legitimationer och kan inte med automatik utökas till att omfatta nya typer av e-legitimationer, särskilt inte de där användaren inte innehar certifikat för signering. Det finns visserligen leverantörer inom dagens Infratjänst som kan stödja legitimering och signering även med andra utfärdare av certifikatbaserade e-legitimationer, men detta kräver tillpassningar i de e-tjänster som ska acceptera e-

legitimationerna vilket försvårar anslutning av nya e-legitimationer.

- Den nuvarande modellen bygger på infrastruktur-komponenter och tjänster som inte återfinns i den federativa modellen. Fortsatt signering enligt nuvarande modell innebär därför att man tillämpar två olika infrastrukturer med olika affärsmodeller, dvs. en federativ modell för identifiering och den nuvarande infrastrukturen för signering.
- Den nuvarande modellen tillåter inte att vem som helst, som inte har avtal med e-legitimationsleverantörerna, kan verifiera elektroniska signaturer. Dessa signaturer kan därför inte användas exempelvis vid internationell informationsutväxling.

De mest signifikanta skillnaderna mellan en central signeringstjänst enligt avsnitt 0 och dagens modell och är att:

- Användaren behöver inte installera någon specialkonstruerad klientprogramvara. Hela processen att signera kan utföras med en vanlig webbläsare.
- Innehavare av alla typer av e-legitimationer ges möjlighet att skriva under elektroniskt. Även användare som inte innehar certifikatbaserade e-legitimationer[1].
- Nya e-legitimationsutfärdare kan adderas till infrastrukturen utan att tillpassning av protokoll och implementering i e-tjänster.
- Alla enheter som kan hantera en e-legitimation och en webbläsare kan användas för signering, ex mobiltelefoner.
- Signaturer kan skapas som kvalificerade elektroniska signaturer och signaturerna kan verifieras av oberoende tredje part som inte har avtal med e-legitimationsutfärdarna.
- Även de som inte har förlitandeavtal gentemot e-legitimations-utfärdarna kan verifiera underskriften på signerade handlingar.

[1] Användare använder endast sin e-legitimation för att legitimera sig mot signeringstjänsten som utför själva signeringen. Det som är avgörande är den tillitsnivå som e-legitimationen erbjuder, inte vilken teknik den tillämpar för legitimeringen.

4 Central signering och kvalificerade elektroniska signaturer

En central fråga för beslut om genomförande är om en central signeringstjänst kan uppfylla signaturlagens krav på en kvalificerad elektronisk signatur.

De mest relevanta kraven i detta hänseende utgörs av 3 § signaturlagen gällande ”Säkra anordningar för signaturframställning”

> **3 §** En anordning för signaturframställning som anges vara säker ska säkerställa att signaturen är tillfredsställande skyddad mot förfalskning.
>
> Anordningen ska även säkerställa att signaturframställningsdata
> 1. i praktiken kan förekomma endast en gång,
> 2. med rimlig säkerhet inte kan härledas, och
> 3. på ett tillfredsställande sätt kan skyddas av den behörige undertecknaren, så att andra inte kan komma åt eller använda dem.
>
> Anordningen får inte förändra de uppgifter som ska signeras elektroniskt eller hindra att de presenteras för undertecknaren före den elektroniska signeringen.

Den viktigaste frågeställningen i detta sammanhang är om signaturframställningsdata (privat signeringsnyckel) i en central signeringstjänst kan skyddas av den behörige undertecknaren, så att andra inte kan komma åt eller använda dem.Uppfyllelse av detta och övriga krav underlättas av om användarens privata signeringsnyckel, så som föreslås, endast existerar vid signeringstillfället i en för ändamålet säker hårdvara samt att signeringsnyckeln förstörs direkt efter användning. En sådan hårdvara utformasäven på ett sådant sätt att signaturnyckeln inte kan läsas ut ur hårdvaran.

Vid ett sådant förfarande bygger kravuppfyllelse på att signeringssystemet på ett betryggande sätt kan legitimera användaren vid signeringstillfället och därmed på ett rimligt sätt säkerställa att ingen annan än användaren själv kan signera i användarens namn med hjälp av signeringstjänsten.

För att belysamöjligheterna för en central signeringstjänst att tillgodose detta krav är det relevant att jämföramöjligheterna med en central signeringslösning i förhållande till en traditionell lokal lösning där själva signaturframställningen sker i användarens dator eller motsvarande lokal enhet (ex mobiltelefon).

Båda lösningarna kräver att användaren som ska signera har tillgång till sin e-legitimation. Skillnaden ligger i att lokal signering bygger på att användarens datormiljö ger ett tillförlitligt skydd mot missbruk medan den centrala signeringstjänsten bygger på att den centrala signeringsmiljön kan ge ett skydd i minst motsvarande grad.

Största hotet mot användarens lokala miljö utgörs av att skadlig kod (virus, trojaner, maskar mm) som användare installerat av oaktsamhet, eller som på annat sätt infiltrerat användarens dator kan ha potential att missbruka användarens signeringsfunktion. Detsamma gäller dock även i motsvarande grad en fientlig programvaras möjlighet att missbruka användarens e-legitimation vid legitimering mot en signeringstjänst. Dock finns många fler möjligheter att uppdaga problem av detta slag vid en central signeringstjänst, dels genom att legitimering vid signering loggas både av identitetsutfärdare som utfärdar identitetsintyget och av signeringstjänsten som legitimerar användaren samt möjlighet att bekräfta signering genom separat kanal, ex genom e-post eller SMS.

Följande tabell redovisar en samanställning av olika säkerhetsaspekter och hot samt en uppskattning av vilken lösning (lokal eller central signering) som erbjuder fördelar (+) respektive sämre förutsättningar (-).

	Fördelar och nackdelar	
Uppgift	**Lokal signering**	**Central signering**
Beroende av en trovärdig central signeringsfunktion	+	-
Hot från virus och annan fientlig programvara i användarens dator	-	+ (p.g.a. bättre spårbarhet)
Förhindrande av attlagrad signeringsnyckel missbrukas	-	+ (raderas efter signering)
Möjlighet att spåra vad som hänt genom loggar och trovärdig registrering av tidpunkt för signering	-	+
Möjlighet att spärra enskilda	-	+

signaturer vid missbruk		
Tredje parts bevittnade av användarens acceptans att signera presenterad handling	-	+ vid alternativ 1
Möjlighet att underrätta användaren om signering genom meddelande i separat kanal	-	+

4.1 Internationella krav

Tjänstedirektivet från EU kommissionen ställer krav på elektroniska tjänster som ska verka över landsgränser. Inom ramen för tjänstedirektivet kan medborgare behöva kommunicera elektroniskt signerade handlingar. Inom ramen för EU kommissionens stödjande aktiviteter för att underlätta utbyte av elektroniskt signerad information i samband med tjänstedirektivet har EU kommissionen i samverkan med medlemsstaterna utfärdat ett kommittologibeslut (”Kommissionens Beslut 2010/425/EU av den 28 juli 2010 om ändring av beslut 2009/767/EG”). I artikel 1 av detta beslut (som står oförändrat sedan 2009/767/EG) framgår följande:

> ”Om det är motiverat på grundval av en ändamålsenlig bedömning av berörda risker och i enlighet med artikel 5.1 och 5.3 i direktiv 2006/123/EG, får medlemsstaterna kräva att tjänsteleverantören för fullgörandet av vissa förfaranden och formaliteter genom de gemensamma kontaktpunkterna i enlighet med artikel 8 i direktiv 2006/123/EG ska använda avancerade elektroniska signaturer baserade på ett kvalificerat certifikat, **med eller utan en säker anordning för skapande av signaturer**, enligt vad som fastställs och regleras genom direktiv 1999/93/EG.”

Genom detta beslut framgår tydligt att grunden för internationell samverkan i fråga om signerade handlingar utgörs av elektroniska signaturer baserat på kvalificerade certifikat men att kravet på en säker anordning för skapande av signaturer inte är obligatoriskt.

Man kan därför förvänta sig at en lösning för elektroniska signaturer med central signeringstjänst enligt detta dokument kan fylla in viktig funktion inom ramen för införande av

tjänstedirektivet även om vi i Sverige inte väljer att godkänna den centrala signeringstjänsten som en säker anordning för skapande av signaturer i enlighet med avsnitt 4.

De signaturer som skapas inom ramen för dagens infratjänst kan endast verifieras av de myndigheter som är anslutna till infratjänsten (har förlitande avtal med e-legitimationsutfärdarna och därmed tillgång till aktuell spärrinformation). Detta gör dagens signaturlösning, eller motsvarande lösning där dokument signeras lokalt i användarens dator med e-legitimationer från dagens ramavtalsleverantörer, olämplig för utväxling av elektroniskt signerade handlingar inom ramen för internationell samverkan.

EN stor fördel i detta hänseende med en central signeringstjänst kombinerat med en federativ infrastruktur för identifiering är främst om befintliga e-legitimationer signaturerna kan användas internationellt genom att signaturerna kan kopplas till ett kvalificerat certifikat samt genom att certifikatens spärrinformation är öppet tillgänglig.

En viktig förutsättning för detta är att signeringstjänstens certifikatutfärdarfunktion kan godkännas och registreras hos PTS och att tjänsten tas med i Sveriges lista över certifikatutfärdare. Vad gäller möjligheten att ge ut kvalificerade certifikat baserat på nycklar som genererats centralt av certifikatutfärdaren, eller att identifiera den som ansöker om ett certifikat med hjälp av medel som i sig inte utgörs av kvalificerade certifikat så finns klart stöd från både internationell standard såväl som implementationer i Europa. Den allmänt accepterade standarden för utgivning av kvalificerade certifikat ETSI TS 101 456 [TS101456] ger tydligt utrymme för en sådan utfärdandeprocess.

5 Krav

Följande kravlista har utgjort grunden för utformning av en signeringstjänst. Kravlistan är utarbetad inom ramen för utredningen om bildandet av en e-legitimationsnämnd och är resultatet av såväl diskussioner inom utredningen som diskussioner med representanter från myndigheter och offentlig verksamhet.

- Användarna ska kunna signera dokument med en standard dator och en standard webbläsare som kör under marknadens vanligt

förekommande operativsystem (Windows, Mac OSX, Linux, Symbian, Android, iPhone, Blackberry, m.m.).

- E-tjänster ska kunna få tillgång till signeringstjänsten för att låta användare underteckna elektroniska dokument med minimala anpassningar av sin e-tjänst.
- E-tjänster måste kunna signera dokument som innehåller data enligt interna format som inte kan visas direkt i användarens webbläsare.
- E-tjänster måste kunna signera data som inte delges annan än användaren själv. I dessa fall får inte den signerade handlingens innehåll överföras till signeringstjänsten.
- Anslutna e-tjänster ska inte behöva befatta sig med skapande av elektronsikt signerade handlingar. Följande hantering ska kunna överlåts till signeringstjänsten:
  - Presentation av handlingen som ska signeras
  - Presentation av innebörden av att signera
  - Användarens godkännande av att signera handlingen
  - Utfärdande av signeringscertifikat[2]
  - Signering av elektronisk handling
  - Tidstämpling av dokument och signatur
  - Framställa signerad handling enligt överenskommet signaturformat
- Signaturen ska om möjligt kunna uppfylla lagens krav på en kvalificerad elektronisk signatur.

[2] Det är nödvändigt att signeringstjänsten utfärdar certifikat eftersom dessa kopplas till den signeringsnyckel som signeringstjänsten skapar för användaren. Dessa certifikat konkurrerar inte med andra certifikat på marknaden då dess enda funktion är att användas för att verifiera den specifika signatur som skapas. Eftersom signaturnyckeln förstörs efter signering kan certifikatet inte kopplas till eller användas för andra ändamål.

6 Användningsfall

Användningsfallen nedan är hypotetiska framtidsscenarier och utgör inte nödvändigtvis en korrekt beskrivning av de myndigheters e-tjänster som nämns. Dess syfte är uteslutande att beskriva situationer som belyser olika tillämpningar av en central signeringstjänst.

6.1 Signering av handling från e-tjänst som presenteras av signeringstjänsten

Anna besöker Skatteverkets webbplats för att deklarera. För att komma åt deklarationstjänsten loggar Anna in på skatteverkets webbplats med sin e-legitimation.

När alla uppgifter matats in vill Anna godkänna sin deklaration. Skatteverkets webbplats skapar då ett elektroniskt dokument som innehåller Annas deklaration med alla lämnade uppgifter införda varefter Anna dirigeras om till signeringstjänsten.

I signeringstjänsten får Anna information av att Skatteverket vill att Anna ska skriva under sin deklaration elektroniskt. Deklarationen som sammanställts av Skatteverket visas upp för Anna som kan gå igenom uppgifterna med sin webbläsare.

Anna väljer funktionen ”Jag skriver under” hos signeringstjänsten varvid Anna dirigeras till sin Identitetsutfärdare för legitimering för underskrift. Anna godkänner underskriften genom att legitimera sig med sin e-legitimation.

Dokumentet signeras av signeringstjänsten och förses med en kvalificerad elektronisk signatur enligt det signaturformat som e-tjänsten begärt.

Anna returneras tillbaks till skatteverkets webbtjänst (via signeringstjänsten) som meddelar att deklarationen nu är underskriven.

6.2 Signering av handling från e-tjänst som presenteras av e-tjänsten

Johan besöker Försäkringskassans webbplats och loggar in för att ansöka om föräldrapenning.

Försäkringskassans webbplats presenterar information som ska undertecknas varvid Johan accepterar att skriva under elektroniskt med sin e-legitimation genom funktionen ”Jag skriver under”.

Johan dirigeras till sin Identitetsutfärdare som begär legitimering för underskrift. Johan godkänner underskrift genom att legitimera sig med sin e-legitimation.

Johan returneras till Försäkringskassan med en signatur som framställts av signeringstjänsten. Försäkringskassan meddelar att ansökan har signerats.

6.3 Signering av handling vald av användaren

Petter ska signera en ansökan om tillstånd att få leverera tjänster i Portugal. Petter har fyllt i ett formulär som sparats i PDF format.

Petter kontaktat signeringstjänsten och presenterar det dokument som ska signeras samt väljer att dokumentet ska tidsstämplas.

Signeringstjänsten presenterar via webbgränssnitt det dokument som kommer att signeras. Petter verifierar dokumentet och väljer funktionen ”Jag skriver under” varvid Petter dirigeras till sin Identitetsutfärdare för legitimering för underskrift. Petter godkänner underskriften genom att legitimera sig med sin e-legitimation.

Petter returneras till signeringstjänsten där Petter får ladda hem det signerade dokumentet som försetts med en kvalificerad elektronisk signatur samt en kryptografisk tidsstämpel.

Utförandealternativ

För att uppfylla alla funktionella krav måste signeringstjänsten ha utförandealternativ som både kan hantera fall där presentation av information som ska signeras hanteras av signeringstjänsten och fall där detta hanteras av e-tjänsten.

I detta avseende innefattar hanteringen av information som ska signeras:

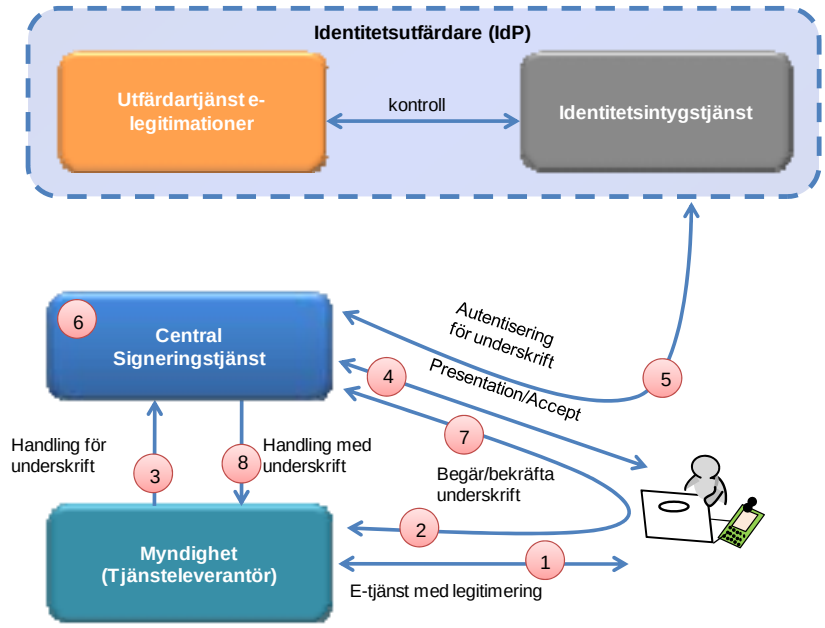
- Presentation av information som ska signeras
- Presentation av innebörden av att signera (detta kan framgå av informationen som signeras eller genom annan information)
- Funktion genom vilken användaren kan acceptera

För att uppfylla dessa krav presenteras två olika utförandealternativ som presenteras i detta avsnitt.

Utförandealternativen representerar främst skillnader mellan användningsfallen i avsnitt 6.1 och 6.2. Användningsfallet i avsnitt 6.3, där handlingen som signeras väljs av användaren, går att realisera inom ramen för båda alternativen genom att skapa en tjänst där användaren kan ladda upp ett dokument som ska signeras. Denna tjänst kan fylla funktionen av en e-tjänst i enlighet med både alternativ 1 och alternativ 2.

6.4 Alternativ 1 – Dokument som ska signeras hanteras av signeringstjänsten

I detta alternativa utförande överlåter e-tjänsten hela signeringsförfarandet till signeringstjänsten.



4. Användaren identifierar sig för en e-tjänst genom sin e-legitimation och utnyttjar en tjänst som kräver användarens elektroniska underskrift (signatur)
5. Användaren överförs till signeringstjänsten med en begäran om signering från e-tjänsten.
6. Signeringstjänsten inhämtar elektronisk handling för underskrift från e-tjänsten.
7. Signeringstjänsten presenterar handlingen som ska signeras för användaren och användaren accepterar att signera
8. Användaren överförs till sin identitetsutfärdare med begäran om legitimering. Användaren legitimeras med stöd av sin e-

legitimation och ett identitetsintyg returneras till signeringstjänsten.

9. Signeringstjänsten skapar användarens nyckelpar, utfärdar ett certifikat för användaren samt signerar den elektroniska handlingen. Vid behov tidsstämplas handlingen. Handling med underskrift skapas genom att foga samman handlingen med certifikat, signatur och eventuell tidsstämpel enligt efterfrågat signaturformat.
10. Användaren returneras till e-tjänsten med en bekräftelse på att handlingen är underskriven.
11. E-tjänsten hämtar hem den signerade handlingen från signeringstjänsten från angiven plats.

Genom detta förfarande kan en e-tjänst få tillgång till en signeringsfunktion som enkelt kan integreras med en e-tjänst med minimala insatser. En viktig fördel är att en tredje part (Signeringstjänsten) står som garant för att användaren verkligen accepterat att signera handlingen och att den information som användaren fått presenterat för sig och accepterat överensstämmer med den signatur som skapats. En annan fördel är att signeringstjänsten kan hantera alla de olika signaturformat som kan komma i fråga, särskilt om signaturen ska kunna användas/verifieras internationellt.

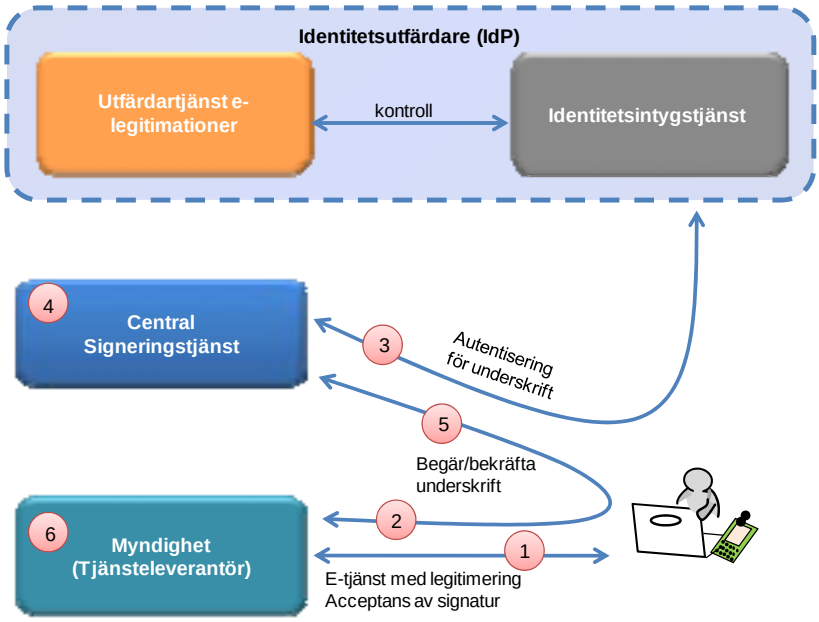
Den stora nackdelen med detta alternativ är att den handling som ska signeras måste hanteras av signeringstjänsten. Detta alternativ kan därför inte tillämpas om:

- E-tjänsten av något skäl inte kan eller får lämna ut handlingen som ska signeras till signeringstjänsten
- Handlingen som ska signerats inte förekommer i ett format som signeringstjänsten kan presentera för användaren på ett för användaren meningsfullt sätt endast med stöd av användarens webbläsare.

Då någon av dessa omständigheter gäller för signeringen så måste alternativ 2 tillämpas.

6.5 Alternativ 2 – Dokumentet som ska signeras hanteras av e-tjänsten

I detta alternativa utförande av signeringstjänsten hanterar signeringstjänsten inte den elektronisk handling som ska signeras. Gränssnittet mot användaren vid signering hanteras i sin helhet av signeringstjänsten



1. Användaren identifierar sig för en e-tjänst genom sin e-legitimation och utnyttjar en tjänst som kräver användarens elektroniska underskrift (signatur). E-tjänsten presenterar den elektroniska handling som ska signeras för användaren och användaren accepterar att skriva under handlingen.
2. Användaren överförs till signeringstjänsten med en begäran om signering från e-tjänsten. Begäran om signering innehåller bl.a. en hash representation av dokumentet som ska signeras.
3. Användaren överförs till sin identitetsutfärdare med begäran om legitimering. Användaren legitimeras med stöd av sin e-legitimation och ett identitetsintyg returneras till signeringstjänsten.

4. Signeringstjänsten skapar användarens nyckelpar, utfärdar ett certifikat för användaren samt signerar den elektroniska handlingen. Vid behov skapas en tidsstämpel.
5. Användaren returneras till e-tjänsten med en bekräftelse på att handlingen är underskriven. Bekräftelsen innefattar bl.a. signatur, certifikat och eventuell tidsstämpel.
6. Handling med underskrift skapas av e-tjänsten genom att foga samman handlingen med certifikat, signatur och eventuell tidsstämpel enligt efterfrågat signaturformat.

Genom detta förfarande kan e-tjänsten få en handling signerad utan att lämna ut uppgifter om den elektroniska handlingen till signeringstjänsten. Detta gör det även möjligt för e-tjänsten att signera handlingar som innehållsmässigt är strukturerade enligt att dataformat som inte signeringstjänsten kan presentera på ett för användaren meningsfullt sätt.

6.6 Fördelning av roller och uppgifter

Sammantaget innebär alternativ 1 och 2 följande skillnader i roller och vem som i praktiken utför väsentliga steg i signeringsprocessen.

	Tjänst som hanterar förfarandet	
Uppgift	**Alternativ 1**	**Alternativ 2**
Presentation av dokument som ska signeras för användaren	Signeringstjänsten	e-tjänsten
Skapande av en hash representation av dokumentet för signering	Signeringstjänsten	e-tjänsten
Motta användarens acceptans att signera	Signeringstjänsten	e-tjänsten
Identifiering av användaren	Signeringstjänsten	Signeringstjänsten
Generera nycklar för användaren samt utfärda certifikat till användaren	Signeringstjänsten	Signeringstjänsten
Tidsstämpling av dokument (Endast om detta begärs av e-tjänsten)	Signeringstjänsten	Signeringstjänsten
Signering av dokument	Signeringstjänsten	Signeringstjänsten
Skapa signerat dokument (*Foga samman dokument, certifikat ev. tidsstämpel samt signatur till ett signerat dokument enligt vedertagen standard*)	Signeringstjänsten	e-tjänsten

7 Krav på E-tjänster

De e-tjänster som utnyttjar signeringstjänsten enligt alternativ 2 kommer att bära ett viktigt ansvar för att signaturen är tillförlitlig. Om e-tjänsten är oärlig kan denne skicka med ett hash till signeringstjänsten som inte motsvarar det som e-tjänsten visat upp för användaren. Varken signaturtjänsten eller användaren har någon möjlighet att kontrollera att hash värdet som signeras överensstämmer med den information som användaren väljer att signera innan signering sker. Detta kan i viss mån motverkas om användarens får tillgång till den signerade handlingen efter signering för kontroll men detta förutsätter att den signerade handlingen har ett format som användaren lätt kan tillgodogöra sig.

Denna problemställning är dock inte ny för central signering. Även vid lokal signering är det svårt att uppnå en hög tillförlitlighet av att användaren faktiskt ser det som signeras då användaren måste förlita sig på den information som kan utläsas från lokal programvara för presentation av information och för signering. Även i många av dagens lösningar är användaren i slutändan tvungen att lita på att e-tjänsten inte beter sig bedrägligt.

Det bör klargöras, mot bakgrund av denna hotbild, vilka typer av e-tjänster som kan tillåtas utnyttja signeringstjänsten enligt alternativ 2, exempelvis om detta bör begränsas till statliga myndigheter.

8 Krav på signeringstjänstens organisation och driftsmiljö

Det är avgörande för förtroendet för utfärdade signaturer att signeringstjänsten hanteras under en organisation som har samhällets förtroende.

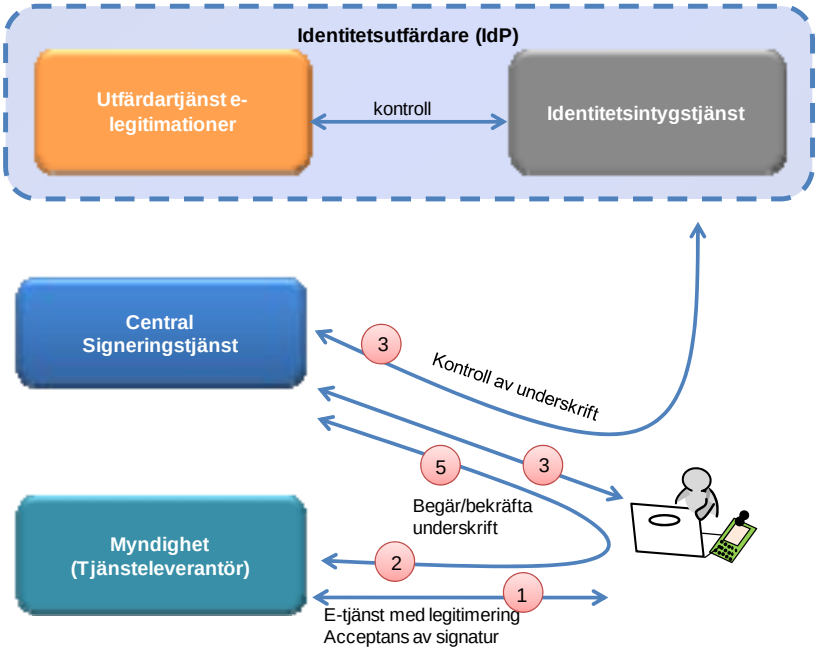
Driftsmiljö och säkerhetsrutiner måste på ett tillförlitligt sätt garantera systemets integritet och förhindra att enskilda administratörer kan missbruka systemet för egna syften.

Signeringstjänsten realiseras i grunden som en webbtjänst. Signeringstjänsten kommunicerar med användaren via HTTP samt kommunicerar vid behov med e-tjänsten via lämpligt gränssnitt.

9 Alternativ till central signering

Om en framtida utvärdering central signering kommer till slutsatsen att ingen form av central signering är acceptabelt, så finns andra alternativ till signering i samverkan med en federativ infrastruktur för identifiering i enlighet med utredningens förslag.

Som exempel kan följande lösning etableras:



1. Användaren identifierar sig för en e-tjänst genom sin e-legitimation och utnyttjar en tjänst som kräver användarens elektroniska underskrift (signatur).
2. Användaren överförs till signeringstjänsten med en begäran om signering från e-tjänsten.
3. Signeringstjänsten överför den information som ska signeras till användaren som signerar informationen med stöd av sin e-legitimation och sin klientapplikation för signering som

användaren erhållit från utfärdaren av användarens e-legitimation.

4. Signeringstjänsten verifierar att rätt användare signerat handlingen genom en kontroll mot identitetsutfärdaren (Förslagsvis genom att tillämpa standarden [SAMLX509].
5. Signeringstjänsten överför användaren tillbaks till e-tjänsten samt överför nödvändigsigneringsinformation.

Genom detta förfarande kan en e-tjänst befrias helt från såväl integration med användarens funktioner för signering, som tolkning av användarens e-legitimation för att fastställa användarens identitet. Signeringstjänsten sköter all integration med olika signeringslösningar i användarnas klienter och information om identitet ges i enlighet med federationens gemensamma attributsprofil i det attributsintyg som erhålls i samband med kontroll av signaturcertifikat (steg 4 enligt [SAMLX509].

Dock är en lösning av detta slag behäftat med i stort sett samma tidigare nämnda svagheter jämfört med dagens lösning på så sätt attanvändarens e-legitimation fortsatt måste vara certifikatbaserad samt att dessa signaturer inte kan verifieras av förlitande part i utlandet som inte har tillgång till aktuell spärrinformation eller den svenska infrastrukturen för identifiering.

Av detta skäl förs inte denna typ av lösning fram som ett primärt förslag.

10 Övergripande arkitektur

I de utförande exempel som anges i detta avsnitt sker även kommunikation mellan signeringstjänst och e-tjänst via HTTP.
Följande funktioner ingår i signeringstjänsten utöver webbgränssnittet mot användare och kommunikation med e-tjänster

- Certifikatutfärdare
- Tidsstämplingsfunktion
- Signeringsfunktion

Beskrivningarna i detta avsnitt utgör exempel på utförande som uppfyller ställda krav. De utgör ett grundförslag på utförande och

specificerar inte en komplett design för implementering. Olika aspekter av arkitekturen kan komma att ändras vid ett slutgiltigt genomförandeprojekt.

10.1 Informationsflöden

Grunden för kommunikation mellan e-tjänst och signeringstjänst samt mellan signeringstjänst och identitetsutfärdare är att kommunicera information via användaren så samma sätt som sker vid SAML authentication request och respons.

Utgångspunkten är att denna kommunikation sker i enlighet med SAML HTTP Post binding [SAML-Bindings].

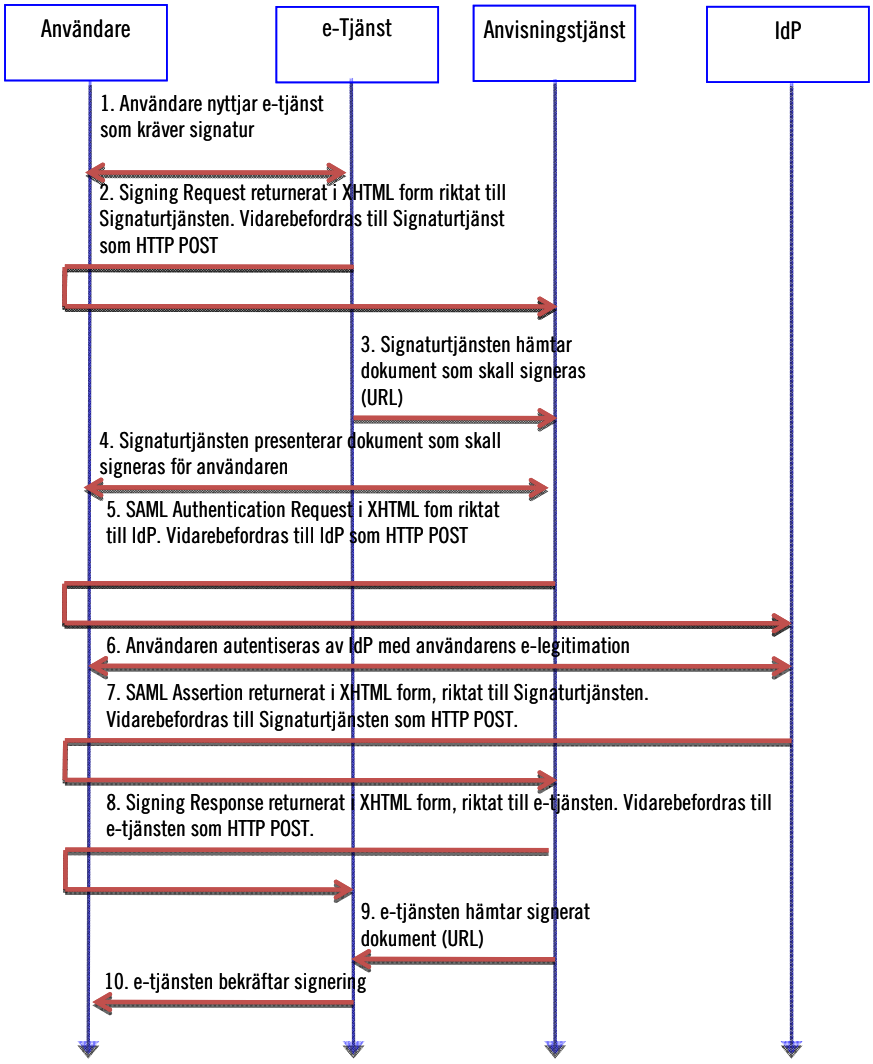
Vid SAML HTTP Post binding kommuniceras ett svar till användaren när denne gör ett aktivt val i sin webbläsare (ex. väljer att skriva under). Användarens val resulterar i en HTTP request från användaren till webbtjänsten. Detta resulterar i en HTTP response som innehåller en XHTML form som innehåller informationen som ska vidarebefordras till nästa webbtjänst (ex en signing request till signeringstjänsten eller en authentication request till identitetsutfärdaren. När XHTML formen öppnas i användarens webbläsare så innehåller denna en instruktion att skicka information till mottagande webbtjänst som HTTP Post.

[SAML-Bindings] specificerar genom SAML HTTP Post binding hur request och response meddelanden kan förmedlas via användaren på detta sätt.

det enda som krävs för en komplett specifikation av den informationsutväxling mellan e-tjänsten och signeringstjänsten som går via användaren är att specificera ett signing request och ett signing response meddelande som kan förmedlas i XHTML form via HTTP Post.

10.2 Informationsflöden - utförande enligt alternativ 1

Informationsutväxling mellan parterna i utförande enligt alternativ ett kan ske på följande sätt:

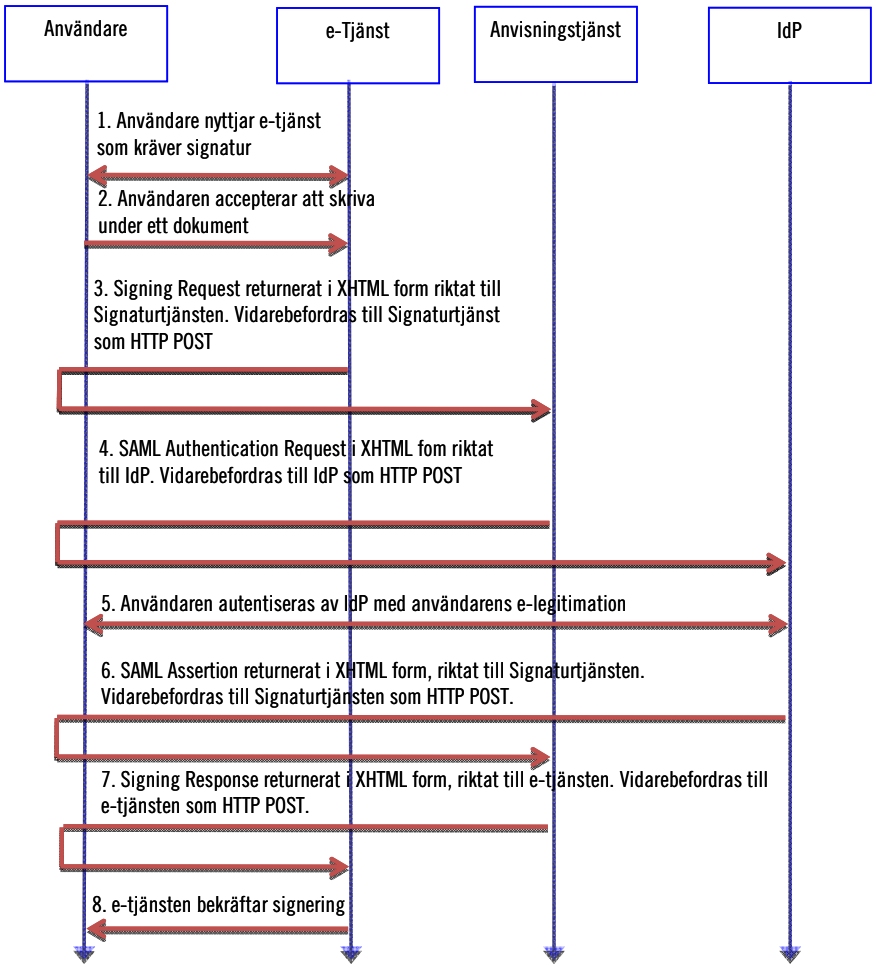


I detta utförande sker signering i signeringstjänsten efter det att användaren autentiserats och ett giltigt identitetsintyg (authentication response) mottagits av signeringstjänsten i steg 7.

Det dokument som signeras skickas inte via användaren för att undvika fördröjningar om dokumentet är stort och användaren har begränsad kommunikationshastighet. Dokument som ska signeras och signerat dokument hämtas av parterna via en URL i setgen 3 och 9. URL till dokumenten medföljer signing request respektive signing reponse i stegen 2 och 8.

10.3 Informationsutväxling – utförande enligt alternativ 2

Informationsutväxling mellan parterna i utförande enligt alternativ två kan ske på följande sätt:



I detta utförande sker signering i signeringstjänsten efter det att användaren autentiserats och ett giltigt identitetsintyg (authentication response) mottagits av signeringstjänsten i steg 6.

Det dokument som ska signeras överförs inte till signeringstjänsten. Istället överför e-tjänsten en hash av dokument som ska signeras i steg 3 till signeringstjänsten. Med hjälp av denna hash kan signeringstjänsten signera dokumentet utan att få tillgång till dokumentet i klartext (i läsbart skick).

På motsvarande vis skickas inte heller ett signerat dokument till e-tjänsten. Istället skickas signaturen på dokumentet till e-tjänsten

tillsammans med användarens certifikat i steg 7. Utifrån denna information kan e-tjänsten själv skapa det signerade dokumentet enligt ett för ändamålet lämpligt signaturformat.

10.3.1 Authentication request och response

Begäran och erhållande av identitetsintyg för användaren (stegen 5 och 7 i alternativ 1 och stegen 4 och 6 i alternativ 2) genomförs som är en ren SAML identifiering in enlighet med HTTP POST Binging, definierat i [SAML-Bindings].

Detta förfarande ska följa tekniska specifikationer för identitetsfederationen för svensk e-legitimering.

i relation till Identitetsutfärdaren så agerar signeringstjänsten som en förlitande e-tjänst (service provider) gentemot identitets-utfärdaren.

10.4 Signing request och response

Signing Request och Signing Response (steg 2 och 8 i alternativ 1 och steg 3 och 7 i alternativ 2) ska innehålla all information som signeringstjänsten och e-tjänsten behöver utbyta för att genom föra signering och hantera felsituationer med undantag för utväxling av dokument i alternativ 1.

Utgångspunkten är att följande information bör ingå:

Signing Request:

- Version (protokollversion)
- Request type (identifierar typ av request. Olika request type identifierare måste definieras för utförande enligt alternativ 1 och alternativ 2)
- Nonce (en unik identifierare för denna request)
- Identitetsattribut för användaren (Attribute assertion) (ej psudonym). Detta utgör de identitetsattribut som signerings-tjänsten måste kunna kontrolleras genom det identitetsintyg som signeringstjänsten erhåller från identitetsutfärdaren. Dessa attribut måste vara en delmängd av de attribut som signeringstjänsten registrerat som antingen required eller requested attributes i federationens metadata (federations-registret)

- Entity ID för den IdP som ska autentisera användaren vid signering
- En referens till det dokument som ska signeras i URL format (Endast alternativ 1)
- Referens till presentationsformat (stylesheeet) (URL format) (endast vid alternativ 1 och endast vid behov)
- Krypteringsnyckel/nycklar för att dekryptera information som hämtas direkt från e-tjänsten
- En hash av det dokument som ska signeras
- Identifierare av önskat signaturformat ([CMS]?, [XML Dsig], [PDF], [CAdES], [XAdES], [PAdES] etc) (Endast alternativ 1)
- Signaturoptioner
  - Tidsstämpling
  - krav på algorithmer
  - mm (Listan ska vara öppen för framtida utvidgning)

Signing Response

- Version (protokollversion)
- Response type (typ av response)
- Nonce (samma som request nonce)
- Statuskod (ex Signatur skapad, Signatur ej skapad med felkod)
- Referens till signerat dokument (URL) (endast alternativ 1)
- Krypteringsnyckel/nycklar för att dekryptera signerat dokument som hämtas direkt från signeringstjänsten (endast alternativ 1)
- Signatur på dokument som signerats (endast alternativ 2

10.4.1 Övrig kommunikation i flödesmodellerna

Informationsutväxling direkt mellan användare och e-tjänst samt mellan användare och identitetsutfärdare specificeras inte. Denna informationsutväxling utformas i sin helhet av e-tjänsten respektive identitetsutfärdaren.

Hämtning av dokument i stegen 3 och 9 sker med en HTTP GET metod enligt [HTTP] protokollet.

10.5 Tidsstämpling i alternativ 2

I alternativ 1 ombesörjer signeringstjänsten eventuell tidsstämpling av signerat dokument och bifogar tidsstämpeln i den signerade handlingen.

I alternativ 2 är detta inte möjligt eftersom signeringstjänsten inte har tillgång till det signerade dokumentet.

Om en e-tjänst behöver tidsstämpla den signerade handlingen och inkludera detta i den signerade handlingen måste e-tjänsten göra en separat begäran om tidsstämpling efter mottagande av signing response.

Detta kan ske utan att röja dokumentet för signeringstjänsten dels genom att följa tillämpliga standarder för signaturformat [CAdES], [XAdES] eller [PAdES] med avseende på vilken data som ska tidsstämplas och hur tidsstämpeln ska inkluderas i den signerade handlingen, samt dels genom att följa tidsstämplingsstandarden RFC 3161 [RFC3161] för att skicka en begäran om tidsstämpling och ta emot tidsstämpel.

10.6 Kommunikations- och meddelandesäkerhet

Följande krav kommunikations och meddelandesäkerhet bör gälla:

- Kommunikation mellan signeringsserver och användare krypteras med SSL/TLS [TLS] med stöd av servercertifikat (ingen klientautentisering).
- Kommunikation mellan användare och e-tjänst skyddas företrädelsevis med SSL/TLS med stöd av servercertifikat (ingen klientautenticering).
- Kommunikation med IdP samt Authentication request och response meddelanden skyddas i enlighet med identitetsfederation för svensk e-legitimation.
- Signature request och response ska krypteras till respektive mottagare och signeras av respektive avsändare.
- Dokument som ska signeras och signerat dokument krypteras med nyckel som medföljer signing request repsektive signing response. Publika nycklar för verifiering av signaturer hämtas från federationsregistret (metadata där

signaturtjänsten såväl som e-tjänsten är registrerade som e-tjänsteleverantörer).

10.7 Loggar

Signeringstjänsten behöver bland annat logga följande information för varje signering

- Signing request och signing response meddelanden
- hash av dokument som signerats
- Signatur
- Användarens signaturcertifikat
- Användarens identitetsintyg från acceptans av signering

Dokumentet som signerats och det signerade dokumentet bör inte loggas.

Loggar ska förses med tidsinformation som är tillförlitlig och spårbar till svensk tid (UTC(SP)).

11 Signering

Signeringstjänsten ska signera elektroniska dokument och i utförande enligt alternativ 1 även skapa ett signerat dokument.

Signeringstjänsten ska kunna skapa en kvalificerad elektronisk signatur enlig svensk lag om kvalificerade signaturer [Sig].

Signeringsprocessen följer ett antal väl definierade steg.

1. En hash av det dokument som ska signeras skapas med en godkänd hash algoritm
2. Dokumentets hash signeras med användarens privata signeringsnyckel
3. Ett signerat dokument skapas genom att foga samman dokumentet med signaturen och användarens signeringscertifikat.

Då signering sker enligt utförande alternativ 2 utför signeringstjänsten endast steg 2, medan steg 1 och 3 utförs av e-tjänsten som begär signering.

Innan steg 2 kan utföras måste användarens signeringsnyckel vara genererad och användarens tillhörande signeringscertifikat måste vara utfärdat.

Certifikaten som påförs den signerade handlingen i steg 3 innefattar förutom användarens certifikat även certifikat för de certifikatutfärdare som krävs för att verifiera användarens certifikat.

Om det signerade dokumentet ska tidsstämplas utförs dessutom följande steg

4. En hash av den information som ska tidsstämplas skapas med en godkänd hash algorithm (normalt en hash av själva signaturen som skapades i steg 3)
5. Hash värdet tidsstämplas
6. Tidsstämpeln infogas i det signerade dokumentet

11.1 Signaturformat

I de fall signeringstjänsten skapar ett signerat dokument (steg 3) samt i de fall signeringstjänsten skapar och för in en tidsstämpel i det signerade dokumentet (steg 4 och 6), så ska detta ske i enlighet med ett definierat signaturformat.

Signaturformatet definierar följande aspekter som är relaterat till stegen i föregående avsnitt:

- Hur signatur och dokument fogas samman till ett signerat dokument
- Hur certifikat fogas till det signerade dokumentet
- Vilken information i det signerade dokumentet som är signerad
- Vilken information som ska tidsstämplas
- Hur en tidsstämpel skal fogas till det signerade dokumentet

I de fall det signerade dokumentet inte ska förses med en tidsstämpel så ska följande signaturformat stödjas av signeringstjänsten:

- XML Signature Syntax [XML Dsig]
- Portable Document Format [PDF]

Följade signaturformat kan dessutom stödjas för icke tidsstämplade dokument:

- Cryptographic Message Syntax[CMS]
- CMS Advanced electronic Signatures enligt profil CAdES-BES [CAdES]
- XML Advanced Electronic Signatures enligt profil XAdES-BES [XAdES]
- PDF Advanced Electronic Signatures part 3 enligt profil PAdES-BES [PAdES]

I de fall en tidsstämpel ska tillfogas den signerade handlingen ska följande signaturformat stödjas av signeringstjänsten:

- XML Advanced Electronic Signatures enligt profil XAdES-T [XAdES]
- PDF Advanced Electronic Signatures enligt profil PAdES-T [PAdES]

Följade signaturformat kan dessutom stödjas för tidsstämplade dokument:

- CMS Advanced electronic Signatures enligt profil CAdES-T [CAdES]

11.2 Multipla signaturer

Samtliga standardiserade signaturformat enligt avsnitt 11.1 stödjer att ett dokument förses med flera signaturer. Detta kan vara aktuellt om samma handling måste signeras av mer än en person.

Signaturformaten [CMS} och [XMLDsig] utgör grunden för samtliga nämnda signaturformat [CMS] utgör grunden för [PDF], [PAdES] och [CAdES] signaturer medan [XMLDsig] utgör grunden för [XAdES] signaturer.

I [CMS] lagras signaturer för var och en som undertecknat dokumentet i ett ”SignerInfo” fält. [CMS} tillhandahåller även ett attribut för kontrasignaturer där varje kontrasignatur signerar en signatur i ett av dokumentets SignerInfo fält.

[XMLDsig] tillåter att flera signaturer kopplas till ett dokument genom att lägga till fler ”Signature” element.

Multipla signaturer hanteras enkelt i alternativ 1 såväl som alternativ 2. I alternativ 1 lägger signaturtjänsten till en ny signatur till en befintlig signatur då e-tjänsten tillhandahåller ett dokument för underskrift som redan är signerat. I alternativ 2 lägger e-

tjänsten själv till den nya signaturen efter det att dokumentet signerats av ytterligare personer.

12 Certifikatutfärdande

Certifikatutfärdarfunktionen skapar användarens nyckelpar för signering och utfärdar certifikat till användare som identifierats av signeringstjänsten.

Användarens privata nyckel ska raderas från systemet efter fullgjord signering och ett nytt nyckelpar ska skapas för varje användare och signeringstillfälle.

Certifikat ska utfärdas som kvalificerade certifikat.

12.1 Utfärdarrutiner

Utfärdarrutiner ska följa ETSI policy för certifikatutfärdare som utfärdar kvalificerads certifikat, TS 101 456 [TS101456].

12.2 Certifikatformat

Certifikat till användare ska utformas i enlighet med följande standards:

Standard	Funktion	Referens
RFC 5280	Huvudspecifikation för utformning av certifikat	[RFC5280]
RFC 3739	Internationell huvudstandard för utformning av kvalificerade certifikat.	[RFC3739]
TS 101 862	EU profil av RFC 3739 som specificerar utformning av kvalificerade certifikat enligt EU direktivet för elektroniska signaturer [EUSig].	[TS101862]

Certifikat bör vidare i tillämpliga delar följa TS 102 280 [TS102280] som är en ETSI profil för utfärdande av certifikat till fysiska personer. Denna standard är dock delvis inaktuell eftersom den refererar till föregångaren till RFC 5280 (nämligen RFC 3280). TS 102 280 kommer inom snart att revideras av ETSI. Till detta är gjort bör man hantera TS 102 280 endast som en rekommendation.

Utöver dessa standarder ska följande krav tillgodoses i certifikat utfärdade till användare:

Kravområde	Krav
Information om att certifikatet utfärdats som ett kvalificerat certifikat	Statement ”id-etsi-qcs-QcCompliance” ska infogas i samtliga certifikat i enlighet med TS 101 862.
Information om att privat nyckel hanteras i en ”säker anordning för signaturframställning” i enlighet med signaturlagen [Sig].	Statement ”id-etsi-qcs-QcSSCD” ska infogas i samtliga certifikat i enlighet med TS 101 862.
Information om förlitandebegränsning	Satement ”id-etsi-qcs-QcLimitValue” enligt TS 101 862 kan infogas för att kommunicera en övre monetär gräns för förlitande på utfärdat certifikat. Enligt gällande praxis kan denna gräns sättas till 0. För alla andra värden ska såväl valuta som beloppsgräns specificeras.
Identitetsattribut	Val av identitetsattribut ska följa RFC 3739. det kan vara nödvändigt att på lämpligt sätt konvertera information om användares identitet från attribut i identitetsintyg till andra attribut i certifikaten. Certifikatutfärdaren ska då tillämpa samma mappning om ett stödsystem för certifikatverifiering via SAML tillämpas
Publik nyckel	Algoritm och nyckellängd ska följa generella krav på signeringsalgoritmer i avsnitt 14.

12.3 Stödsystem för certifikatverifiering

Certifikatutfärdarfunktionen ska tillhandahålla spärrinformation. Minimikravet är att tillhandahålla en spärrlista (CRL) i enlighet med RFC 5280 [RFC5280].

12.3.1 Spärrinformation

Spärrinformation ska tillhandahållas i form av en spärrlista (CRL). En sådan spärrlista ska vara en CRL version 2 spärrlista i enlighet med RFC 5280 [RFC5280].

Som komplement kan även spärrinformation tillhandahållas som en on-line tjänst enligt OCSP protokollet [RFC2560].

Den spärrinformation som tillhandahålls måste oavsett teknik vara allmänt tillgänglig. Det får inte krävas ett särskilt avtal med certifikatutfärdaren (Signeringstjänsten) för att få tillgång till spärrinformation.

12.3.2 Certifikatverifiering via SAML

Certifikatutfärdarfunktionen kan även tillhandahålla en certifikatverifieringsfunktion via SAML där certifikatutfärdarfunktionen agerar attributstjänst.

Genom denna attributstjänst kan en e-tjänst som verifierar en användares certifikat skicka en attributsförfrågan till certifikatutfärdaren där användarens certifikat bifogas. Om certifikatet är giltigt returnerar certifikatutfärdarfunktionen ett attributsintyg med användarens identitetsattribut (angivet i enlighet med identitetsfederationens attributsprofil).

Denna attributstjänst ska implementera ”SAML V2.0 Attribute Sharing Profile for X.509 Authentication-Based Systems” [SAMLX509] samt tillämpningsprofilen ”SAML V2.0 Deployment Profiles for X.509 Subjects” [SAMLX509Dep]

13 Tidsstämpling

En tidsstämplingstjänst kan upprättas för att dels skapa tidsstämplade signerade dokument som en del av signeringsfunktionen enligt alternativ 1.

En tidsstämplingsfunktion kan även upprättas som en separat tjänst som kan anropas av en e-tjänst för att tidsstämpla ett dokument. Detta kan vara ett signerat dokument i enlighet med någon av de angivna standarderna för tidsstämplade signerade dokument, men kan även vara vilken annan handling som helst.

Tidsstämplingstjänsten tar emot ett hash av ett dokument som ska tidsstämplas och signerar detta hash tillsammans med tidsinformation (ett time-stamp token). Själva handlingen som ska tidsstämplas skickas inte till tidsstämplingsfunktionen.

13.1 Format

Format för tidsstämplar (time-stamp token) samt format för begäran om tidsstämpling ska följa RFC 3161 [RFC3161].

13.2 Transportprotokoll

Då tidsstämplingsfunktionen tillhandahålls som separat tjänst mot e-tjänster så ska transportprotokoll för begäran om tidsstämpling samt returnering av tidsstämpel vara HTTP [HTTP] och följa regler för HTTP transport i RFC 3161 [RFC3161].

13.3 Tillförlitlig tid

Det är avgörande för tidstämplingstjänstens trovärdighet att denna har tillgång till tillförlitlig tid. Tidskällan ska vara direkt spårbar till UTC(SP) (Swedish National time scale).

14 Algoritmer

Val av algoritmer och nyckellängder för tjänster som omfattas av signeringstjänsten bör följa NIST SP 800-131 [SP800-131]. ETSI TS 102 176-1 [ETSI-Algo] är en europeisk specifikation från ETSI som täcker samma område som SP 800-131, men denna är från 2007 och inte lika aktuell som SP 800-131.

Följande algoritmer rekommenderas som minsta acceptabla säkerhetsnivå för samtliga tjänster:

Användningsområde	Algoritm
Symetrisk kryptering	AES-128
Hash algoritm	SHA-256
Publik nyckel algoritm för signering och autentisering	RSA med 2048 bitars modulus. **Not:** Certifikatutfärdare som utfärdar certifikat med en giltighetstid på över 4 år (inkluderat självsignerade rotcertifikat) bör använda RSA med minst 4096 bitars modulus.
Publik nyckel algoritm för skapande av symmetrisk sessionsnyckel (Key agreement)	Diffie Hellman, p=2048 bitar

Dessa rekommendationer är kompatibla med NIST SP 800-131.

15 Referenser

[SAML-Bindings] ”Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0”, OASIS Standard, 15 March 2005.

[CMS] RFC 5652, ”Cryptographic Message Syntax (CMS)”, IETF Standard, September 2009.

[XML Dsig] ”XML Signature Syntax and Processing (Second Edition)”, W3C Recommendation, 10 June 2008.

[PDF] ISO 32000-1:2008, ”Document management — Portable document format — Part 1: PDF 1.7”, ISO Standard, 1 July 2008.

[CAdES] ETSI TS 101 733 V1.8.1, ”Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)”, ETSI Technical Specification, November 2009.

[XAdES] ETSI TS 101 903 V1.4.1, ”XML Advanced Electronic Signatures (XAdES)”, ETSI Technical Specification, June 2009

[PAdES] ETSI TS 102 778 part 1-5, ”Electronic Signatures and Infrastructures (ESI);PDF Advanced Electronic Signature Profiles”, ETSI Technical specifications, various dates.

[HTTP] RFC 2616, ”Hypertext Transfer Protocol -- HTTP/1.1”, IETF Draft Standard, June 1999.

[TLS] RFC 5246, ”The Transport Layer Security (TLS) Protocol Version 1.2”, IETF Proposed standard, August 2008.

[Sig] Lag (2000:832) om kvalificerade elektroniska signaturer.

[SP800-131] NIST SP 800-131, ”Recommendation for the Transitioning of Cryptographic Algorithms and Key Lengths”, NIST special publication draft, June 2010

[TS101456] TS 101 456, ”Electronic signatures and infrastructures (ESI); Policy requirements for certification authorities issuing qualified

certificates", ETSI Technical Specification, May 2007.

[ETSI-Algo] TS 102 176-1, "Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms", ETSI Technical Specification, November 2007.

[RFC3161] RFC 3161, "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)" IETF Proposed Standard, August 2001.

[RFC5280] RFC 5280, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", IETF Proposed standard, May 2008

[RFC3739] RFC 3739, "Internet X.509 Public Key Infrastructure: Qualified Certificates Profile". IETF Proposed Standard, March 2004.

[TS101862] ETSI 101 862, "Qualified certificate profile", ETSI Technical Specification, January 2006.

[TS102280] TS 102 280 "X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons", ETSI Technical Specification, March 2003.

[OCSP] RFC 2560, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP", IETF Proposed Standard, June 1999.

[SAMLX509] "SAML V2.0 Attribute Sharing Profile for X.509 Authentication-Based Systems", OASIS Committee Specification 01, March 2008.

[SAMLX509Dep] "SAML V2.0 Deployment Profiles for X.509 Subjects", OASIS Committee Specification 01, March 2008.

[EUSig] "DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures", January 2000.

Statens offentliga utredningar 2010

Kronologisk förteckning

1. Lätt att göra rätt – om förmedling av brottsskadestånd. Ju.
2. Ett samlat insolvensförfarande – förslag till ny lag. Ju.
3. Metria – förutsättningar för att ombilda division Metria vid Lantmäteriet till ett statligt ägt aktiebolag. M.
4. Allmänna handlingar i elektronisk form – offentlighet och integritet. Ju.
5. Skolgång för alla barn. U.
6. Kunskapslägesrapport på kärnavfallsområdet 2010 – utmaningar för slutförvarsprogrammet. M.
7. Aktiva åtgärder för att främja lika rättigheter och möjligheter – ett systematiskt målinriktat arbete på tre samhällsområden. IJ.
8. En myndighet för havs- och vattenmiljö. M.
9. Den framtida organisationen för vissa fiskefrågor. Jo.
10. Kvinnor, män och jämställdhet i läromedel i historia. En granskning på uppdrag av Delegationen för jämställdhet i skolan. U.
11. Spela samman – en ny modell för statens stöd till regional kulturverksamhet. Ku.
12. I samspel med musiklivet – en ny nationell plattform för musiken. Ku.
13 Upphandling på försvars- och säkerhetsområdet. Fi.
14. Partsinsyn enligt rättegångsbalken. Ju.
15. Kriminella grupperingar – motverka rekrytering och underlätta avhopp. Ju.
16. Sverige för nyanlända. Värden, välfärdsstat, vardagsliv. IJ.
17. Prissatt vatten? M.
18. En reformerad budgetlag. Fi.
19. Lärling – en bro mellan skola och arbetsliv. U.
20. Så enkelt som möjligt för så många som möjligt – från strategi till handling för e-förvaltning. Fi.
21. Bättre marknad för tjänstehundar. Jo.
22. Krigets Lagar – centrala dokument om folkrätten under väpnad konflikt, neutralitet, ockupation och fredsinsatser. Fö.
23. Tredje sjösäkerhetspaketet. Klassdirektivet, Klassförordningen, Olycksutredningsdirektivet, IMO:s olycksutredningskod. N.
24. Avtalad upphovsrätt. Ju.
25. Viss översyn av verksamhet och organisation på informationssäkerhetsområdet. Fö.
26. Flyttningsbidrag och unionsrätten. A.
27. Gemensamt ansvar och gränsöverstigande samarbete inom transportforskningen. N.
28. Vändpunkt Sverige – ett ökat intresse för matematik, naturvetenskap, teknik och IKT. U.
29. En ny förvaltningslag. Ju.
30. Tredje inre marknadspaketet för el och naturgas. Fortsatt europeisk harmonisering. N.
31. Första hjälpen i psykisk hälsa. S.
32. Utrikesförvaltning i världsklass. En mer flexibel utrikesrepresentation. UD.
33. Kvinnor, män och jämställdhet i läromedel i samhällskunskap. En granskning på uppdrag av Delegationen för jämställdhet i skolan. U.
34. På väg mot en ny roll – överväganden och förslag om Riksutställningar. Ku.
35. Kunskap som befrielse? En metanalys av svensk forskning om jämställdhet och skola 1969–2009. U.
36. Svensk forskning om jämställdhet och skola. En bibliografi. U.
37. Sverige för nyanlända utanför flyktingmottagandet. IJ.
38. Mutbrott. Ju.
39. Ny ordning för nationella vaccinationsprogram. S.

40. Cirkulär migration och utveckling – kartläggning av cirkulära rörelsemönster och diskussion om hur migrationens utvecklingspotential kan främjas. Ju.
41. Kompensationstillägg – om ersättning vid försenade utbetalningar. S.
42. Med fiskevård i fokus – en ny fiskevårdslag. Jo.
43. Förundersökningsbegränsning. Ju.
44. Mål och medel – särskilda åtgärder för vissa måltyper i domstol. Ju.
45. Händelseanalyser vid självmord inom hälso- och sjukvården och socialtjänsten. Förslag till ny lag. S.
46. Utländsk näringsverksamhet i Sverige. En översyn av lagstiftningen om utländska filialer i ett EU-perspektiv. N.
47. Alkoholkonsumtion, alkoholproblem och sjukfrånvaro – vilka är sambanden? En systematisk litteraturöversikt. S.
48. Multipla hälsoproblem bland personer över 60 år. En systematisk litteraturöversikt om förekomst, konsekvenser och vård. S.
49. Förbud mot köp av sexuell tjänst. En utvärdering 1999–2008. Ju.
50. Försvarsmaktens helikopterresurser. Fö.
51. Könsskillnader i skolprestationer – idéer om orsaker. U.
52. Biologiska faktorer och könsskillnader i skolresultat. Ett diskussionsunderlag för Delegationen för jämställdhet i skolans arbete för analys av bakgrunden till pojkars sämre skolprestationer jämfört med flickors. U.
53. Pojkar och skolan: Ett bakgrundsdokument om "pojkkrisen". Översättning på svenska av engelsk rapport: Boys and School: A Background Paper on the "Boy Crisis". + Engelsk rapport. U.
54. Förbättrad återbetalning av studieskulder. U.
55. Romers rätt – en strategi för romer i Sverige. IJ.
56. Innovationsupphandling. N.
57. Effektivare planering av vägar och järnvägar. N.
58. Rehabiliteringsrådets delbetänkande. S.
59. Underhållsskyldighet i internationella situationer – Underhållsförordningen, 2007 års Haagkonvention och 2007 års Haagprotokoll + Bilagedel. Ju.
60. Ett utvidgat skydd mot åldersdiskriminering. IJ.
61. Driftskompatibilitet och enheter som ansvarar för underhåll inom EU:s järnvägssystem. N.
62. Så enkelt som möjligt för så många som möjligt. Under konstruktion – framtidens e- förvaltning. Fi.
63. EU:s direktiv om sanktioner mot arbetsgivare. Ju.
64. "Se de tidiga tecknen" – forskare reflekterar över sju berättelser från förskola och skola. U.
65. Kompetens och ansvar. S.
66. Barns perspektiv på jämställdhet i skola. En kunskapsöversikt. U.
67. I rättan tid? Om ålder och skolstart. U.
68. Ny yttrandefrihetsgrundlag? Yttrandefrihetskommittén presenterar tre modeller. Ju.
69. Förbättrad vinterberedskap inom järnvägen. N.
70. Ny struktur för skydd av mänskliga rättigheter. + Bilagor + Lättläst + Daisy. IJ.
71. Sexualbrottslagstiftningen – utvärdering och reformförslag. Ju.
72. Folkrätt i väpnad konflikt – svensk tolkning och tillämpning. + Bilaga 7, Svensk manual i humanitär rätt m.m. Fö.
73. Svensk sjöfarts konkurrensförutsättningar. N.
74. Mer innovation ur transportforskning. N.
75. Gymnasial lärlingsutbildning – utbildning för jobb. Erfarenheter efter två års försök med lärlingsutbildning. U.
76. Transportstyrelsens databaser på vägtrafikområdet – integritet och effektivitet. N.
77. Sammanläggningar av landsting – övergångsstyre och utjämning. Fi.
78. Fondverksamhet över gränserna. Genomförande av UCITS IV-direktivet. Fi.
79. Pojkars och flickors psykiska hälsa i skolan: en kunskapsöversikt. U
80. Skolan och ungdomars psykosociala hälsa. U.
81. En ny biobankslag. S.
82. Trafikverket ICT. N.

83. Att bli medveten och förändra sitt förhållningssätt. Jämställdhetsarbete i skolan. U.
84. Hedersrelaterad problematik i skolan – en kunskaps- och forskningsöversikt. U.
85. Vem arbetar efter 65 års ålder? En statistisk analys. S.
86. Personalförsörjningen i ett reformerat försvar. Fö.
87. Skadestånd och Europakonventionen. Ju.
88. Vägen till arbete. Arbetsmarknadspolitik, utbildning och arbetsmarknadsintegration. Fi.
89. Finns det samband mellan samsjuklighet och sjukfrånvaro? En systematisk litteraturöversikt. S.
90. En ny lag om ekonomiska föreningar. Del 1+2. Ju.
91. Planering på djupet – fysisk planering av havet. M.
92. En effektivare förvaltning av statens fastigheter. Fi.
93. Att skapa arbeten. Löner, anställningsskydd och konkurrens. Fi.
94. Gotland – användningen av beteckningarna regionfullmäktige och regionstyrelse. Fi.
95. Se, tolka och agera – allas rätt till en likvärdig utbildning. U.
96. Riktiga betyg är bättre än höga betyg. Förslag till omprövning av betyg. U.
97. Resultatuppföljning, läskvalitet och skolutveckling – tre bidrag till diskussionen om jämställdhet i skolan. U.
98. Gårdsförsäljning. S.
99. Flickor, pojkar, individer – om betydelsen av jämställdhet för kunskap och utveckling i skolan. U.
100. Ansvar för järnvägssäkerheten. Kan en annan fördelning gynna en marknadsdriven utveckling? N.
101. Handlingsplan för att utveckla strategier i miljömålssystemet. M.
102. Massuppsägningar, arbetslöshet och sjuklighet. En rapport om konsekvenser av 1900-talets friställningar för slutenvårdsutnyttjande och risk för förtida död. S.
103. Särskilda spaningsmetoder. Ju.
104. E-legitimationsnämnden och Svensk e-legitimation. Fi.

Statens offentliga utredningar 2010

Systematisk förteckning

Justitiedepartementet

Lätt att göra rätt
– om förmedling av brottsskadestånd. [1]
Ett samlat insolvensförfarande – förslag till ny lag. [2]
Allmänna handlingar i elektronisk form
– offentlighet och integritet. [4]
Partsinsyn enligt rättegångsbalken. [14]
Kriminella grupperingar – motverka rekrytering och underlätta avhopp. [15]
Avtalad upphovsrätt. [24]
En ny förvaltningslag. [29]
Mutbrott. (38)
Cirkulär migration och utveckling
– kartläggning av cirkulära rörelsemönster och diskussion om hur migrationens utvecklingspotential kan främjas. [40]
Förundersökningsbegränsning. [43]
Mål och medel – särskilda åtgärder för vissa måltyper i domstol. [44]
Förbud mot köp av sexuell tjänst. En utvärdering 1999–2008. [49]
Underhållsskyldighet i internationella situationer – Underhållsförordningen, 2007 års Haagkonvention och 2007 års Haagprotokoll + Bilagedel. [59]
EU:s direktiv om sanktioner mot arbetsgivare. [63]
Ny yttrandefrihetsgrundlag? Yttrandefrihetskommittén presenterar tre modeller. [68]
Sexualbrottslagstiftningen – utvärdering och reformförslag. [71]
Skadestånd och Europakonventionen. [87]
En ny lag om ekonomiska föreningar. Del 1+2. [90]
Särskilda spaningsmetoder. [103]

Utrikespartementet

Utrikesförvaltning i världsklass. En mer flexibel utrikesrepresentation. [32]

Försvarsdepartementet

Krigets Lagar – centrala dokument om folkrätten under väpnad konflikt, neutralitet, ockupation och fredsinsatser. [22]
Viss översyn av verksamhet och organisation på informationssäkerhetsområdet. [25]
Försvarsmaktens helikopterresurser. [50]
Folkrätt i väpnad konflikt – svensk tolkning och tillämpning. + Bilaga 7, Svensk manual i humanitär rätt m.m. [72]
Personalförsörjningen i ett reformerat försvar. [86]

Socialdepartementet

Första hjälpen i psykisk hälsa. [31]
Ny ordning för nationella vaccinationsprogram. [39]
Kompensationstillägg – om ersättning vid försenade utbetalningar. [41]
Händelseanalyser vid självmord inom hälso- och sjukvården och socialtjänsten. Förslag till ny lag. [45]
Alkoholkonsumtion, alkoholproblem och sjukfrånvaro – vilka är sambanden? En systematisk litteraturöversikt. [47]
Multipla hälsoproblem bland personer över 60 år. En systematisk litteraturöversikt om förekomst, konsekvenser och vård. [48]
Rehabiliteringsrådets delbetänkande. [58]
Kompetens och ansvar. [65]
En ny biobankslag. [81]
Vem arbetar efter 65 års ålder? En statistisk analys. [85]
Finns det samband mellan samsjuklighet och sjukfrånvaro? En systematisk litteraturöversikt. [89]
Gårdsförsäljning. [98]
Massuppsägningar, arbetslöshet och sjuklighet. En rapport om konsekvenser av 1900-talets friställningar för slutenvårdsutnyttjande och risk för förtida död. [102]

Finansdepartementet

Upphandling på försvars- och säkerhetsområdet. [13]

En reformerad budgetlag. [18]

Så enkelt som möjligt för så många som möjligt – från strategi till handling för e-förvaltning. [20]

Så enkelt som möjligt för så många som möjligt. Under konstruktion – framtidens e- förvaltning. [62]

Sammanläggningar av landsting – övergångsstyre och utjämning. [77]

Fondverksamhet över gränserna. Genomförande av UCITS IV-direktivet. [78]

Vägen till arbete. Arbetsmarknadspolitik, utbildning och arbetsmarknadsintegration. [88]

En effektivare förvaltning av statens fastigheter. [92]

Att skapa arbeten. Löner, anställningsskydd och konkurrens. [93]

Gotland – användningen av beteckningarna regionfullmäktige och regionstyrelse. [94]

E-legitimationsnämnden och Svensk e-legitimation. [104]

Utbildningsdepartementet

Skolgång för alla barn. [5]

Kvinnor, män och jämställdhet i läromedel i historia. En granskning på uppdrag av Delegationen för jämställdhet i skolan. [10]

Lärling – en bro mellan skola och arbetsliv. [19]

Vändpunkt Sverige – ett ökat intresse för matematik, naturvetenskap, teknik och IKT. [28]

Kvinnor, män och jämställdhet i läromedel i samhällskunskap. En granskning på uppdrag av Delegationen för jämställdhet i skolan. [33]

Kunskap som befrielse? En metaanalys av svensk forskning om jämställdhet och skola 1969–2009. [35]

Svensk forskning om jämställdhet och skola. En bibliografi. [36]

Könsskillnader i skolprestationer – idéer om orsaker. [51]

Biologiska faktorer och könsskillnader i skolresultat. Ett diskussionsunderlag för Delegationen för jämställdhet i skolans arbete för analys av bakgrunden till pojkars sämre skolprestationer jämfört med flickors. [52]

Pojkar och skolan: Ett bakgrundsdokument om pojkkrisen. Översättning på svenska av engelsk rapport: Boys and School: A Backgroundpaper on the "Boy Crisis". + Engelsk rapport.[53]

Förbättrad återbetalning av studieskulder. [54]

"Se de tidiga tecknen" – forskare reflekterar över sju berättelser från förskola och skola. [64]

Barns perspektiv på jämställdhet i skola. En kunskapsöversikt. [66]

I rättan tid? Om ålder och skolstart. [67]

Gymnasial lärlingsutbildning – utbildning för jobb. Erfarenheter efter två års försök med lärlingsutbildning. [75]

Pojkars och flickors psykiska hälsa i skolan: en kunskapsöversikt. [79]

Skolan och ungdomars psykosociala hälsa. [80]

Att bli medveten och förändra sitt förhållningssätt. Jämställdhetsarbete i skolan. [83]

Hedersrelaterad problematik i skolan – en kunskaps- och forskningsöversikt. [84]

Se, tolka och agera – allas rätt till en likvärdig utbildning. [95]

Riktiga betyg är bättre än höga betyg. Förslag till omprövning av betyg. [96]

Resultatuppföljning, läskvalitet och skolutveckling – tre bidrag till diskussionen om jämställdhet i skolan. [97]

Flickor, pojkar, individer – om betydelsen av jämställdhet för kunskap och utveckling i skolan.[99]

Jordbruksdepartementet

Den framtida organisationen för vissa fiskefrågor. [9]

Bättre marknad för tjänstehundar. [21]

Med fiskevård i fokus – en ny fiskevårdslag. [42]

Miljödepartementet

Metria – förutsättningar för att ombilda division Metria vid Lantmäteriet till ett statligt ägt aktiebolag. [3]

Kunskapslägesrapport på kärnavfallsområdet 2010 – utmaningar för slutförvarsprogrammet. [6]

En myndighet för havs- och vattenmiljö. [8]
Prissatt vatten? [17]
Planering på djupet – fysisk planering av havet. [91]
Handlingsplan för att utveckla strategier i miljömålssystemet. [101]

Näringsdepartementet

Tredje sjösäkerhetspaketet. Klassdirektivet, Klassförordningen, Olycksutredningsdirektivet, IMO:s olycksutredningskod. [23]
Gemensamt ansvar och gränsöverstigande samarbete inom transportforskningen. [27]
Tredje inre marknadspaketet för el och naturgas. Fortsatt europeisk harmonisering. [30]
Utländsk näringsverksamhet i Sverige. En översyn av lagstiftningen om utländska filialer i ett EU-perspektiv. [46]
Innovationsupphandling. [56]
Effektivare planering av vägar och järnvägar. [57]
Driftskompatibilitet och enheter som ansvarar för underhåll inom EU:s järnvägssystem. [61]
Förbättrad vinterberedskap inom järnvägen. [69]
Svensk sjöfarts konkurrensförutsättningar [73]
Mer innovation ur transportforskning. [74]
Transportstyrelsens databaser på vägtrafikområdet – integritet och effektivitet. [76]
Trafikverket ICT. [82]
Ansvar för järnvägssäkerheten. Kan en annan fördelning gynna en marknadsdriven utveckling? [100]

Integrations- och jämställdhetsdepartementet

Aktiva åtgärder för att främja lika rättigheter och möjligheter – ett systematiskt målinriktat arbete på tre samhällsområden. [7]
Sverige för nyanlända. Värden, välfärdsstat, vardagsliv. [16]
Sverige för nyanlända utanför flyktingmottandet. [37]
Romers rätt – en strategi för romer i Sverige. [55]
Ett utvidgat skydd mot åldersdiskriminering. [60]
Ny struktur för skydd av mänskliga rättigheter. + Bilagor + Lättläst + Daisy. [70]

Kulturdepartementet

Spela samman – en ny modell för statens stöd till regional kulturverksamhet. [11]
I samspel med musiklivet – en ny nationell plattform för musiken. [12]
På väg mot en ny roll – överväganden och förslag om Riksutställningar. [34]

Arbetsmarknadsdepartementet

Flyttningsbidrag och unionsrätten. [26]