

Uppgjord Fredrik Ljunggren	Dok.id KIREI-2010-01		
Godkänd	Datum 2010-02-10	Rev A	Referens SOU 2009:86 (delvis)

Yttrande över e-delegationens betänkande SOU 2009:86 - Strategi för myndigheternas arbete med e-förvaltning.

Kirei AB har ombetts lämna synpunkter på e-delegationens betänkande SOU 2009:86. Kirei väljer att endast lämna yttrande om de delar som rör e-legitimationer.

I e-delegationens betänkande om strategi för myndigheternas arbete med e-förvaltning, föreslås att en samordningsfunktion i myndighetsform inrättas i syfte att avlasta myndigheterna och utveckla federerad elektronisk identifiering i Sverige. Detta är ett stort steg i rätt riktning för att etablera den samhällsviktiga infrastrukturen och den facto-standard för elektronisk identifiering som krävs för både offentlig verksamhet och näringsliv.

Det är dock viktigt att uppbyggnaden genomförs på ett sätt som gör att hela samhället kan dra nytta av infrastrukturen. Därför anser vi att utgångsläget för federerad eID i Sverige bör:

1. vara baserad på öppna standarder,
2. ge ett fullgott skydd av den personliga integriteten,
3. vara teknikneutralt,
4. vara tillräckligt kostnadseffektivt och
5. vara tillgängligt för aktörer i alla delar av samhället.

Det är vår uppfattning att den föreslagna arkitekturen, rätt implementerad, kan möta dessa krav.

E-delegationens förslag innehåller dock ett grundläggande fel som skulle kunna få mycket stor betydelse för utvecklingen av elektronisk identifiering i Sverige, nämligen att samordningsfunktionen som etablerar svensk e-legitimation inte samtidigt bör vara federationsoperatör eller identitetsintygsgivare. Detta är tre skilda funktioner som verkar på olika nivåer i federationen, med olika uppgifter och olika ansvar.

Vi menar att statliga samordningen av e-legitimering bör ske genom att realisera två separata funktioner, gärna som uppdrag till två olika myndigheter:

- En samordningsfunktion med fokus på styrning och som har som huvudsakligt uppdrag att direkt, eller indirekt via ackrediterade granskarer, godkänna identitetsleverantörer samt att publicera regler och tekniska ramverk för både identitetsleverantörer och tjänsteleverantörer.
- En upphandlingsfunktion som genomför upphandlingar av identitetsintygsgivare baserat på de regler och ramverk som samordningsfunktionen publicerar och som genom avtal med dessa tillgodoser myndigheternas behov av elektronisk identifiering.

Uppgjord Fredrik Ljunggren	Dok.id KIREI-2010-01		
Godkänd	Datum 2010-02-10	Rev A	Referens SOU 2009:86 (delvis)

Genom att ha en tydlig separation mellan dessa funktioner kan även andra aktörer genomföra upphandlingar baserat på samma regler och med samma förutsättningar, vilket gör det möjligt för övriga sektorer i samhället att forma sina egna identitetsfederationer med passade affärsmodeller, oberoende av de statliga systemen.

Vi tror också att den förlitandemodell som föreslås av e-delegationen komplicerar de juridiska förhållandena på ett onödigt sätt. I e-delegationens förslag betraktas identitetsintygsgivaren som en underleverantör till förlitande part. Vi anser istället att tilliten i federationen bör utgå från identitetsintygsgivarna och låta dessa teckna de nödvändiga förlitandeavtalen med utgivarna (i de fall då dessa inte är samma juridiska person).

Därmed blir det endast identitetsintygsgivarna som federationsoperatören behöver upphandla och teckna avtal med.

Detta tror vi skulle leda till att det på relativt kort sikt etableras en robust och säker infrastruktur för kostnadseffektiv elektronisk identifiering i Sverige, vilket stimulerar innovation och leder till nya affärsmöjligheter, nya tjänster och effektiviseringar inom både näringsliv och offentlig verksamhet. Genom denna bredare användning och större samhällsnytta kommer man också kunna nå målet att infrastrukturen för identifiering bär sina egna kostnader.

Roller och ansvar

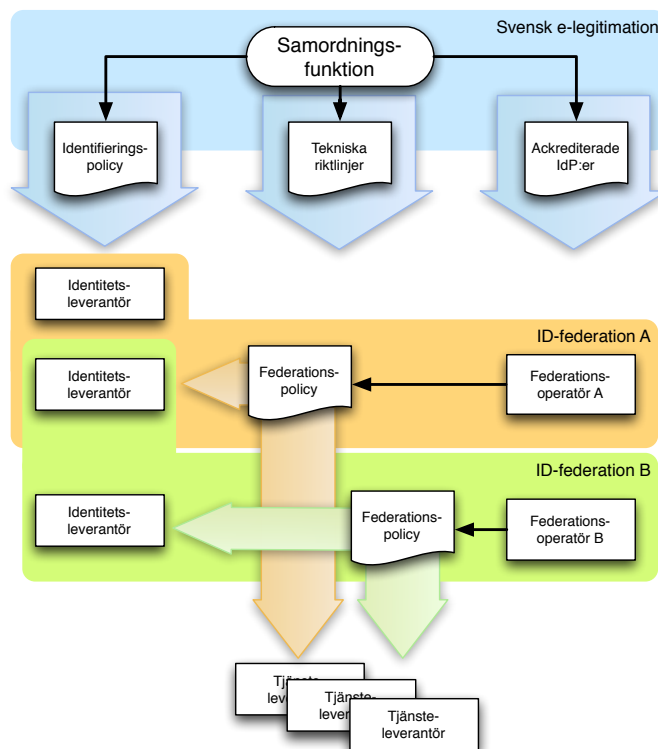
Ett problem med dagens e-legitimation är att det bara är statens behov av identifiering av medborgare som i någon mån uppfylls. Andra sektorer – t.ex. näringslivets behov av säker identifiering hanteras inte alls. Vi menar att det är orimligt att anta att en statlig myndighet kan ta på sig ansvaret att täcka hela samhällets behov av säker identifiering, men genom att dela upp styrning och upphandling på det sätt vi beskrivit ovan kan andra aktörer (t.ex. VHS, SKL, Svenska Handelskamrarna) genomföra egna upphandlingar och etablera identitetsfederationer som uppfyller sina egna behov, men med statens regelverk för *svensk e-legitimation* som bas.

Denna modell ger utrymme för flera helt skilda federationer att samexistera med samma policy och teknik. Varje federation kan ha det affärsupplägg och de avtalsmässiga konstruktioner som krävs för dess medlemmar.

Samordningsfunktionen publicerar den policy som reglerar utgivning och hantering av identiteter. Samordningsfunktionen publicerar också de tekniska riktlinjer som samtliga aktörer använder för att realisera den tekniska infrastruktur som krävs. Detta är mycket viktigt eftersom det krävs en hög grad av teknisk interoperabilitet för att systemen ska fungera i praktiken.

Samordningsfunktionen ackrediterar också externa aktörer som utför revision och certifiering av identitetsleverantörer gentemot policyn. Detta hand-

Uppgjord Fredrik Ljunggren	Dok.id KIREI-2010-01		
Godkänd	Datum 2010-02-10	Rev A	Referens SOU 2009:86 (delvis)



Figur 1: Roller och ansvar

lar sannolikt om revisionsbolag som redan idag utför liknande revisioner. Samordningsfunktionen publicerar därvid en lista över godkända identitetsleverantörer. Dessa listor används vid upphandling av identifieringstjänster och ingår även som en del av den tekniska infrastrukturen som varje federation förlitar sig på.

Man kan också tänka sig att samordningsfunktionen tillhandahåller registerfunktioner mot t.ex. folkbokföringsregistret och bolagsregistret till de ackrediterade identitetsintygsgivarna. Detta leder sannolikt till en högre kvalitet och lägre kostnader för identifieringstjänsten.

Samordningsfunktionen har således inte någon dyr eller betungande uppgift. Arbetet är i mångt och mycket delegerat till ackrediterade aktörer. Samordningsfunktionen kan om man så vill förlita sig på existerande assurancesramverk för stora delar av policyn – t.ex. Kantara/Liberty IAF. För flera av dessa ramverk finns det redan en etablerad marknad av granskare (ofta revisionsbolag) som gör att man kan komma igång med arbetet på kort tid.

Samordningsfunktionen är inte heller direkt inblandad i teknisk drift — all teknik finns hos federationsmedlemmarna (identitetsleverantörer och tjänsteleverantörer) samt i viss mån även hos federationsoperatörerna. Eventuella

Uppgjord Fredrik Ljunggren	Dok.id KIREI-2010-01		
Godkänd	Datum 2010-02-10	Rev A	Referens SOU 2009:86 (delvis)

registerfunktioner upphandlas lämpligen direkt av respektive registerhållare.

Federationsoperatören är den som för federationens räkning upphandlar identifieringstjänsterna och agerar avtalspart mot både tjänsteleverantörer och identitetsintygsgivare. Federationsoperatören har en juridisk och affärs-mässig roll i att koppla samman ett antal identitetsintygsgivare och tjänsteleverantörer genom federationen. Federationspolicyn är det avtal som stipulerar de affärsmässiga, juridiska och tekniska förutsättningarna inom federationen.

En identitetsfederation blir alltså både ett tekniskt ramverk samt ett avtalsmässigt samarbete som ger de deltagande tjänsteleverantörerna tillgång till en uppsättning identitetsleverantörer. Vilka affärsmodeller som ska gälla blir då en fråga för varje upphandling och inte något som samordningsfunktionen stipulerar.

Identitetsleverantören utför identifiering av innehavaren baserat på en godkänd e-legitimation och utfärdar det elektroniska identitetsintyg som förlitande part kan tolka. Dagens leverantörer av identifiering bör genom kravställning och ekonomiska incitament stimuleras att erbjuda tjänsterna direkt via de gränssnitt som samordningsorganet föreskriver. Det finns dock inget som hindrar att en identitetsleverantör består av en avtalsmässig sammanlutning av utfärdare och en identitetsintygsgivare.

Under en övergångsperiod kan överbrygningsfunktioner etableras. Detta sätt att hantera befintlig teknik är emellertid behäftat med de problem som en centraliserad lösning medför; nämligen kostnadsdrivande teknik, ökad sårbarhet genom att en enskild aktör utför all identifiering och därvid uppstår även problematik med skydd av innehavarnas personliga integritet.

Centralisering förhindrar även bildandet av fler federationer och cementerar den gamla tekniken och de gamla strukturerna. Det är därför helt avgörande att en sådan lösning endast etableras under en i förväg väldefinierad övergångsperiod.

Ett bättre sätt att hantera de gamla metoderna för identifiering vore att låta dem samexistera parallellt med federationstekniken under den period som krävs för att utfärdarna och de förlitande parterna skall hinna anpassa sina system till det nya ramverket.

Därmed behöver inget i dagens system för e-legitimation ändras när detta nya ramverk etableras. Inga av dagens förlitande parter behöver ändra på någon del av sina administrativa eller tekniska rutiner förrän dagens modell slutgiltigt avskaffas.