2010-02-05

.SE:s remissvar angående e-delegationens Strategi för myndigheternas arbete med e-förvaltning

Stiftelsen för Internetinfrastruktur (hädanefter .SE) har ombetts lämna synpunker på e-delegationens *Strategi för myndigheternas arbete med e-förvaltning* (SOU 2009:86). I bilaga samlas i listform de förslag .SE presenterar med anledning av strategin

Användarfokus?

Strategin säger sig ta sin utgångspunkt i användarnas behov. Det är berömvärt. Texten nämner emellertid sällan användaren/medborgaren, och är knapphändig på vad användarfokus ska innebära.

På .SE tror vi att användaren tar sin utgångspunkt i nyttoeffekten av elektronisk kommunikation (och inte effektiviseringsbehovet i staten). Användaren gör troligtvis liten eller ingen skillnad på om man kommunicerar med en privatperson, ett företag elller en myndighet. Användaren förväntar sig med största sannolikhet mycket lättförståeliga e-tjänster, och vill inte behöva hålla ordning på många olika inloggningsförfaranden etc. Detta är relativt självklara synpunkter, men behöver ändå betonas, eftersom användarens alternativ är att helt överge det offentligas e-tjänster, och återgå till traditionella kommunikationskanaler. Det får oss exempelvis att tro att en e-legitimation enbart definerad utifrån några centrala myndigheters behov aldrig kan bli etablerad som en de-facto-standard för identifiering etc. Mer om detta senare.

Om syftet med strategin så långt den kan sammanfattas är att effektivisera staten så att säga koncerninternt, så finns det desto fler saker den inte säger och som vi på .SE gärna skulle se som mer utvecklade förslag från e-delegationen:

Strategin säger mycket lite om användarens/medborgarens integritet i det informationssamhälle som e-delegationen vill bidra till att skapa.

Likaså nämns användarna/medborgarna mycket begränsat när det gäller s.k. e-inclusion, dvs. användarnas åtkomstmöjligheter till elektroniska tjänster (i stor utsträckning kan det tolkas som åtkomst till Internet), användarnas kunskap/alfabetism för elektroniska tjänster, samt deras tillit till tjänsterna.

Nära förknippat med både integritet och tillit till förvaltningens e-tjänster ligger medborgarnas förtroende för myndigheternas informationssäkerhetsarbete.
Även om sådana aspekter inte primärt sorterar under finansdepartementets ansvarsområde, så är de likväl en förutsättning för framgång med e-förvaltning.

I .SE:s årliga undersökning av hälsoläget i .se[1] tittar vi på bl.a. myndigheters och kommuners nätnärvaro med olika utgångspunkter. Resultaten från dessa undersökningar pekar på stora brister i grundläggande infrastruktur, hantering av e-post och skydd av webbapplikationer.

[1] http://www.iis.se/docs/Rapport-Halsolaget-2009-final23.pdf

- ⇨ .SE föreslår att strategin förtydligas med ett uttalat mål, och tillhörande åtgärder för att värna om den enskildes personliga integritet.
- ⇨ .SE föreslår att strategin förtydligas med ett uttalat mål, och tillhörande åtgärder för att öka myndigheternas säkerhet och stabilitet när det gäller system och infrastruktur för elektronisk kommunikation.
- ⇨ .SE föreslår att strategin förtydligas med ett uttalat mål, och tillhörande åtgärder för att öka myndigheternas informationssäkerhetsarbete, med syfte att öka användarnas tillit till tjänsterna.

Delegationens och myndigheternas arbetsmetod
Att strategin innhåller krav på såväl mätbara och uppföljningsbara mål, som pekar ut utvecklingsansvariga myndigheter är ett symptom på att planeringen av arbetet gått framåt. Mål och utpekat ansvar är två förutsättningar för att realisera arbetet. Insikten att arbetet komer att ta tid (år 2014), samt att den baseras på en stegvis och efterfrågedriven utveckling pekar också på ett visst mått av realism.

Det är positivt att delegationen ska ta fram en vägledning för myndigheternas verksamhetsplanering för e-förvaltning. I slutändan är det nog dock finansieringen av den behovsdrivna e-förvaltningen som är nyckeln till framgång i arbetet. Förslaget om extern finansiering är en klok metod att skapa och synliggöra rimliga incitament för respektive myndighet. Metoden undanröjer emellertid inte risken för att arbetet för en sammahållen e-förvaltning efter hand sjunker ner i sediment av politisk prioritering, och att Vinnovas forsknings- och utvecklingsmedel dräneras på resurser som skulle kunna användas på ett bättre sätt och till hela samhällets fromma, inte bara den offentliga förvaltningen.

E-delegationen söker ett långsiktigt mandat för sin strategi. Ur ett politiskt perspektiv är e-förvaltning inte heller särskilt kontroversiellt. Det borde därmed vara möjligt att nå en politisk konsensus i stora delar av strategin. För att säkra ett långsiktigt arbete bör regeringen underkasta riksdagen att besluta om fortsatt arbete för e-förvaltning. Motsvarande gjordes exempelvis då riksdagen beslutade om 15 (sedermera 16) miljökvalitetsmål. Att vidga arbetet för e-förvaltning till riksdagen ökar möjligheterna för kontinuitet i arbetet, och i viss mån en säkrare finansiering. Kontinuiteten i arbetet är också angelägen med tanke på att denna strategi är åtminstone den tredje omstarten för ett nationellt arbete med e-förvaltning.

- ⇨ .SE föreslår att regeringen underkastar riksdagen att besluta om mål för förvaltningsutveckling, bl.a. med hjälp av IT.

En strategi för ett eller flera mål?

Med strategi menas vanligtvis en metod att nå ett eller flera mål. Enligt strategins sammanfattning ska myndigheterna ”*…öka sin produktivitet och effektivitet…*” samt ”*…öka samhällets utvecklingsförmåga och innovationskraft genom e-förvaltning.*”

Det första målet skulle kunna liknas vid ett allt igenom internt effektiviseringsarbete inom staten, betraktad som en koncern. Som tur är preciseras målbilden exempelvis på sid 31 i att e-förvaltning är en form av kontinuerlig verksamhetsutveckling, med mera.

Detta andra mål antyder att ett samordnat statligt agerande skulle bidra till innovation i samhället i stort. Målet är emellertid inte lika distinkt formulerat, och lämnar därför öppet för tolkning av vad det kan innebära i praktiken.

Det offentliga är enbart genom sin storlek en dominerande aktör för en god utveckling av informationssamhället. En harmoniserad offentlig sektor kan med rätt ledning förmås anta en

stark normgivande roll för mycket mer än rent 'koncerninternt' effektiviseringsarbete i myndigheterna.
Rätt hanterad kan myndigheternas strategi för arbete med e-förvaltning uppfylla viktiga politiska mål också *utanför* finansdepartementets specifika ansvarsområde. Det offentligas dominerande roll i informationssamhället kan, rätt använd, bidra till exempelvis inte bara IT-politiska, utan även arbetsmarknadspolitiska, tillväxtpolitiska och miljöpolitiska målsättningar. Rätt hanterad kan myndigheternas arbete med att utveckla e-förvaltningen till och med bidra till utveckling av nya företag, produkter och nya avsättningsmarknader.

Tyvärr gäller även det omvända. Om målet för det offentligas roll i informationssamhället inte är kristallklart, och åtgärderna i strategin som en följd därav inte utformas på rätt sätt, kan det lika gärna komma att utgöra hinder för utvecklingen på motsvarande politikområden. Detta fenomen exemplifieras under kommentarerna om e-legitimationer, men gäller i princip för de flesta områden som strategin avser.

Detta problem refereras ofta som "stuprören i staten", något som i högsta grad är aktuellt i denna strategi. Strategin är *det* starkaste instrument staten har att tillgå för att bidra till utveckling för elektronisk kommunikation i flera andra sektorer. Det vore olyckligt om staten inte nyttjar den möjligheten. Otydligheten i det andra målet riskerar emellertid att leda till en walk-over i politisk ledning och i politisk vilja, och strategin riskerar då att reduceras till det första målet om koncernintern effektivisering av statens administration. På .SE efterfrågar vi därför ett förtydligande av målets betydelse.

- ⇨ .SE föreslår fler och tydligare mål med högre konkreetisering för de sektorer som strategin kan bidra till.

e-legitimationer

Utmärkande för informationssamhället är att omvandlingstrycket är stort, och att det är svårt att förutse vilken inriktning teknikutvecklingen tar. Dagens system för e-legitimationer kan vi konstatera är exkluderande i det att alla användare inte kan få en e-legitimation. De är slutna i betydelsen att de förutsätter vissa förbestämda operativsystem och programvaror. De är bundna i betydelsen att de förutsätts användas i en persondator. De baseras på en affärsmodell som i huvudsak tillgodoser behoven hos ett fåtal centrala myndigheter. På utbudssidan utgör de ett oligopol där endast ett fåtal aktörer tillhandahåller e-legitimationer, något som inte bidrar till konkurrensens positiva sidor i produktutveckling och prispress. På .SE anser vi att det finns mer att önska av dagens system för e-legitimationer. Vi har också gett uttryck för våra åsikter om att utgångsläget för federerad eID i Sverige bör:

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

Det användarperspektiv som e-delegationen nämner inledningsvis lyser här med sin frånvaro. Enligt befintlig text finns exempelvis inga planer på att tillhandahålla möjlighet till identifiering mellan individer. Inte heller tycks man ha som ambition för myndigheter att kunna legitimera sig gentemot individer eller företag, en minst lika viktig funktion i ett fungerande informationssamhälle.

Vi vill vända på resonemanget, och utifrån användarens behov presentera en önskelista på e-legitimationer.

Metoden för identifiering och signaturer ska kunna väljas av användaren.[2] Målet bör vara en marknad för e-legitimationer där ett flertal aktörer vill ge ut e-legitimationer, med en mångfald av tekniska lösningar och säkerhetsnivåer i utbudet. Allmänhetens förväntan på en e-legitimation baseras på att den ska uppfylla lika många funktioner som den traditionella legitimationen gör. Det betyder t.ex. att den inte definieras utifrån det offentligas behov, utan likaväl ska kunna användas av företag och individer. Alla behöver kunna indentifera sig elektroniskt inför varandra, oavsett roll eller sammanhang. Legitimationerna behöver vara mobila, och finnas i en sådan mångfald av lösningar att de tekniskt sett blir plattformsoberoende.

E-delegationen föreslår en s.k. federationslösning för e-legitimationer. På .SE välkomnar vi förslaget som modell, och som ett steg i rätt riktning mot ovanstående önskelista. Vår övertygelse är att man med denna modell enkelt kan åstadkomma samordning av federationer inom både stat, kommun, landsting och privat sektor kan ske på ett effektivt sätt och till en mycket låg kostnad. Se mer på http://www.kirei.se/2009/10/19/eid-i-sverige/

- ⇨ .SE välkomnar förslaget till en federationslösning för identifiering och autenticering i elektronisk kommunikation och förutsätter att e-delegationen bjuder in expertis på området till fortsatta diskussioner om detaljerna kring en sådan lösning.

Affärsdimensioner av en e-legitimation
E-delegationens förslag bygger på att en samordningsfunktion ska etableras i Nämnden för e-samordning. På .SE välkomnar vi den samordnande funktionen. Vi ställer oss emellertid helt oförstående till förslaget om *en* upphandlande funktion för försörjning av e-legitimationer till det offentliga. En sådan lösning skapar ett monopol i efterfrågan, och kommer troligtvis att *motverka* teknikutveckling och produktutveckling. Det kommer troligtvis bibehålla situationen med ett oligopol i utbudet, dvs. undanröja förutsättningarna för en dynamisk marknad av mångfald i tjänster. Det kommer troligtvis att leda till en tjänst för alla sammanhang och e-tjänster, en lösning som är både tekniskt onödig och informationsekonomiskt osund. Det får därmed en direkt motverkande effekt mot s.k. identitetsfederationer.

SE delar inte heller uppfattningen att federationssamordnaren nödvändigtvis ska drivas av det offentliga. Mer om detta nedan.

Det tidigare problemet med affärsmodellerna
I de tidigare affärsmodellerna för e-legitimationer som utvecklades på 1990-talet och i början av 2000-talet uppstod problem eftersom volymerna av utfärdade e-legitimationer var för små för den befintliga affärsmodellen. Både affärsmodellerna och e-legitimationerna definierades utifrån ett begränsat behov hos ett fåtal myndigheter, och av en oligopolsituation i utbudet. Modellerna förutsatte t.ex. en enkelriktad kommunikation, dvs. myndighetens behov av att identifiera individen (men inte tvärtom).

Att det idag inte finns några tillgängliga federationssamordnare på den svenska marknaden kan i stor utsträckning härledas till de (bakvända) affärsmodeller som definerades vid denna tidpunkt. Det är emellertid inte ett rimligt argument för att sådana samordnare inte skulle kunna uppstå idag.[3]

---

[2] I detta sammanhang blir alltså den s.k. Anvisningstjänsten enligt Stragetings terminologi endast aktuell vid e-tjänster tillhandahållna av myndigheter.
[3] Jfr. s 121 Likaså är det inte rimligt att regeringen avstår från åtgärder med hänvisning till ”Dagens juridiska strukturer…” (samma sida). Det är ju regeringens huvudsakliga uppgift att föreslå ändring av sådana strukturer.

Förslaget
Staten har monopol på att definiera individens identitet. Det sker främst i form av personnummer. Det är så långt statens unika roll sträcker sig. Alla andra moment i e-legitimationerna kan utföras av för ändamålet bättre lämpade aktörer.

Medborgarnas identitet och andra egenskaper noteras i folkbokföringen, resp aktiebolagsregistret. För att underlätta för framväxten av en marknad för e-legitimationer och andra elektroniska tjänster som förmedlar identifiering och autenticering skulle staten kunna tillhandahålla folkbokföringen i elektronisk form till alla företag som klarade en fördefinerad ackreditering.[4] Det skulle ske kostnadsfritt och under kontrollerade former. Företag har sedan att tillhandahålla tjänster som tillgodoser ett reellt behov utifrån användarnas behov.[5]

Genom en sådan ordning skulle staten renodla sin roll, och med strategins terminologi anta rollen som registerhållare. Företag skulle sedan ha möjlighet att etablera ett helt ekosystem av olika identifieringstjänster, specialutformade för ändamål, sammanhang, och aktuellt säkerhetsbehov, men baserade på den säkerhet som det innebär att staten står för en identifieringen.[6] Detta är en tillämpning av tankarna i det s.k. PSI-direktivet, dvs. att offentlig data vidareutnyttjas för andra ändamål än de ursprungligen samlats in för.

Affärsmässigt innebär förslaget en möjlighet till en fungerande marknad. Marginalkostnaden för en elektronisk transaktion (t.ex. en elektronisk signatur) i dessa sammanhang är mycket liten. Den stora kostnaden är att upprätthålla ett register. Om staten tillhandahåller detta register kostnadsfritt, kan tjänster tillhandahållas nära marginalkostnaden för en elektronisk transaktion (maximalt några kronor), i stället för uppåt 30-40 kronor per transaktion, som varit aktuellt i tidigare affärsmodeller. Det är t.o.m. troligt att några aktörer skulle tillhandahålla sådana e-legitimationer kostnadsfritt (genom s.k. s.k. bundling, eller paketering av tjänster).

Den föreslagna affärsmodellen är också motsatsen till en central upphandling. Den är i stället ytterst decentraliserad, där uppemot 300 myndigheter och 300 kommuner och landsting själva beställer identifierings- och autenticieringslösning beroende på sammanhang. När tjänsterna utformas decentraliserat utifrån användarnas behov, kan de också användas av alla andra i samhället som efterfrågar motsvarande tjänster, dvs. företag och enskilda.

- ⇨ .SE föreslår att Skatteverket kostnadsfritt tillhandahåller delar av folkbokföringen i elektronisk form till företag och andra aktörer som i sin tur vill tillhandahålla elektroniska tjänster baserade på identifiering och autenticering. På motsvarande sätt tillhandahålls bolagsregistret. Nämnden för e-samordning ska utforma och upprätthålla ett ackrediterings- eller licensieringssystem för dessa företag.

IPv6

När datorer kommunicerar med varandra över Internet använder de regler för kommunikationen, så kallade protokoll. Det mest spridda är Internet-protokollet, IP. Dagens Internet domineras fortfarande nästan helt av den fjärde versionen av detta protokoll, som betecknas IPv4 och som togs fram redan på 80-talet.

---

[4] Statens åtagande skulle mao. begränsas till att agera ”registerhållare”, samt möjligtvis för vissa offentliga tjänster ”anvisningstjänst”.
[5] .SE delar alltså inte uppfattningen att federationssamordnaren nödvändigtvis ska drivas av det offentliga. Eftersom användaren i sin elektroniska kommunikation via Internet når hela världen, kommer det att behövas flera parallella federationssamordnare, helt oavsett var gränsen till Sverige dras.
[6] Företag skulle kunna tillhandahålla parallella anvisningstjänster resp. agera som identitetsintygsgivare.

Att IPv4 har funnits länge är inget problem i sig. Standarderna på Internet utvecklas kontinuerligt och mycket av den infrastruktur som är på plats i dag bygger på teknik som ursprungligen utvecklades på 1970- och 80-talen. Det finns dock ett stort, för att inte säga oöverstigligt, problem med IPv4 som man känt till sedan länge men som nu gör sig alltmer påmint.

Problemet hänger samman med att de så kallade IP-adresserna, det vill säga den unika nummer som identifierar varje ändutrustning – t.ex. dator, skrivare, router, accesspunkt - ansluten till Internet. I IPv4 består adressen av 32 databitar. Det innebär att det bara kan finnas drygt fyra miljarder unika IP-adresser. Det orsakade inga som helst problem 1981, men i takt med att världen blir alltmer uppkopplad uppstår det helt enkelt adressbrist på Internet.

Eftersom det var välkänt redan på 1990-talet att IP-adresserna skulle kunna ta slut, tog man initiativet till en ny version av IP-protokollet som fick namnet IPv6. Under detta årtionde utvecklades emellertid också ett antal andra, mer kortsiktiga tekniker, som gjorde att det gick att komma runt problemen och därmed kunde man skjuta upp arbetet med att sjösätta en helt ny standard. Det är också så man har löst problemet så här långt.

Det starkaste argumentet för att gå över till IPv6 har alltid varit och är fortfarande att man får fler adresser. Det är kanske den främsta orsaken till att övergången måste ske med kniven mot strupen, nu när adressbristen börjar bli akut. Men även om det inte låter så upphetsande med fler adresser i sig, så möjliggör det faktiskt en massa tillämpningar som annars blir svåra att genomföra.

Själva tekniken håller nu på att bli så billig att vad som helst kan kopplas upp till Internet, vilket öppnar för intressanta tillämpningar inom till exempel hemelektronik och telefoni. Det har länge talats om smarta hus och en del exempel som används framstår lätt som lite fåniga, och uttjatade som att kylskåpet själv beställer mjölk.

Internet håller verkligen på att sprida successivt sig från datorerna till ”prylarna”. Mediaspelare, mobiltelefoner, elektroniska fotoramar, Internet-telefoner, elektroniska anslagstavlor, hemautomatisering, larm m.m.

Genuint smarta lösningar med verklig nytta kan byggas för till exempel system för uppvärmning, där sensorer kan känna av värme från solljus och minska temperaturen på värmeelementen i de rum av huset som vetter mot solen.

Transportsektorn vill också ha kommunikation. Lastbilar och annan utrustning kan samla information om utnyttjande och slitage och tidsbokning för service kan göras individuellt per fordon istället för att göra det enligt schabloner. Kartor, rutter och annan kommunikation kan enkelt förmedlas från en ledningscentral till chauffören. Trådlös kommunikation i en lastbil, på en båt eller tåg kan spåra försändelser och prognoser för ankomst etc. kan räknas fram.

Hur ser då situationen ut för IPv6 i nuläget? Hur är förutsättningarna för att börja använda det, när det nu brådskar så? Faktum är att det redan i dag finns ett världsomspännande, nära på heltäckande nät. Alla stora operatörer har stöd för IPv6 och det har kunnat genomföras utan några större investeringar. Troligen har runt 80 procent av världens Internetleverantörer infört IPv6-stöd. Det som fattas är den sista biten ut till användarna, så för att använda IPv6 i dag måste de allra flesta utnyttja något som kallas tunnelteknik.

I det här sammanhanget är det värt att understryka att det finns ett viktigt värde i att försvara Sveriges traditionella roll som föregångsland vad gäller Internet. Just i och med att vi har varit långt framme finns kanske inte samma behov av fler IP-adresser som på andra håll, så det

argumentet är starkare i till exempel Asien. Men hur går det för ett Sverige där man fortfarande bara använder IPv4 om det blir så att många webbplatser och -tjänster på det internationella planet endast går att nå via IPv6? Webbtjänster som Google och Microsoft har redan byggt ut sitt stöd för att vara redo när anstormningen kommer, så detta är definitivt ett framtidsscenario att räkna med.

Ett ytterligare argument för införandet av IPv6 är att i takt med att IPv4-adresserna blir svårare att erhålla kommer också möjligheten för nya aktörer att etablera sig på marknaden att minska. Att t.ex. Telia Sonera har tillräckligt med adresser blir i detta fall nästan ett problem då det gör att de får en ännu mer dominerande ställning på marknader som redan idag skulle behöva mer konkurrens.

Enligt de prognoser som finns kommer möjligheten att tilldelas nya adresser att bli väldigt dålig så snart som i början av 2012 och för att inte hamna i ett nytt år 2000-scenario är det viktigt att påbörja arbetet så snart som möjligt.

En del kommuner har tagit initiativ till att införa IPv6, utvecklingen går att följa på http://www.kommunermedipv6.se/.

- ⇨ .SE föreslår att det i regeringens uppdrag till kammarkollegiet uttryckligen ska framgå att ramavtal ska omfatta IPv6 som ett krav som inte får undantas.

DNS och DNSSEC

Domännamnssystemet är en av hörnstenarna på Internet och är till för att förenkla adressering av resurser på Internet. Det är viktigt att varje verksamhets egen DNS-infrastruktur ansluter till aktuell standard och är konstruerad på ett sätt som gör att den tillhandahåller en stabil tjänst med god nåbarhet, vare sig man driver DNS själv eller har lagt ut driften på någon extern partner.

En årlig undersökning som .SE företar visar att det finns bristande kunskaper om vad som krävs för att hålla en hög kvalitet på DNS. Omfattande fel och brister är relativt vanligt förekommande och påverkar i allra högsta grad tillgången till tjänster inom e-förvaltningen.

DNS Security Extensions (DNSSEC) är ett säkrare sätt att göra uppslagningar på Internetadresser för exempelvis webb och e-post. Till skillnad från det vanliga domännamnssystemet (DNS) är uppslagningar med DNSSEC kryptografiskt signerade, vilket gör det möjligt att säkerställa både att de kommer från rätt avsändare och att innehållet inte har ändrats under överföringen.

För gemene man innebär det att risken för att bli lurad vid till exempel bankaffärer eller shopping på nätet minskar, eftersom det blir lättare för användaren att fastställa att man verkligen kommunicerar med rätt bank eller butik snarare än med en bedragare.

PTS konstaterar att "*Dagens svenska samhälle är beroende av att Internet fungerar tillfredsställande vilket även inbegriper det för användbarheten kritiska domännamnssystemet (DNS). Falsk DNS-information medför risk för att e-posttrafik leds till oönskat ställe, annans information stjäls eller att transaktioner störs*." Mer om PTS syn går att läsa i PTS-ER-2006:36.

Det är dock viktigt att notera att DNSSEC inte stoppar alla typer av bedrägerier. Det är endast konstruerat för att förhindra attacker där angriparen manipulerar svar på DNS-frågor för att uppnå sitt mål.

2008 fick forskaren Dan Kaminsky på allvar upp säker DNS på Internetvärldens agenda och .SE fick därmed stort internationellt genomslag för sitt arbete med säkrare DNS-uppslagningar. Det som presenterades kom att kallas Kaminskybuggen. Han demonstrerade ett nytt och mycket enkelt sätt att genomföra en sedan tidigare känd attack mot DNS och på så sätt möjliggöra för en angripare att styra om anrop från t.ex. kända webbsidor till angriparens egen i syfte att t.ex. komma över inloggningsuppgifter eller andra personuppgifter. Detta understryker vikten av att införa DNSSEC.

Under 2010 kommer DNSSEC att införas centralt för all DNS-hantering på Internet och även på ett större antal topp-domäner motsvarande .se. Det verkar som om detta år blir det år då DNSSEC på allvar slår igenom i hela världen.

- ⇨ .SE föreslår att det i regeringens uppdrag till Kammarkollegiet uttryckligen skall framgå att ramavtal skall omfatta DNSSEC som krav som inte får undantas.
- ⇨ .SE föreslår att e-delegationen definierar en branschstandard för DNS-tjänst med kvalitet.

Det har redan initierats en inventering av vilka offentliga aktörer som använder DNSSEC. På följande adresser finns en uppdatering. http://www.kommunermeddnssec.se/, http://www.myndighetermeddnssec.se/, http://www.landstingmeddnssec.se/

Eventuella frågor angående remissen besvaras av Staffan Jonson
Telefon 073-317 39 67, eller e-post: staffan.jonson@iis.se

Med vänlig hälsning

{Signerat}

Danny Aerts

Bilaga

Samlad uppställning av :SE:s förslag med anledning av strategin:

- .SE föreslår fler och tydligare mål med högre konkretisering för de sektorer som strategin kan bidra till.
- .SE föreslår att strategin förtydligas med ett uttalat mål, och tillhörande åtgärder för att värna om den enskildes personliga integritet.
- .SE föreslår att strategin förtydligas med ett uttalat mål, och tillhörande åtgärder för att öka myndigheternas säkerhet och stabilitet när det gäller system och infrastruktur för elektronisk kommunikation.
- .SE föreslår att strategin förtydligas med ett uttalat mål, och tillhörande åtgärder för att öka myndigheternas informationssäkerhetsarbete, med syfte att öka användarnas tillit till tjänsterna.
- .SE föreslår att regeringen underkastar riksdagen att besluta om mål för förvaltningsutveckling, bl.a. med hjälp av IT.
- .SE välkomnar förslaget till en federationslösning för identifiering och autenticering i elektronisk kommunikation.
- .SE föreslår att Skatteverket kostnadsfritt tillhandahåller delar av folkbokföringen i elektronisk form till företag och andra aktörer som i sin tur vill tillhandahålla elektroniska tjänster baserade på identifiering och autenticering. På motsvarande sätt tillhandahålls bolagsregistret, Nämnden för e-samordning ska utforma och upprätthålla ett ackrediterings- eller licensieringssystem för dessa företag.
- .SE föreslår att det i regeringens uppdrag till kammarkollegiet uttryckligen ska framgå att ramavtal ska omfatta IPv6 som ett krav som inte får undantas.
- .SE föreslår att det i regeringens uppdrag till kammarkollegiet uttryckligen skall framgå att ramavtal skall omfatta DNSSEC som krav som inte får undantas.
- .SE föreslår att e-delegationen definierar en branschstandard för DNS-tjänst med kvalitet.

Det har redan initierats en inventering runt vilka offentliga aktörer som använder DNSSEC. På följande adresser finns en uppdatering. http://www.kommunermeddnssec.se/, http://www.myndighetermeddnssec.se/, http://www.landstingmeddnssec.se/