

A photograph of a woman with dark hair carrying a young boy on her shoulders. The boy is wearing a red t-shirt and blue jeans, and is smiling broadly. The woman is wearing a dark blue top and is looking up at the boy with a smile. They are in a backyard with a wooden deck, a table with chairs, and a house in the background. The text "E-legitimation för säkra e-tjänster" is overlaid on the image in white.

E-legitimation för säkra e-tjänster

Lägesrapport från 24-timmarsdelegationen
Februari 2005

ett öppnare och
enklare Sverige

24SJU 

Till Statsrådet Sven-Erik Österberg

24-timmarsdelegationen (kallas i det följande normalt enbart "delegationen") skall enligt direktiven:

- identifiera områden i offentlig sektor där e-tjänster har en potential att skapa stor nytta för medborgare och företag samt effektivisera offentlig sektor, men där det finns hinder som behöver undanröjas eller skäl att påskynda utvecklingen samt ta initiativ till åtgärder för att driva på utvecklingen inom dessa områden,
- pröva nya vägar att öka samverkan mellan staten, kommuner och landsting samt mellan offentlig sektor och andra aktörer vid utveckling och tillhandahållandet av elektroniska tjänster,
- initiera samverkansprojekt med näringslivet,
- främja kunskapsöverföring mellan forskning och utveckling och framtagandet av praktiska och nyttskapande elektroniska tjänster, bedöma behov av och former för särskilda stödinsatser för utvecklingen av elektroniska tjänster,
- stimulera utnyttjandet av kombinerade servicekanaler såsom t ex avancerad telefonservice och servicekontor genom vilka medborgare och företag kan erbjudas personlig hjälp med att utnyttja de elektroniska tjänsterna,

- pröva vilka typer av elektroniska tjänster som kan vara lämpliga att leverera via nya kommunikationsplattformar såsom mobila elektroniska kommunikationssystem och interaktiv digital-TV.

Delegationen skall arbeta åtgärdsinriktat.

Delegationens inriktning

Delegationens uppgift är att förenkla kontakter med offentliga aktörer genom e-tjänster. Utgångspunkt är användarens - individens respektive företagets - behov. Tjänsterna skall ha hög tillgänglighet, med teknik anpassad efter användarens förutsättningar samt god och likvärdig service, oavsett lokalisering och tidpunkt. Hög grad av flexibilitet, och en långtgående samverkan mellan de olika offentliga aktörerna erfordras. En utveckling mot fler eller förnyade e-tjänster skall frigöra resurser och bidra till att utveckla kvaliteten i verksamheten.

Delegationens arbetsmetodik i övrigt har beskrivits i det första delbetänkandet.

Delegationen överlämnar här sin lägesrapport e-legitimation för säkra e-tjänster.

Eva Fernvall
Ordförande

1. Sammanfattande synpunkter

Delegationen förordar i denna lägesrapport e-legitimationen som en gemensam säkerhetslösning för e-tjänster inom den offentliga sektorn.

Delegationen har regeringens uppdrag att enligt direktiven, Delegationen för utveckling av offentliga e-tjänster (dir 2003:81), främja utvecklingen av e-tjänster inom den offentliga sektorn. I maj 2004 överlämnade delegationen sitt delbetänkande, e-tjänster för alla (SOU 2004:56). I delbetänkandet presenteras delegationens mål samt arbetsmetoder. Inriktningen av delegationens insatser avser att utgå från individers olika livssituationer. Ett antal sådana har definierats i delbetänkandet.

Ett antal insatser pågår inom den offentliga sektorn i syfte att utveckla e-tjänster. En sådan viktig aktör i utvecklingen av e-tjänster är Statskontoret, som särskilt stödjer utvecklingen med upphandlingar, metod och teknik, i första hand för det statliga området. Utvecklingen i sig görs av respektive myndighet. Regeringen har därutöver beviljat vissa myndigheter särskilt stöd för utvecklingen av e-tjänster. För utvecklingen av IT inom hälso- och sjukvården har en överenskommelse slutits mellan regeringen och Landstingsförbundet om ett antal insatser. Delegationen är av den uppfattningen att ett statligt stöd i syfte

att stimulera kommuner att i samverkan utveckla e-tjänster som ökar effektiviteten och skapar nytta för medborgare och företag ligger i linje med övriga stödsatser.

E-tjänster erbjuder möjligheten för personer och företag att med en kontakt få tjänster utförda där flera aktörer inom den offentliga sektorn är inblandade samt bidra med kostnadseffektiva lösningar. Delegationen är en av de få aktörer som har förutsättningar att stimulera utvecklingen av e-tjänster som är gemensamma för stat, landsting och kommun. För att en sådan insats skall bli framgångsrik måste alla delar av den offentliga sektorn sluta upp kring en gemensam ide där alla delar tar sitt tydliga ansvar. Den främste bäraren av en sådan sammanhållande ide är regeringen.

För att säkert och enkelt kunna använda e-tjänster behövs en gemensam syn på säkerhet. Delegationen har behandlat denna fråga i nära kontakt med företrädare för Statskontoret, e-nämnden, IT-strategigruppen, Skatteverket, Svenska Kommunförbundet m fl. På initiativ av delegationen har en utredning bedömt säkerhetsbehovet för fem e-tjänster¹. Utredningen innehåller även en metod för säkerhetsbedömning av e-tjänster.

¹ Förnyad ansökan om ekonomiskt bistånd, gymnasieval, medborgarassistenten, ansökan om barnomsorg samt föreningsbidrag och lokalbokning

Medborgarna behöver också kunna identifiera sig på ett enhetligt sätt gentemot aktörerna inom den offentliga sektorn. Detta kan ske genom att medborgarna använder en så kallad e-legitimation. Bankerna, Telia och Steria marknadsför sedan ett par år sådana e-legitimationer. Statskontoret har av dessa leverantörer upphandlat tjänster för verifiering av e-legitimationer. Lösningen med e-legitimation är utvecklad för att användas både inom offentlig och privat verksamhet. Detta är en fördel eftersom medborgarna då inte behöver skaffa en särskild e-legitimation för att kunna utföra tjänster inom den offentliga sektorn.

För att e-legitimationen skall kunna användas inom den kommunala sektorn krävs dock att kommunerna gör väsentliga IT-investeringar. Kommunerna har som regel en splittrad systemstruktur och saknar oftast ett för alla system gemensamt behörighetsregister. Företrädare för kommunerna anser vidare att

kommunerna inte kan bära kostnader för att verifiera e-legitimationens giltighet.

Delegationen är dock trots dessa invändningar av den uppfattningen att e-legitimationen uppfyller ställda säkerhetskrav samt bör utgöra den gemensamma säkerhetslösningen för e-tjänster inom den offentliga sektorn.

Slutligen vill delegationen beröra regeringens beslut om utvecklingsresurser till delegationen. Delegationen har en relativt god framförhållning när det gäller stöd till olika insatser. Av de åtta miljoner som tilldelats delegationen kan fyra miljoner användas under 2005. Delegationen har under sin verksamhet kommit till insikten om nödvändigheten av en mer omfattande informationsinsats. Planeringen av denna inleddes under 2004 och vissa insatser har påbörjats. Huvudparten av de resurser som ställts till delegationens förfogande under 2004 kommer att användas för denna informationsinsats.

2. E-legitimation och medborgarnas tillit

Tillitsfrågan är av avgörande betydelse för användningen av e-tjänster. Medborgaren måste t ex ha förtroende för att de uppgifter och handlingar som lämnas till eller fås av myndigheten via Internet hanteras på ett säkert och riktigt sätt. Både myndigheter och allmänheten skall kunna förmedla information elektroniskt med samma tillit och legala verkan som när man skickar information i form av dokument med handskriven underskrift.

Man kan i huvudsak lägga tre aspekter begreppet tillit (ITPS rapport A2003:15):

- Funktionaliteten: att användaren litar på att den fysiska utrustningen kommer att fungera.
- Datasäkerheten: att användaren kan skydda sin trafik, identifiera sig själv och andra och vara säker på att rätt meddelande kommer till rätt mottagare.
- Integritetsfrågorna: att medborgarna är skyddade mot att ”storbror kan se dig”.

Det kan också noteras att IT-politiska strategigruppen tagit fram en rapport kring tillitsbegreppet.

Inom ramen för säkerhetsfrågor arbetar flera EU-länder på att skapa en enhetlig legitimation som garanterar identifikation och säker överförbarhet. Arbetet bygger på ett EU-direktiv, infört i svensk lagstiftning som lagen om elektronisk signatur. Det anses viktigt att skapa ett enhetligt system – åtminstone på nationell nivå men helst inom hela EU. Man

eftersträvar att göra systemet generellt för både offentlig och privat verksamhet. Poängen är att individen enbart skall behöva använda en identifieringshandling vid användning av Internetbaserade tjänster oavsett om tjänsten är i offentlig eller privat regi.

2.1 Vad är en e-legitimation?

En e-legitimation är en elektronisk ID-handling med vars hjälp en individ kan legitimera sig på nätet. E-legitimationen innehåller oftast de uppgifter som behövs för att identifiera en individ elektroniskt t ex namn, personnummer, legitimationens giltighetstid osv. Men dessa uppgifter behöver inte lagras i den elektroniska ID-handlingen utan kan också levereras av utgivaren på förfrågan om vem en viss unik elektronisk ID-handling tillhör. I sådant fall innehåller ID-handlingen en unik beteckning som på ett säkert sätt kan knytas till en person. Den gemensamma nämnaren för alla e-legitimationer är att de baseras på sk PKI (Public Key Infrastructure) som mycket kortfattat kan beskrivas som ett system för kryptering där avsändaren och mottagaren har varsin krypteringsnyckel, en privat och en publik nyckel.

2.2 Identifiering med e-legitimation - ett samspel mellan olika aktörer

Den offentliga sektorn har över tre miljoner unika

besökare under en månad på sina webbsidor. Många av dem utför de tjänster över nätet som den offentliga sektorn erbjuder. För att offentliga aktörer skall kunna erbjuda e-tjänster så behövs lösningar för elektronisk identifiering och underskrift. Det underlättar naturligtvis för individen att enbart behöva använda sig av en typ av e-legitimation, vare sig man som kund i ett företag använder privata e-tjänster eller som medborgare brukar offentliga e-tjänster. Sådana lösningar tillhandahålls av marknaden.

I ett system för identifiering och signering med certifikat finns fyra aktörer. Innehavaren är den som ska identifieras. Tjänsten är den som har behov av att identifiera motparten. Utfärdaren är den som ställt ut certifikatet. Leverantören av verifieringstjänst är den som gentemot Tjänsten ansvarar för verifieringen av certifikatet.

Samspelet mellan dessa aktörer innebär att Utfärdaren ger ut certifikatet till Innehavaren och avtalar med denne om de villkor som gäller för certifikatet. Innehavaren använder sedan certifikatet mot Tjänsten för identifiering och underskrift i enlighet med de regler som gäller mellan Innehavaren och Tjänsten. För att kontrollera certifikatets äkthet vänder sig Tjänsten till Leverantören av verifieringstjänst enligt det affärsavtal Tjänsten har med leverantören. Leverantören av verifieringstjänst kontrollerar certifikatet hos aktuell Utfärdare i enlighet med de regelverk och affärsavtal som finns mellan Leverantören och Utfärdarna.

Tjänsten kan även användas för kryptering och därmed för att säkerställa att dokument inte förvanskas medvetet eller omedvetet. Därutöver används tjänsten till att signera dokument.

2.3 Myndigheters användning av e-legitimation

Ett avgörande steg i utvecklingen av 24-timmarsmyndigheten är att kunna skicka och ta emot viktiga handlingar elektroniskt samt att kunna hantera förtrolig information i en direkt kommunikation via Internet. Både myndigheter och allmänheten skall kunna förmedla information elektroniskt med samma tillit och legala verkan som när man skickar information i form av dokument med handskreven underskrift eventuellt på myndighetens papper.

I mer än trettio år har det funnits metoder för att åstadkomma säker och förtrolig dialog mellan datorer över nätverk. Med sådana metoder kan man belägga identiteten hos den man kommunicerar med och föra en förtrolig dialog samt kontrollera att de meddelanden som utväxlas inte har blivit förvanskade. Sverige har varit ett föregångsland på området ”säker och förtrolig elektronisk kommunikation”. Under 1990-talet bedrevs ett framgångsrikt standardiseringsarbete och flera stora installationer av denna teknik gjordes inom svenska myndigheter.

Trots att tekniken finns och trots att det finns erfarenheter av den i landet har det visat sig svårt att ta steget från att förse en avgränsad grupp användare, t ex de anställda inom en myndighet eller på ett sjuk-

hus, med metoder för säker elektronisk kommunikation till att ge sådana möjligheter till allmänheten i 24-timmarsvisionens anda. För den avgränsade gruppen kan man ha kontroll över tekniken, utbilda användarna och styra användningen. För 24-timmars-tjänster gäller det att ge allmänhet tillgång till lösningar för säker elektronisk kommunikation med den teknik man har i hemmen och mot de tillämpningar som är intressanta. Detta utan att staten tvingas till stora och teknikberoende investeringar.

Olika tjänsteleverantörer har utvecklat identifieringsmetoder för sin egen verksamhet. Det är ofta flerställiga koder², blanketter med engångskoder och fysiska tillbehör. Metoderna har nått stor spridning, men gemensamt för de flesta av dessa är att de av säkerhetstekniska skäl endast kan användas hos den tjänsteleverantör som tillhandahållit lösningen. Därmed tvingas konsumenten till att ha lika många sådana lösningar som tjänsteleverantörer.

Det finns även generella ID-lösningar där en och samma lösning med fördel kan användas hos många tjänsteleverantörer. Den mest spridda generella lösningen är en e-legitimation, som bygger på asymmetrisk kryptering och brukar kallas certifikat. Det innebär att mottagaren kan verifiera signaturens äkthet, men inte rekonstruera den. Mycket talar för att marknaden för metoder för säker elektronisk identifiering under överskådlig tid kommer att domineras av denna metod.

² Så kallade PIN-koder

Det idag vanligaste, när det gäller generella ID-lösningar är att den som vill kunna identifiera sig laddar ner en fil som innehåller ett certifikat till sin dator, som sedan kan användas för att generera en unik signatur. Man talar i dessa fall om mjuka certifikat. Utvecklingen går sannolikt mot en ökad användning av sk hårda certifikat som är lagrade på ett smart kort och mot certifikat som kan användas vid uppkopplingar med mobiltelefon.

Det är lättare och billigare att distribuera ett mjukt certifikat än ett hårt, och dessa ställer inga krav på att datorn ska ha en kortläsare. Samtidigt är säkerheten hos ett mjukt certifikat beroende av att innehavaren har en fungerande brandvägg i sin dator. För den som tar emot en signatur spelar det däremot ingen roll när det gäller själva verifieringen om certifikatet är mjukt eller hårt.

2.4 Hur skaffar sig medborgaren e-legitimation?

Det finns flera sätt för medborgare att få tillgång till e-legitimationer. För den som är Internetbankskund i någon av bankerna kan e-legitimation införskaffas via Internetbanken. Bankerna har redan grundidentifierat sina kunder med olika säkerhetslösningar t ex säkerhetsdosor, engångskoder och egna certifikatlösningar. Kunden kan genom att logga in på sin Internetbank teckna avtal med sin bank om e-legitimation.

För den som inte är Internetbankskund finns det idag möjligheter att skaffa e-legitimation hos Nordea, TeliaSonera samt Steria.

2.5 Hur kan en e-legitimation användas?

En e-legitimation kan användas för att identifiera sig gentemot myndigheter, kommuner, landsting, företag och organisationer via Internet. En e-legitimation kan också användas för att ersätta traditionella underskrifter i den mån det är möjligt enligt gällande lagstiftning. Mottagaren kontrollerar att e-legitimationen är giltig samt att den inte har spärrats.

Genom att använda en e-legitimation i kommunikationen mellan två parter går det att:

- Säkerställa vem som skickat ett meddelande.
- Skydda informationen från insyn.
- Kontrollera att informationen inte förändrats under kommunikationen.
- I efterhand bevisa att ett meddelande skapats, skickats och tagits emot.

E-legitimation innebär att myndigheterna kan erbjuda e-tjänster där flera eller till och med alla steg i kommunikationen sker elektroniskt.

I dagsläget är användningen av mjuka certifikat begränsad även om det sker en kontinuerlig ökning. Orsakerna till den begränsade användningen är framförallt att det finns få tjänster.

2.6 Utvecklingsbehov för ökad spridning av e-legitimation i den kommunala sektorn

E-legitimation erbjuder en säker gemensam lösning för e-tjänster inom den offentliga sektorn. Medborgare och företag kan med e-legitimationen på ett smidigt

sätt utföra tjänster över nätet. Inom den offentliga sektorn är det i huvudsak den statliga sektorn som använder e-legitimation för sina tjänster. Hinder för att e-legitimation inte används inom den kommunala sektorn är enligt företrädare för kommunsektorn;

- kommunerna behöver utveckla ett för alla sina verksamhetssystem gemensamt behörighetsregister för att kunna införa e-legitimation utan dyrbara investeringar i vart och ett av de olika verksamhetssystemen,
- att kommunerna inte kan bära kostnaderna för att verifiera e-legitimationernas giltighet så som prispbildningen nu ser ut enligt Statskontorets upphandling.

2.7 Delegationens bedömning av e-legitimation

Det finns en mängd tjänster såväl inom staten som inom den kommunala sektorn som kostnadseffektivt kan tillhandahållas elektroniskt. Många av dessa tjänster är emellertid av den arten att de ställer krav på att den medborgare eller det företag som behöver tjänsten kan identifieras på ett säkert sätt.

På den svenska marknaden finns flera olika utgivare av e-legitimationer. En gemensam grund för alla dessa är att de utgår från sk PKI. En annan gemensam nämnare för svenska e-legitimationer är att de alla bygger på något som kan benämnas som en avtalsmodell. I ett antal europeiska länder har e-legitimationer utfärdats till medborgare genom statliga initiativ. Resultatet av dessa initiativ har varit omdiskuterade eftersom det bland annat medför stora kost-

nader för staten att agera certifikatutfärdare, distribuera legitimationer samt tillhandahålla spärllistor mm. Den svenska modellen innebär att staten, myndigheter, kommuner och så vidare betalar för tjänsten verifieringen (kontrollen om en e-legitimation är giltig eller inte). Kostnaden för att ta fram e-legitimationer bärs däremot av marknadsaktörerna.

Införandet av e-legitimation på den svenska marknaden utgår från:

- att starta med en enkel lösning som är både tekniskt och ekonomiskt realiserbar,
- att senare, när det blir tekniskt och ekonomiskt möjligt, lösningar som är starkare ur säkerhetssynpunkt och som också är funktionellt mera utvecklade (främst förbättrad mobilitet).

De e-legitimationer som idag är mest spridda är de ”mjuka” lösningarna. De:

- fungerar tämligen enkelt för användarna
- kan på ett standardiserat sätt integreras på olika aktörers hemsidor,
- är tillräckligt säkra för många tjänster,
- kan spridas snabbt så snart det finns flera e-tjänster,
- kan användas inte bara gentemot myndigheter utan också på den privata marknaden.

Delegationen kan konstatera att det utvecklingsarbete bl a vissa banker och stora statliga myndigheter bedrivit har skapat en grund för en säker teknisk lösning. Statskontoret har vidare tecknat ramavtal som gör det möjligt för både statliga myndigheter, det stora flertalet kommuner och landsting att avropa tjänster som ger den nödvändiga säkerheten vad avser identifiering och signering. Därmed finns också goda förutsättningar för myndigheter, kommuner och landsting att utveckla sådana e-tjänster som kräver säker identifiering.

Inom ramen för Statskontorets senaste ramavtal lades också grunden för prismodeller som är bättre anpassade till små myndigheters och kommuners situation. I syfte att ytterligare utveckla dessa prismodeller har en grupp myndigheter, kommuner och landsting inlett samtal med de privata leverantörer med vilka Statskontoret har tecknat avtal. Det vore enligt delegationens bedömning av stort värde inte minst för kommunerna att dessa samtal leder till ett konstruktivt resultat.

Många olika parter har således bidragit till att den svenska offentliga sektorn har tillgång till en säker elektronisk identifiering på ett sätt som står sig väl i jämförelse med andra länder.

3. Delegationens planerade insatser

Den statliga sektorn har kommit relativt långt i utvecklingen av e-tjänster. Inom de kommunala och landstingskommunala områdena går det betydligt långsammare. För att stimulera utvecklingen planerar delegationen på kort sikt å ena sidan en informationsinsats å andra sidan en belysning av olika finansieringsmodeller och lönsamhetskalkyler för utveckling av e-tjänster. Delegationen avser också att inbjuda till ett antal hearings kring frågor som finns avseende utveckling och användning av e-tjänster.

3.1 Informationsinsats om e-samhället och e-tjänster

Delegationen har för avsikt att under 2005 genomföra en informationsinsats riktade till aktörerna inom den offentliga sektorn kring e-samhället och e-tjänster. Avsikten är primärt att belysa hur verksamheten kan utvecklas, förändras och effektiviseras med elektroniska tjänster samt att ge goda exempel på e-tjäs-

ter samt samverka för att erbjuda dessa. Informationsinsatsen kommer även att innefatta e-tjänster som är av särskild betydelse för personer och företag och som har bidragit till effektiviseringar. Insatserna för informationsinsatsen skulle kunna följa följande uppläggning. Se vidare projektplan i bilagan.

3.2 Finansieringsmodeller för utveckling av e-tjänster

Ett återkommande påtalat hinder för utvecklingen av e-tjänster är bristen på resurser, svårigheten att upprätta lönsamhetskalkyler samt prissättningsmodeller. Delegationen avser att i kommande rapport belysa dessa områden. Arbeten pågår såväl inom Ekonomistyrningsverket som inom Statskontoret i dessa frågor. Hur offentlig sektor och privat näringsliv kan samverka i utvecklingen av e-tjänster är i det sammanhanget av stort intresse.

Bilaga 1. Informationsinsats om e-samhället och e-tjänster

Projektplan:

Syftet är:

- att genom kommunikation stödja de krafter inom den offentliga sektorn som driver verksamhetsutvecklingen med e-tjänster, och öka intresse och efterfrågan hos medborgare och företag.

Målen är:

- att visa på den potential som finns för elektroniska tjänster såväl i form av nytta för medborgare och företag som möjligheter till effektivisering av den offentliga verksamheten,
- att öka kännedomen om elektroniska tjänster inom den offentliga sektorn,
- att bjuda in fler aktörer att bidra och därmed ge ett bättre underlag för delegationens arbete,
- att öka publiciteten kring delegationens arbete, elektroniska tjänster och de insatser som görs av stat, kommun och landsting för att utveckla elektroniska tjänster.

Målgrupper:

Ledningarna för statliga myndigheter och verk, kommuner och landsting.

Andra viktiga interna opinionsbildare inom offentlig sektor – t ex IT-chefer och informationschefer.

Medborgare och företag. Här kan också finnas delgrupper, som t ex äldre och funktionshindrade.

Journalister, politiker och andra viktiga opinionsbildare.

Övergripande planering

För kommunikationsinsatserna inriktas insatserna utifrån följande övergripande planering:

2004

Framtagande av planer och material.

Kontakt med intressenter.

Planering och förankring inom delegationen.

2005

Insatser riktade till offentliga sektorns aktörer.

Insatser riktade till medborgare och företag.

Eventuellt en större kampanj tillsammans med Utbildningsradion och folkrörelser.

Uppföljande insatser



**24-timmarsdelegationen, www.24SJU.se
Vasagatan 8-10, 103 33 Stockholm, tfn 08-405 10 00
Christina Kvarnström, huvudsekreterare**

