Stockholms universitet

Rektor

BESLUT
2021-06-24 Dnr SU FV-1449-21

Rikard Skårfors
FD, Utbildningsledare
Rektors kansli, Ledningssekretariatet

Regeringskansliet (Infrastrukturdepartementet)

Yttrande över betänkandet Vem kan man lita på? Enkel och ändamålsenlig användning av betrodda tjänster i den offentliga förvaltningen (SOU 2021:9)

Stockholms universitet har av Regeringskansliet (Infrastrukturdepartementet) anmodats att inkomma med synpunkter på Utredningens om betrodda tjänster delbetänkande *Vem kan man lita på? Enkel och ändamålsenlig användning av betrodda tjänster i den offentliga förvaltningen* (SOU 2021:9). Universitetet har följande att anföra.

Generella synpunkter

Stockholms universitet anser att betänkandet överlag är välskrivet och att det förs relevanta diskussioner kring både utmaningar med betrodda tjänster i offentlig förvaltning och olika vägar att hantera dessa utmaningar. Sannolikheten för att behoven av betrodda tjänster fortsatt kommer att öka är hög, och det är därför viktigt att frågan bevakas med avseende på såväl regleringen kring dessa tjänster som på olika lösningar som leder till en enkel och ändamålsenlig, men också rättssäker och demokratisk, användning av tjänsterna.

Stockholms universitet tillstyrker i stort förslagen men önskar utveckla några aspekter till utredningens fortsatta arbete, vilka redovisas i det följande.

Förvaltningspolitiska aspekter

Utredningen föreslår (kapitel 8) att ett mer samlat ansvar för betrodda tjänster ska åläggas Myndigheten för digital förvaltning (DIGG). DIGG föreslås tillhandahålla en nationell förvaltningsgemensam valideringstjänst, och även utreda behovet av ett valideringsverktyg för att bevara undertecknade och stämplade handlingars giltighet. Utredningen föreslår också att DIGG ges en stärkt roll som förvaltningspolitisk kunskaps- och stödmyndighet i frågor om betrodda tjänster med uppgift att främja användningen av sådana tjänster. DIGG ska också, i samarbete med Post- och telestyrelsen (PTS), vara den myndighet som bevakar och ser till att Sverige tar en mer aktiv roll i det internationella standardiseringsarbete som omgärdar denna typ av tjänster.

Stockholms universitet

Stockholms universitet håller med om att det behövs ett mer samlat och utvecklat stöd för förvaltningen att tillgå för frågor kopplade till betrodda tjänster. Frågor om kunskapsinsamling, lärande, utveckling och stöd löses inte av sig själv utan måste organiseras fram. Inte minst är det viktigt att Sverige, utifrån kunskaper och vunna erfarenheter, stärker sin position i det internationella standardiseringsarbetet.

Givet hur förvaltningspolititiken är organiserad i dag faller det sig naturligt att förlägga det förvaltningspolitiska arbetet för frågan om betrodda tjänster till DIGG. Universitetet har inga invändningar i sak mot utredningens organisatoriska och ansvarsfördelningsmässiga förslag men vill framhålla det mer övergripande problemet med att isolera enskilda förvaltningspolitiska frågor på det sätt som utredningen nu vill göra genom att lägga ansvaret för betrodda tjänster på DIGG.

Förvaltningspolitik handlar om idéer och åtgärder som riktas mot hela (eller stora delar av) förvaltningen och som rör dess organisation, personal och arbetssätt. Det är således en ”politik på tvären” som rör alla myndigheter inom alla politikområden. Därför kännetecknas också förvaltningspolitiken av stor målkomplexitet där olika grundläggande värden ska värnas samtidigt, inte bara demokrati, rättssäkerhet och effektivitet, utan också professionalitet och brukarinflytande. På så sätt utgör förvaltningspolitiken en kärnpunkt i regeringens politik. I dag saknas det dock en myndighet med ett övergripande och samlat ansvar för det förvaltningspolitiska förnyelse- och metodutvecklingsarbetet. I stället finns det ett antal mindre och smalare förvaltningspolitiska kunskaps- och utvecklingsmyndigheter med ansvar för vissa avskilda frågor, till exempel för ekonomistyrning (Ekonomistyrningsverket), för upphandling (Upphandlingsmyndigheten), för arbetsgivarfrågor (Arbetsgivarverket), för ekonomiadministration (Statens servicecenter), för jämställdhet (Jämställdhetsmyndigheten) och för digitalisering (DIGG).

Forskning visar att det finns en påtaglig risk att frågor som på detta vis avgränsas och ges en egen organisation (en förvaltningsmyndighet) drivs på ett sätt som gör att det uppstår suboptimering och fragmentering. Dessa små förvaltningspolitiska myndigheter kan förvisso ha betydande kunskaper om sin egen (avgränsade) fråga, men kan ha svårt att se hur deras fråga relaterar till andra förvaltningspolitiska frågor och värden. Egna mål och resultatkrav, grundade i visst värde, riskerar att bli det allt annat överskuggande, medan önskvärda synergieffekter riskerar att utebli, särskilt som dessa myndigheter också sorterar under olika departement. Regeringen har under senare år, liksom flera offentliga utredningar, pekat på behovet av att tänka brett, varierat och samlat kring förvaltningens organisation och styrning. Men ett sådant tänkande är i dag inte inorganiserat i staten. För vissa centrala förvaltningspolitiska frågor är organiseringen mycket svag eller till och med obefintlig, vilket exempelvis gäller frågorna om stat/kommunrelationen, kompetensförsörjning, organisering, samordning, medialisering och reglering.

Stockholms universitet vill här lyfta fram vikten av att regeringen ser över förvaltningspolitikens organisering och utreder möjligheten att inrätta en större

Stockholms universitet

förvaltningspolitisk kunskapsmyndighet med ett samlat ansvar för utvecklings- och förnyelsefrågorna, där frågor om styrning (inte bara ekonomistyrning), personal, reglering (inkl. internationellt standardiseringsarbete), digitalisering, organisering, stat/kommun-relationen m.m. samorganiseras. Det skulle skapa förutsättningar för öppna och balanserade diskussioner – diskussioner som utgår från samtliga förvaltningspolitiska värden – och som kan generera ett mer långsiktigt och hållbart förvaltningspolitiskt utvecklingsarbete.

Juridiska aspekter

Rubrikerna i det följande motsvarar avsnitten i delbetänkandets kapitel 8, Utredningens förslag.

8.2 När bör den offentliga förvaltningen använda avancerade eller kvalificerade elektroniska underskrifter?

Utredningen anser att bedömningen av när avancerade eller kvalificerade underskrifter ska användas bör ligga på de enskilda myndigheterna. Stockholms universitet avstyrker delvis detta, utifrån följande.

Förtroendet för den offentliga förvaltningen är av yttersta betydelse för att upprätthålla en demokratisk rättsstat och en god samhällsekonomi. Sverige brukar inte sällan lyftas fram som ett land där förtroendet för myndigheterna är särskilt högt. För att upprätthålla detta förtroende i ett samhälle som blir alltmer digitaliserat, där enskilda använder e-tjänster som tillhandahålls av förvaltningen i allt större utsträckning, är det i ett större perspektiv centralt att den offentliga förvaltningen iakttar högsta möjliga informationssäkerhet. IT-skandaler eller andra sådana säkerhetsproblem, som på ett eller annat sätt orsakas inom en myndighet, leder ofta till tapp eller låg rankning i förtroendemätningar.

En så hög informations- och cybersäkerhet som möjligt handlar emellertid långt ifrån endast om att rankas högt i undersökningar om myndigheternas anseende. Det handlar om hur väl den offentliga förvaltningen värnar enskildas personliga integritet och skydd för personuppgifter såväl som skyddet för Sveriges yttre och inre säkerhet. Därtill har Sverige som medlemsstat i EU ett ansvar enligt t.ex. eIDAS-förordningen, att främja den inre marknaden och bidra till en säker handel, både över gränserna och inom landet. I detta avseende är det väsentligt att den offentliga förvaltningen håller en så hög standard som möjligt även beträffande begagnandet av betrodda tjänster, såsom elektroniska underskrifter och stämplar.

Det är viktigt att närmare reflektera över skillnaden mellan avancerade och kvalificerade underskrifter. Det kan, såsom utredningen påpekar, vara en förenklad slutsats att hävda att kvalificerade underskrifter alltid är säkrare än avancerade (s. 143). I praktiken kan en tillhandahållare av en avancerad underskrift ha en lika god nivå av säkerhet som en tillhandahållare av en kvalificerad sådan.

Stockholms universitet

Icke desto mindre har tillhandahållaren av den avancerade underskriften inte underkastat sig samma krav, samma nivå av tillsyn och ekonomiska risk, som den som tillhandahåller en kvalificerad underskrift, vilket talar för att det typiskt sett finns väsentligt större anledning att lita på den sistnämnda.

Därutöver är det endast kvalificerade elektroniska underskrifter som anses vara att jämställa med en handskriven underskrift enligt art. 25.2 i eIDAS-förordningen. Den internationella utblick som utredningen presenterar visar också att det fungerar väl att använda kvalificerade underskrifter inom den offentliga förvaltningen i andra länder (ss. 143ff.). Det framgår också av de siffror som presenteras i denna del, att det synes förekomma ett större utbud av kvalificerade underskrifter i länder där det finns krav på att använda sådana, t.ex. Norge och Italien (s. 144).

Även om det är önskvärt med en så hög säkerhet som möjligt, vilket talar för användningen av kvalificerade elektroniska underskrifter, måste detta även vägas mot de kostnader som det innebär. Denna aspekt lyfts inte särskilt fram av utredningen i kartläggningen, utan i denna diskuteras frågor som osäkerhet kring regelverket, teknisk kunskapsbrist och bevarandeproblematik.

Det finns därför anledning att gå in närmare på denna problematik även utifrån ekonomiska utgångspunkter. En fråga är om kartläggningen hade fått ett annat utfall om de offentliga aktörer som ingått i kartläggningen hade haft de ekonomiska förutsättningarna att lägga de kostnader som krävs för att införa en kvalificerad elektronisk underskrift. I det läget hade den aktuella aktören i trygg förvissning kunnat konsultera Post- och telestyrelsens (PTS) förteckning, där tillhandahållare av sådana tjänster finns uppsatta, vilka genomgått en särskild ansökningsprocess. Vidare skulle aktören kunna vara tämligen säker på att de krav som ställs i eIDAS skulle vara uppnådda. Det finns därför anledning att anta att valet mellan en avancerad och en kvalificerad underskrift i stor utsträckning är en kostnadsfråga och möjligen även det avgörande skälet till att den offentliga förvaltningen hellre använder avancerade underskrifter. En betydelsefull parameter i denna del, är att det inte heller finns några uttryckliga rättsliga krav på att använda kvalificerade signaturer. Finns det inga rättsliga krav, finns det heller inga tydliga incitament till att bekosta en högre säkerhetsnivå, även om det skulle vara att föredra.

Utifrån kartläggningen kommer utredningen fram till att avancerade respektive kvalificerade underskrifter bör användas när det är påkallat utifrån författningskrav, verksamhetens behov och i informationssäkerhetshänseende. Det anses inte heller lämpligt att på en generell nivå slå fast när avancerade eller kvalificerade elektroniska underskrifter bör användas (s. 149). Frågan är emellertid om det i alla avseenden är lämpligt att lämna till enskilda myndigheter att avgöra sådana frågor, som kan ha en större räckvidd än myndighetens egen verksamhet. Är det t.ex. rimligt att använda en avancerad underskrift när enskilda ska lämna underskrift under straffansvar, såsom vid inlämnande av självdeklaration? Det kan även finnas andra situationer där underskriften har en mycket stor betydelse för den enskilde eller för en annan myndighet.

Stockholms universitet

Det kan handla om myndighetsutövning mot enskild, såsom ett beslut om nekad aktivitetsersättning eller för att säkerställa äktheten på t.ex. ett examensbevis.

Det kan också finnas viktiga säkerhetsintressen som den enskilda myndigheten av olika skäl kanske inte kan avgöra helt på egen hand, som rör rikets yttre eller inre säkerhet. I de situationer som här har beskrivits är bedömningen inte enbart en fråga om verksamhetens behov, rättsliga förutsättningar och krav som finns på informationssäkerhet inom denna, utan handlar även om andra, både enskilda och allmänna intressen.

Med tanke på de effektiviseringskrav som den offentliga förvaltningen verkar under, finns det risk för att mer kortsiktiga ekonomiska ställningstaganden får en oproportionerligt stor tyngd vid sådana bedömningar som görs inom ramen för den egna verksamheten. Det är förhållandevis lätt att räkna på en skada eller incident som har skett, men desto svårare att göra det med utgångspunkt i potentiella risker och oönskade konsekvenser.

Ett särskilt prövningsförfarande skulle därför kunna införas när t.ex. en myndighet vill införa en elektronisk underskrift i någon form, så att även utomstående bedömare kan avgöra vilken säkerhetsnivå som är rimlig.

Det skulle därför vara önskvärt med ytterligare utredning om möjligheterna att reglera vissa kriterier på hög nivå, i lag, som tydliggör i vilka situationer som kvalificerade respektive avancerade underskrifter bör användas. Detta framstår som tidigare nämnts, som rimligt att i fall där underskriften på något sätt är av stor betydelse för ett enskilt eller allmänt intresse. En sådan utveckling skulle vidare stärka rättssäkerheten väsentligt i den digitala offentliga förvaltningen, bidra till bättre ansvarsutkrävande och sänka risken för manipulation. I dessa situationer framstår det också som motiverat att bära de ökade kostnader som begagnandet av en kvalificerad elektronisk underskrift medför.

En utökad användning av kvalificerade underskrifter skulle förutom att det skulle bidra till att tillgodose vissa angelägna enskilda och allmänna intressen, troligen ge upphov till flera nya aktörer på marknaden för betrodda tjänster som är beredda att ta den ekonomiska risken, vilket i sin tur skulle kunna bidra till en stärkt produktutveckling och lägre priser på sikt.

8.3 En utökad tillitsförteckning

Utredningen föreslår en utökad tillitsförteckning, som inkluderar icke kvalificerade tillhandahållare av betrodda tjänster. Stockholms universitet tillstyrker förslaget och förordar att detta sker i kombination med en kvalitetsmärkning.

Med hänsyn till den utbredda användningen av avancerade elektroniska underskrifter inom den offentliga förvaltningen framstår denna åtgärd som både rimlig och angelägen. Det förefaller också som troligt att denna kan bidra till ett ökat införande av avancerande elektroniska signaturer inom den offentliga förvaltningen.

Det framstår som positivt att PTS, som har den kompetens som krävs på området, kvarstår som ansvarig för att tillhandahålla tillitsförteckningen. Detta skulle emellertid kunna kombineras med någon form av samrådsfunktion bestående av andra myndigheter vilket t.ex. gäller inom försäljning av säkerhetskänslig verksamhet. Vad beträffar säkerhetsfrågor är det emellertid en styrka att kunna använda den offentliga förvaltningens samlade expertis på området i så stor utsträckning som möjligt. Likväl skulle en samrådsfunktion på området betrodda tjänster inte nödvändigtvis behöva vara behäftad med samma rigorösa krav som vid säkerhetskänslig verksamhet.

PTS bör för att kunna genomföra sitt åtagande på området ges föreskriftsrätt. Det är inte lämpligt att belasta lagtexten med detaljer avseende uppställda kriterier och tekniska krav. Detta görs lämpligen på myndighetsnivå, även om det finns anledning att följa upp detta i framtiden.

Utredningen föreslår att en mer omfattande tillsyn för icke kvalificerade tillhandahållare införs. Universitetet tillstyrker detta, inte minst då meningen med en utökad tillitsförteckning kan gå om intet om det inte finns några möjligheter till utökad kontroll. Det finns inte heller något som talar emot att icke kvalificerad tillhandahållare som inte fortsatt når upp till kraven får avföras från tillitsförteckningen eftersom ett sådant beslut kan överklagas till domstol.

Sammantaget kan förslaget om utökad tillitsförteckning tillsammans med en mer omfattande tillsyn för icke kvalificerade tillhandahållare, antas innebära att säkerheten höjs även beträffande avancerade elektroniska underskrifter, även om kraven av förklarliga skäl är lägre än för kvalificerade tillhandahållare. Benämningen tillitsförteckning framstår som tydlig och adekvat.

8.4 En nationell valideringstjänst

Stockholms universitet tillstyrker delvis förslagen, men menar att myndigheter i vissa fall bör vara skyldiga att använda sådana underskrifter och stämplar som kan valideras av den föreslagna valideringstjänsten, t.ex. när handlingar upprättas som ett led i myndighetsutövning.

Utredningen lämnar ett förslag om en ny nationell valideringstjänst som är en både väl avvägd och internationellt beprövad åtgärd (ss. 165ff.). En nationell valideringstjänst framstår som en viktig beståndsdel i navet i den digitala förvaltningen. En författningsreglering av tjänsten ter sig därför nödvändig för att uppnå en effektiv styrning och säkerhet. Det är därutöver positivt för den inre marknadens funktion, då det finns en central tjänst att vända sig till, som är anpassad till de svenska och europeiska tillitsförteckningarna. Det finns också flexibilitet för att i viss utsträckning kunna validera underskrifter och stämplar från tredje land.

Stockholms universitet

Förslaget om föreskriftsrätt för DIGG tillstyrks av universitetet, då lagstiftningen inte bör belastas med detaljer om funktioner och gränssnitt. Vidare förutsätts att olika format måste kunna valideras liksom underskrifter och stämplar från utlandet.

Det föreslås att det ska vara frivilligt att använda sig elektroniska underskrifter som går att validera i den nationella valideringstjänsten (s. 169). Det är möjligt att frivillighet är både lämpligt och nödvändigt i ett övergångsskede. Inom vissa tidsramar bör ambitionen dock vara att myndigheter ska vara skyldiga att använda sådana underskrifter och stämplar som kan valideras i tjänsten som är hänförliga till vissa delar av den offentliga verksamheten, såsom när det är fråga om myndighetsutövning eller det finns särskilda behov av att kunna säkerställa en viss underskrifts äkthet. Detta kan vara av central betydelse för tilliten och rättssäkerhet i förvaltningen. Detta borde inte heller utgöra ett problem i förhållande till den kommunala självstyrelsen, om fråga är om t.ex. myndighetsutövning inom den kommunala förvaltningen.

I den mån det finns sektorspecifika valideringstjänster, såsom SUNET:s valideringstjänst för universitet och högskolor, som följer DIGG:s tekniska ramverk, bör det säkerställas att de kan bibehållas och utvecklas.

Det centrala är att det ska vara tydligt för myndigheterna vad som krävs och att det innebär tillräckliga incitament till att den nationella valideringstjänsten eller motsvarande tjänster kommer till användning på ett effektivt och förtroendestärkande sätt, vilket ofta bäst säkerställs genom lagstiftning.

Några invändningar mot att utöka kretsen som får använda tjänsten till privata aktörer som utför offentliga tjänster, såsom vård- och utbildningsföretag, synes inte föreligga. Det ligger, som utredningen påpekar, väl i linje med de åtaganden som föreligger enligt lagen om tillgänglighet till digital förvaltning.

Att externa parter, såsom enskilda personer och företag samt andra myndigheter kan validera offentliga dokument via tjänsten är mycket positivt för såväl rättssäkerhet och transparens som förtroendet för den offentliga förvaltningen i stort.

En avgiftsbeläggning av den nationella valideringstjänsten framstår som skälig.

Personuppgiftsansvar kan aktualiseras inom den nationella valideringstjänsten. Utredningen föreslår därför att ett stöd för nödvändig behandling av den nationella valideringstjänsten ska föreskrivas i lag. Detta förslag tillstyrks av Stockholms universitet.

Bedömningen rörande offentlighet- och sekretess framstår som rimlig och det kan därutöver säkerställas att uppgifter som omfattas av sekretess genom användning av en lokalt installerad version av valideringstjänsten.

Stockholms universitet

8.5 Bevarande

Stockholms universitet tillstyrker förslagen, men vill samtidigt framhålla behovet av omvärldsbevakning och strategier rörande den inverkan som utvecklingen av kvantdatorteknik kan föra med sig.

En viktig fråga vad beträffar elektroniskt underskrivna eller stämplade allmänna handlingar är hur och i vilken omfattning de ska bevaras, vilket kan vara en utmaning.

Frågan om vilken strategi för långtidsvalidering som ska väljas, bedömer utredningen på goda grunder vara en fråga för fortsatt utredning av Riksarkivet och DIGG (s. 188). En möjlig väg som diskuteras är användning av s.k. valideringsintyg som metod, vilket t.ex. används i SUNET:s valideringstjänst. Att iaktta försiktighet i valet av metod för bevarande med tanke på den komplexitet som det kan vara förenat med i den föreslagna nationella valideringstjänsten framstår som väl motiverat och en ytterligare utredning i detta avseende förordas.

Utredningen anser vidare att Riksarkivet ska få i uppdrag att utreda förutsättningarna för att införa generella bestämmelser och/eller annat stöd rörande bevarande av elektroniskt undertecknade eller stämplade handlingar. Det finns flera oklarheter i lagstiftningen i nuläget, vilket gäller t.ex. möjligheterna till gallring och informationsvärdering mot bakgrund av det omfattande informationsflöde som för närvarande råder.

Värdet av att bibehålla en elektronisk underskrift kan variera beroende på vilken handling som den är en del av. För detta behövs klargöranden på föreskriftsnivå. Det kan inte heller anses tillfredsställande att det används flera olika definitioner avseende begreppet gallring i olika delar av den offentliga förvaltningen om det inte är särskilt motiverat.

När det gäller elektroniskt underskrivna handlingar som ska inhämtas från andra aktörer för att säkerställa möjligheterna till kontroll är det inte heller klarlagt vilka rättsliga förutsättningar som föreligger.

Utredningen nämner den hotbild rörande elektroniska handlingar som föreligger mot bakgrund av utvecklingen inom kvantdatorteknik, som innebär att den kryptering som ligger till grund för underskriften kan kompromitteras (s. 187). Detta diskuteras dock inte närmare i genomgången av risker (s. 221). I denna del framstår det som väsentligt att etablera tydliga krav på omvärldsbevakning och strategier för hur en sådan teknisk utveckling ska hanteras då det kan innebära en risk för påtagligt ökad sårbarhet. Det är inte klart i vilken utsträckning kvantdatortekniken kan användas på detta sätt och det går inte heller att förutse när ett genombrott i denna tekniska utveckling kommer att ske, även om en tioårsperiod brukar anges som ett riktmärke.

Stockholms universitet

8.6 Ett utökat och reformerat stöd till den offentliga förvaltningen avseende betrodda tjänster

Stockholms universitet tillstyrker förslagen, men erinrar om den principiella diskussionen under *Förvaltningspolitiska aspekter* ovan.

Någon form av samverkansgrupp likt Samverkansgruppen för informationssäkerhet (SAMFI) skulle kunna vara lämplig även avseende betrodda tjänster, då det är angeläget att använda den expertis som finns inom den offentliga förvaltningen som helhet.

8.8 Ökad medverkan i standardiseringsarbete

Stockholms universitet tillstyrker förslaget.

Det får anses vara av mycket stor betydelse att svenska myndigheter aktivt deltar i det standardiseringsarbete som sker i Europa, inte bara för att öka möjligheterna att påverka utvecklingen utan också för kunskapsinhämtning, erfarenhetsutbyte m.m. Det är bra att detta samordnas bättre, men det kan också vara relevant att närmare utreda vad det är för hinder som anses föreligga, då regeringens strategi för standardisering har funnits sedan 2018 utan att något aktivt deltagande i någon större omfattning kommit till stånd.

8.9 Utformning av författningsbestämmelser rörande underskrifter

Stockholms universitet instämmer delvis i utredningens bedömning.

Utredningen diskuterar olika alternativ för utformning av författningsbestämmelser med utgångspunkt i olika utredningar som tidigare företagits, från IT-utredningen 1994 till Digitaliseringsrättsutredningen 2018 (ss. 208ff.). Sverige har trots detta inte kommit lika långt i arbetet med att införa elektroniska underskrifter som i t.ex. Danmark. Utredningen nämner också ett system med elektronisk bevittning av underskrifter som införts i Storbritannien, vilket hade varit intressant att få mer information om. Utgör detta en modell för Sverige?

Det kan vara lämpligt att som utredningen föreslår, bestämmelser utformas med teknikneutralitet som utgångspunkt samt att detaljreglering bör ske på så låg nivå som möjligt. Endast i de fall då det anses nödvändigt bör säkerhetsnivån anges (ss. 214ff.). Frågan är emellertid om detta är en tillräckligt tydlig reglering för att myndigheter och enskilda ska kunna uppfatta vad som krävs.

I utredningens kartläggning har bland annat framkommit att osäkra regler om användning av elektroniska underskrifter är tillåten eller ej, upplevs som mer problematiska än regler som uttryckligen förhindrar användningen av elektroniska underskrifter (s. 216).

Säkerhetsnivån hos en elektronisk underskrift är emellertid vid läsning av eIDAS-förordningen central och endast kvalificerade elektroniska underskrifter jämställs med

Stockholms universitet

handskrivna. Som nämndes tidigare är allmänhetens förtroende också i stor utsträckning avhängigt av god säkerhet. Att på samma sätt som i eIDAS-förordningen använda en väl inarbetad terminologi som avancerade och kvalificerade underskrifter i nationell lagstiftning framstår i det perspektivet som ändamålsenligt.

Ett alternativ skulle kunna vara att i en generell bestämmelse ange vilken säkerhetsnivå som bör gälla för elektroniska underskrifter generellt, t.ex. en avancerad underskrift, om inget annat sägs. Detta kräver emellertid att lagstiftaren på olika områden tar ställning till i vilka sammanhang som en hög säkerhet, dvs. en kvalificerad underskrift krävs. Detta skulle troligen underlätta möjliggörandet av elektroniska underskrifter beträffande områden där stränga formkrav gäller såsom vid testamente eller fastighetsköp. Det är också viktigt att ta ställning till hur elektronisk bevittning kan ske, då det alltjämt torde finnas behov av detta i olika situationer.

Utredningen diskuterar vidare i vilken utsträckning krav på underskrifter verkligen behövs (s. 220). Detta kan vara lämpligt, men det är också viktigt att poängtera underskrifters betydelse som bevis, för ansvarsutkrävande, förtroende osv. Det som i nuläget framstår som mer angeläget är att införa de åtgärder som krävs, för att införa möjlighet till elektroniska underskrifter på bred front, men som samtidigt upprätthåller en god nivå av säkerhet. Se vidare *Säkerhetsaspekter* nedan.

Säkerhetsaspekter

Utredningen tar upp många säkerhetsaspekter vilket i sig är nödvändigt. Dessa tjänster kommer att vara säkerhetskritiska, och det under lång tid. Underskrifter, stämplar osv. måste ha sin giltighet under många decennier, och det ställs därför höga säkerhetskrav.

Trots det hade Stockholms universitet gärna sett ett större fokus på vissa säkerhetsaspekter som erfarenhetsmässigt är problematiska. Den amerikanska myndigheten National Institute of Standards and Technology (NIST) har tagit fram ett cybersäkerhetsramverk som listar fem funktioner som behövs för att hantera riskerna för cybersäkerhetsangrepp.

- Identifiera – Identifikation av hot, möjliga angrepp osv. samt även vilka tillgångar, människor, data, förmågor osv. som är skyddsvärda.
- Skydda – Införa olika mekanismer för att skydda tillgångar från angrepp eller annan påverkan så att kritiska tjänster fortsatt kan levereras.
- Upptäcka – Utveckla metoder, mekanismer, och processer för att uppnå möjligheten att *kontinuerligt* upptäcka angrepp eller andra brott mot säkerhetsmekanismerna.
- Svara – Utveckla metoder, mekanismer, processer och organisation för att kunna ta tillvara upptäckta problem i det förra steget och att svara på rätt sätt när de uppkommer.

Stockholms universitet

- Återhämta – Utveckla metoder, mekanismer, processer, planer, och organisation för att snabbt och säkert kunna återställa tjänsten samt minska skadeverkningar och övrig påverkan på det omgivande systemet och samhället.

Avsnitt 9.5 berör vissa av punkterna ovan, men inte alla. Exempelvis nämns inte förmågan till upptäckt. Det kan i sammanhanget nämnas att det är så man valt att lösa problemet som aktualiserades i och med DigiNotar-angreppet som beskrivs i 9.3.1. Det generella problemet med *Public Key Infrastructure* (PKI) för digitala certifikat för webbtjänster är att den inte är ett äkta träd, utan istället vad man ibland i datalogiska sammanhang kallar en ”skog”. Det finns inte en rot i det träd som utgörs av PKI, alltså ett toppcertifikat som certifierar samtliga underliggande tjänsteleverantörer som varande pålitliga. Istället finns flera möjliga certifikat på olika nivåer.

Problemet som DigiNotar-angreppet satte ljuset på är att de kunde ställa ut ett certifikat för Google.com (och liknande domäner) som webbläsare tar för trovärdigt, trots att Google inte efterfrågat något certifikat från DigiNotar, tecknat något avtal med dem om att ställa ut ett certifikat, eller över huvud taget velat använda sig av DigiNotars tjänster. Idag löses det här problemet genom att det blivit tekniskt möjligt för användare av certifikattjänster att se om något certifikat ställts ut för användarens räkning, och då kontrollera om detta är i enlighet med användarens egna önskemål. Denna lösning faller alltså under *upptäcka* ovan. Men den möjliggör bara upptäckt om man har en organisation på plats som kontinuerligt övervakar att inga falska certifikat ställts ut, och som vidtar lämpliga åtgärder om det sker.

Vidare pekade den stora driftstörningen hos en tjänsteleverantör i november 2011, som påverkade Apoteket AB, Bilprovningen, SBAB m.fl., på ett problem som lätt kan drabba förmågan att svara på och återhämta sig efter en händelse. Myndigheten för samhällsskydd och beredskap (MSB) hade svårt att få tillgång till detaljerad och uttömmande information från leverantören om precis vad som hänt, eftersom leverantören hävdade företagssekretess. Att få tillgång till korrekt och detaljerad information i det akuta skedet är naturligtvis A och O för att säkerställa ett snabbt, proportionerligt och verkningsfullt svar. Det är tillika viktigt för återhämtningsfasen att ännu mer detaljerad information om händelseförlopp, brister osv. är tillgänglig för att bl.a. tillförsäkra sig om att man kan förhindra ett återupprepande.

I ovanstående fall fick inte denna incident några katastrofala återverkningar på tjänsteleverantören, men som bl. a. DigiNotar-fallet visar är ett angrepp av den här typen ofta förödande för företaget som drabbas. Dessa företags vilja att frivilligt dela med sig av den här typen av information torde därför vara ytterst begränsad. Användare av dylika tjänster bör därför ta höjd för att tillförsäkra sig om att korrekt och detaljerad information görs tillgänglig utan onödig fördröjning. Som MSB:s rapport från incidenten ovan visar är det generellt svårt för myndigheter att skriva på den typ av tystnadsförsäkringar (*non-disclosure agreement*) som är vanliga i det privata näringslivet. Detta försvårar ytterligare samarbetet mellan användaren och tjänsteleverantören och är något man måste vara medveten om i sammanhanget.

Stockholms universitet

Sammanfattningsvis ser Stockholms universitet gärna att större vikt läggs vid de tre senare uppräknade funktionerna i NIST-ramverket, alltså *upptäcka*, *svara* samt *återhämta* för att försäkra sig om att systemet som helhet skall fungera tillfredsställande.

Detta beslut är fattat av rektor, professor Astrid Söderbergh Widding, i närvaro av prorektor Clas Hättestrand och tillförordnad universitetsdirektör Åsa Borin. Studeranderepresentanter har informerats och haft tillfälle att yttra sig. Övrig närvarande har varit Rikard Skårfors, Ledningssekretariatet (protokollförare). Föredragande i ärendet har varit utbildningsledare Rikard Skårfors.