ELEKTRONISKT UNDERSKRIVNA HANDLINGAR

RIKSARKIVET

ELEKTRONISKT UNDERSKRIVNA HANDLINGAR

RIKSARKIVET

RAPPORT 2006:1

Riksarkivets rapportserie
riktar sig i första hand till statliga myndigheter men kan även användas av andra myndigheter och organ som har att tillämpa arkivlagen.

Elektroniskt underskrivna handlingar

Upplaga 1:1

ISBN 91-38-32325-7 ISSN 1402-9685
ISBN 978-91-38-32325-0

Publikationsansvarig: Per Jansson, arkivråd.
Grafisk form: Nils Möllerström AB, Stockholm.
Original: Nora Liljeholm.
Förlagor till illustrationer: Jonas Öholm, Skatteverket.
Tryck: Elanders Gotab AB, Vällingby 2006.

Skriften beställs från:
Fritzes Kundservice, 106 47 Stockholm,
telefon: 08 - 690 91 90, orderfax: 08 - 690 91 91,
internet: www.fritzes.se, e-post: order.fritzes@nj.se

FÖRORD

I denna rapport behandlas frågor som är av betydelse för bevarande och gallring av elektroniskt underskrivna handlingar och vissa andra handlingar som kommer in till eller upprättas inom ramen för myndigheternas elektroniska tjänster (e-tjänster). Det sker med utgångspunkt från såväl författningsregleringen som beskrivningar av vad som utgör en elektroniskt underskriven handling, dess beståndsdelar och funktioner.

Under arbetet med rapporten har bl.a. följande frågor analyserats.

- Vad är en elektroniskt underskriven handling? Vilka är handlingens beståndsdelar – funktionellt och tekniskt? Vilka handlingar kommer in till eller upprättas hos mottagande myndighet vid den kontroll som sker där?

- Vilka krav kan ställas när det gäller formatet på de handlingar som ges in via en e-tjänst? Vad regleras genom arkivförfattningarna?

- Hur bör en mottagande myndighet hantera de elektroniskt underskrivna handlingarna, och övriga handlingar som kommer in till och upprättas hos myndigheten? Vilka krav bör ställas på kontroll, stämpling, och andra skyddsåtgärder?

- Vilka förutsättningar finns för gallring av handlingar som har kommit in till eller upprättats hos en myndighet inom ramen för en e-tjänst?

Rapporten har tagits fram i samverkan med SAMSET-projektets juristgrupp som är ett forum för samverkan mellan myndigheter som har kommit långt i arbetet med att införa e-tjänster och som har ställts inför dessa frågor.

I SAMSET:s juristgrupp ingår:
verksjuristen Johan Bålman (ordförande), Skatteverket,
stabsjuristen Jaan Entson, Försäkringskassan,
avdelningsdirektören Gustaf Johnssén, Riksarkivet (tidigare Statskontoret)
verksjuristen Anna Sjöstrand, Centrala studiestödsnämnden,
förvaltningsjuristen Helene Ålund, Bolagsverket,
säkerhetsarkitekten Jonas Öholm, Skatteverket, och
1:e arkivarien Britt-Marie Östholm, Riksarkivet.

I arbetet har även deltagit:
projektledaren för SAMSET Dag Osterman, Skatteverket, avdelningsdirektören Torbjörn Hörnfeldt, Riksarkivet, och advokaten Per Furberg, Setterwalls.

Frågorna har även diskuterats i ett större forum där arkivansvariga från bl.a. Skatteverket, Försäkringskassan, Bolagsverket och Centrala studiestödsnämnden har deltagit.

Arbetet inom SAMSET:s juristgrupp avslutades i juni 2005. Rapporten har därefter bearbetats av Britt-Marie Östholm, Torbjörn Hörnfeldt, Jonas Öholm och Per Furberg.

Tomas Lidman, riksarkivarie

INNEHÅLL

1 SAMMANFATTNING

När en myndighet inför en e-tjänst är den första åtgärden att kartlägga vilka handlingar som förväntas komma in och upprättas inom ramen för tjänsten. Elektroniskt underskrivna handlingar som kommit in till myndigheten utgör *allmänna handlingar* enligt 2 kap. tryckfrihetsförordningen. Detsamma gäller för handlingar som kommer in till eller upprättas hos myndigheten när de elektroniskt underskrivna handlingarna kontrolleras.

Myndigheterna är skyldiga att bevara allmänna handlingar i *ursprungligt skick*. Alla åtgärder som innebär förstöring av allmänna handlingar, uppgifter i allmänna handlingar eller annan informationsförlust utgör gallring, och får inte vidtas utan stöd i gallringsföreskrifter. Handlingar som får gallras, skall kunna presenteras i ursprungligt skick under den tid som de bevaras. Om myndigheternas rutiner för att framställa, kontrollera och bevara handlingar får en olämplig utformning finns det risk för att det ursprungliga skicket går förlorat eller att handlingarna inte kan läsas.

Elektroniskt underskrivna handlingar behöver redan från början *framställas* i ett format som gör att de kan läsas även på lång sikt. Om det blir nödvändigt med konvertering för att handlingarna skall kunna bevaras i läsbart skick förlorar underskriften till största delen sin funktion. När det gäller handlingar som framställs inom ramen för en e-tjänst styr myndigheterna själva vilka format som skall användas. Ett bevarande av såväl innehåll som underskrift kan alltså säkerställas.

När en handling har kommit in till en myndighet *kontrolleras* att den är oförvanskad och att den härrör från den som framstår som utställare. Kontroll och dokumentation av utfallet bör ske så snart handlingen har kommit in till myndigheten. För den fortsatta hanteringen är det av betydelse hur och när kontroll har skett, och hur utfallet har dokumenterats.

Den inkomna handlingen bör *stämplas* med myndighetens elektroniska stämpel direkt efter den initiala kontrollen. Stämpeln dokumenterar att kontroll har skett. Stämpeln kan även användas för kontroll av att handlingen inte har förvanskats efter att den första kontrollen gjordes. En sådan kontrollmöjlighet blir av särskild betydelse om det ursprungliga kontrollmaterialet inte finns kvar.

För att handlingarna skall kunna *bevaras och skyddas* på lång sikt behövs en kombination av åtgärder, bl.a. skyddad förvaring, beständiga databärare och identiska exemplar med åtskild förvaring.

Om de elektroniskt underskrivna handlingarna framställs i lämpligt format, kontroll sker direkt vid ankomsten till myndigheten, utfallet av kontrollen dokumenteras och handlingen förses med myndighetens stämpel, skapas förutsättningar för *gallring* av handlingar som har kommit in eller upprättats enbart för kontrolländamål. Några generella regler om gallring av kontrollmaterial kan emellertid inte beslutas i dagsläget, då en bedömning av vad som skall bevaras respektive gallras bör utgå från en kartläggning av samtliga handlingar med anknytning till e-tjänsten. Användningen av e-underskrifter är under utveckling och det är inte möjligt att förutsäga vilka handlingar som kommer att bli aktuella i olika typer av e-tjänster.

Sammanfattningsvis förordas att varje myndighet redan när en e-tjänst planeras

- kartlägger vilka handlingar som förväntas komma in till myndigheten och upprättas inom ramen för e-tjänsten,

- skapar förutsättningar för att framställa handlingar i ett format som gör det möjligt att bevara dem utan konvertering,

- utarbetar rutiner för att
  - förlägga kontrollen till den tidpunkt då handlingarna kommer in till myndigheten,
  - dokumentera utfallet av kontrollen,
  - stämpla handlingarna med myndighetens stämpel, och
  - bevara handlingarna i ursprungligt skick och skydda dem mot förvanskning under den tid som de skall bevaras.

2 FÖRFATTNINGSREGLERINGEN

2.1 OFFENTLIGHETSPRINCIPEN

Offentlighetsprincipen kan beskrivas som en grundsats enligt vilken samhällsorganens verksamhet skall bedrivas under allmän insyn och kontroll. Denna princip, som syftar till att främja ett fritt meningsutbyte och en allsidig upplysning, har flera beståndsdelar. En av dem är handlingsoffentligheten, dvs. rätten att ta del av allmänna handlingar. Regler om handlingsoffentlighet finns i 2 kap. TF.

Handlingsoffentligheten garanterar allmänhetens rätt till insyn i såväl myndigheternas ärenden – *ärendeinsyn* – som deras verksamhet i stort – *verksamhetsinsyn*. Genom tillgången till allmänna handlingar kan allmänheten och massmedia få en allsidig, fullödig och objektiv information om de offentliga organens verksamhet. Därmed skapas möjligheter för en fri och konstruktiv debatt i skilda samhällsfrågor. Under senare årtionden har handlingsoffentligheten dessutom kommit att tjäna ett syfte som informationsförmedlare i vidare mening. Hos myndigheterna finns en riklig tillgång på uppgifter både om förhållanden inom den offentliga verksamheten och på det privata området. Genom handlingsoffentligheten kan forskare, företag m.fl. få fram uppgifter som kan användas för den egna verksamheten. Förutom att vara uppbyggd av de två grundstenarna ärendeinsyn och verksamhetsinsyn kan handlingsoffentligheten därmed sägas ha inslag av *kunskapsinsyn.*[1]

Rätten att ta del av allmänna handlingar förutsätter att de bevaras och ordnas så att det går att hitta bland dem, och vårdas så att de inte skingras eller förstörs. Därför skall det, i enlighet med 2 kap. 18 § TF, finnas grundläggande bestämmelser i lag om hur allmänna handlingar skall bevaras samt om gallring och annat avhändande av sådana handlingar. Bestämmelsen utgör grunden för en arkivreglering, och syftar till att betona arkivreglernas betydelse som handlingsoffentlighetens stödsystem. Bestämmelser om att allmänna handlingar skall bevaras och på vilket sätt detta skall ske finns i arkivlagen (1990:782), arkivförordningen (1991:446) och Riksarkivets föreskrifter.

1 SOU 1997:39 s. 492, SOU 2001:3 s. 51 f.

2.2 ALLMÄN HANDLING

Reglerna i 2 kap. TF om handlingsoffentlighet bygger på vissa grundbegrepp, bl.a. begreppet handling som har definierats i 2 kap. TF på ett sätt som delvis avviker från allmänt språkbruk. Dessa regler och begrepp är tillämpliga även på arkivområdet. För arkivförfattningarna är det därför avgörande vad som föreskrivs i 2 kap. TF, inte vad som anges i exempelvis förvaltningslagen eller rättegångsbalken om när en handling är inkommen eller när ett mål eller ett ärende anses vara anhängiggjort.

2.2.1 Vad är en allmän handling

Med *handling* förstås framställning i skrift eller bild samt upptagning som kan läsas, avlyssnas eller på annat sätt uppfattas endast med tekniskt hjälpmedel. För bedömningen av vad som utgör en handling saknar det betydelse vilka materiel och metoder som har använts när handlingen framställdes. En handling kan således vara en handskrift eller en ritning på papper eller pergament, ett fotografi, en audio- eller videoupptagning eller en elektronisk handling.

En handling är *allmän* om den förvaras hos en myndighet och är att anse som inkommen till eller upprättad hos myndigheten. Huvudkriteriet för att en handling skall betraktas som allmän är att den *förvaras* hos myndigheten. Det betyder inte att handlingen rent fysiskt måste befinna sig i myndighetens lokaler. Avgörande är om myndigheten faktiskt förfogar över möjligheten att lämna ut handlingen.

En upptagning för automatiserad behandling betraktas som förvarad hos myndigheten, om upptagningen är *tillgänglig* för myndigheten med tekniskt hjälpmedel som myndigheten själv utnyttjar för överföring i sådan form att den kan läsas, avlyssnas eller på annat sätt uppfattas. En sammanställning av uppgifter ur en upptagning för automatiserad behandling anses dock vara förvarad hos myndigheten endast om myndigheten kan göra sammanställningen tillgänglig med rutinbetonade åtgärder. Bestämmelserna om upptagningar för automatiserad behandling har nyligen ändrats i syfte att åstadkomma en anpassning till dagens IT-användning.

Som *inkommen* betraktas en handling när den har anlänt till myndigheten eller kommit en behörig befattningshavare till handa. I fråga om de nämnda upptagningarna gäller i stället att en upptagning anses ha kommit in till en myndighet när annan har gjort den tillgänglig på det sätt som krävs för att en upptagning skall anses vara förvarad hos myndigheten.

En handling anses *upprättad* när den har expedierats eller – om den inte expedieras – när det ärende till vilket den hänför sig har slutbehandlats hos myndigheten eller – om handlingen inte hänför sig till visst ärende – när den har justerats av myndigheten eller på annat sätt färdigställts.

2.2.2 En anpassning till dagens användning av IT

Uttalanden i lagmotiv och doktrin rörande upptagningar har tidigare i allt väsentligt tagit sikte på *potentiella handlingar,* dvs. möjliga sammanställningar i IT-miljö av uppgifter som anses finnas hos en myndighet även om myndigheten aldrig har haft eller kommer att ha anledning att göra sammanställningen i sin egen verksamhet. En förutsättning för att en sådan sammanställning skall utgöra allmän handling är att den kan göras tillgänglig med rutinbetonade åtgärder. Begreppet potentiell handling utgår från synsättet att varje sakligt sammanhängande konstellation av uppgifter som kan produceras utifrån tillgängliga uppgiftssamlingar kan utgöra en handling. Att varje ”atomär” uppgift och kombination av sådana kan utgöra en handling framstår ofta som främmande för vanliga användare, men så är det enligt bestämmelserna i 2 kap. TF. De senaste ändringarna har inte inneburit några inskränkningar i rätten att ta del av potentiella handlingar.

En fokusering på *potentiella* handlingar är mindre lämplig i dagens IT-miljö, där myndigheternas handlingsbestånd i allt högre utsträckning kommit att omfatta elektroniska ersättare för traditionella pappershandlingar. Typiska exempel är e-brev, promemorior, protokoll och beslut i elektronisk form. Den ändring som har gjorts i 2 kap. TF syftar till att klargöra att myndigheternas datalagrade information även omfattar så kallade *färdiga handlingar.* Man har därvid utgått från handlingsoffentlighetens grundsyfte, nämligen att tillhandahålla ett informationsinnehåll i en viss form, oavsett vilket medium som är bärare av informationsinnehållet.[2] För färdiga handlingar gäller att de skall kunna göras tillgängliga med tekniskt hjälpmedel som myndigheten själv förfogar över för överföring i sådan form att de kan läsas, avlyssnas eller på annat sätt uppfattas. Detta gäller oavsett om det endast krävs rutinbetonade åtgärder för att ta fram handlingarna i uppfattbar form eller ett mera omfattande arbete.[3]

Gränsen mellan färdiga och potentiella handlingar är inte helt klar. Det har inte heller ansetts lämpligt att i grundlagstext förtydliga var gränsen går. Ledning får istället hämtas i detaljerade arkivregler om hur allmänna handlingar i elektronisk form skall bevaras.[4] Från bevarandesynpunkt kan man i grova drag skilja mellan

- *färdiga handlingar* av dokumenttyp, t.ex. en elektroniskt underskriven handling, eller en skannad handling,

2 SOU 2001:3 s.116.

3 Se vidare prop. 2001/02:70 s. 20 f.

4 SOU 2001:3 s.139 f och prop. 2001/02:70 s. 22.

- *färdiga handlingar* som utgörs av förberedda sammanställningar i ett system, t.ex. en ”skärmbild” som används regelmässigt i verksamheten, och
- *handlingar som inte är färdiga*, dvs. sammanställningar som myndigheten saknar anledning att göra i sin dagliga verksamhet men som kan göras, t.ex. med hjälp av en rapportgenerator, ett frågespråk eller särskilt programmeringsarbete.

Genom de nyligen gjorda ändringarna i 2 kap. TF betonas för myndigheterna vikten av att avgränsa vad som skall utgöra färdiga handlingar och att ge IT-systemen sådana funktioner att det är möjligt att presentera handlingarna upprepat över tiden.

Som en följd av ändringarna i 2 kap. TF har Riksarkivets föreskrifter om upptagningar för automatiserad behandling förtydligats i syfte att säkerställa en upprepad presentation av färdiga handlingar (dokument och sammanställningar) i myndigheternas IT-system.[5]

Myndigheternas datalagrade information omfattar dels *färdiga handlingar*, dels *potentiella handlingar*.[6] Det är färdiga och underskrivna elektroniska handlingar av dokumenttyp som behandlas i denna rapport.

2.3 BEVARANDE I URSPRUNGLIGT SKICK

Rätten till insyn enligt 2 kap. TF förutsätter att handlingarna bevaras i *ursprungligt skick*, dvs. med det innehåll de hade i det ögonblick då de kom in till myndigheten eller upprättades där. I annat fall finns endast förvanskningar av de ursprungliga handlingarna att ta del av.[7]

För att det skall vara möjligt att upprepa *sammanställningar* som myndigheten har kunnat göra i ett IT-system krävs att digitala data bevaras tillsammans med bl.a. dokumentation över de databasstrukturer och sammanställningsmöjligheter som funnits hos myndigheten. För *färdiga handlingar av dokumenttyp* gäller därutöver att handlingarna skall kunna presenteras i samma form som när de kom in till eller upprättades hos myndigheten. Även möjligheter som funnits att bedöma om handlingarna är oförvanskade och äkta behöver bevaras. Handlingarna skall också skyd-

5 RA-FS 2003:2.

6 SOU 2001:3 s. 135 och prop. 2001/02:70 s. 21.

7 Se prop. 2001/02:70 s. 35.

das från skada, förstörelse, tillgrepp och obehörig åtkomst. De skall även, i enlighet med arkivförfattningarna och 15 kap. sekretesslagen, beskrivas och registreras så att deras sammanhang med andra handlingar och verksamheten framgår.

När konventionella pappersrutiner i allt högre grad ersätts med elektronisk ärendehantering, e-tjänster och e-post får bestämmelserna i arkivförfattningarna om hur handlingar skall framställas, förvaras och skyddas stor betydelse.[8]

Behovet av att bevara handlingar i ursprungligt skick, måste beaktas redan när elektroniska system och e-tjänster planeras. Hela processen för att hantera allmänna handlingar behöver säkerställas.

2.4 ARKIVLAGEN

En myndighets arkiv bildas av myndighetens allmänna handlingar. Handlingarna i ett ärende skall arkiveras när ärendet har slutbehandlats hos myndigheten. I samband därmed skall myndigheten pröva i vilken omfattning minnesanteckningar, utkast och koncept, skall tas om hand för arkivering. När det gäller diarier, journaler och förteckningar som förs fortlöpande anses varje anteckning vara arkiverad i och med att den har gjorts.[9]

Arkivet skall bevaras och vårdas så att det kan tillgodose rätten att ta del av allmänna handlingar, behovet av information för rättskipningen och förvaltningen, och forskningens behov.[10] Regler om arkivvård finns i 4 – 6 §§ arkivlagen. Av 4 § framgår att varje myndighet svarar för vården av sitt arkiv om inte en arkivmyndighet har övertagit detta ansvar. I 5 § finns bestämmelser som rör åtgärder som skall vidtas som grund för arkivvården. Vid registrering av allmänna handlingar skall myndigheten ta vederbörlig hänsyn till registreringens betydelse för en ändamålsenlig arkivvård, och vid framställningen av handlingar använda materiel och metoder som är lämpliga med hänsyn till behovet av arkivbeständighet.[11] I 6 § arkivlagen finns vidare bestämmelser om att arkivet bl.a. skall avgränsas och organiseras, beskrivas och förtecknas samt skyddas mot förstörelse, skada, tillgrepp och obehörig åtkomst.

8 Se vidare prop. 2001/02:70 s. 35 f.

9 Se 3 § arkivförordningen. Regleringen omfattar även upptagningar för automatiserad behandling som förs fortlöpande.

10 Se 3 § arkivlagen.

11 Med arkivbeständighet menas enligt lagmotiven att handlingarna skall framställas på ett sådant sätt att de kan läsas, avlyssnas eller på annat sätt uppfattas under den tid som de skall bevaras (prop. 1989/90:72 s. 72).

2.5 RIKSARKIVETS FÖRESKRIFTER

Riksarkivet utfärdar verkställighetsföreskrifter med stöd av arkivförordningen (1991:446) och får föreskriva om bl.a. vad som krävs av materiel och metoder med hänsyn till behovet av beständighet, användningen av skrivmateriel och förvaringsmedel, avgränsning och organisation av arkivet, arkivredovisning, skydd av arkivet, och gallring.

För frågan om bevarande och gallring av elektroniskt underskrivna handlingar blir i första hand bestämmelserna om framställning, förvaring och skydd av betydelse. Avgörande är också den definition av gallring som finns i Riksarkivets föreskrifter. Även frågor som rör avgränsning och organisation kan komma att aktualiseras när det gäller hantering och lagring av elektroniskt underskrivna handlingar.

De föreskrifter som Riksarkivet har utfärdat är skrivna i tre nivåer. Den högsta nivån är medieoberoende, vilket betyder att författningarna är tillämpliga på alla slags allmänna handlingar, oberoende av hur de framställs och lagras.[12] På mellannivå finns mediespecifika författningar som anger vad som gäller för handlingar på olika medier med avseende på framställning, hantering, förvaring, skydd och vård. På den lägsta nivån finns tekniska krav och hänvisningar till standarder.

2.5.1 Framställning av handlingar

Materiel och metoder, m.m.

Enligt Riksarkivets föreskrifter skall en myndighets handlingar framställas så att de kan bevaras över tiden. Det innebär att de skall kunna läsas, avlyssnas eller på annat sätt uppfattas under hela bevarandetiden. I pappersmiljö innebär det att myndigheten skall välja papper, skrivare, faxar, kopiatorer m.m. som uppfyller de tekniska kraven i Riksarkivets föreskrifter. Framställs handlingarna i enlighet med dessa krav underlättas den fortsatta hanteringen samtidigt som det skapas goda förutsättningar för ett långsiktigt bevarande.

Vad som avses med beständighet och bevarande är inte lika självklart när det gäller upptagningar för automatiserad behandling. Upptagningarna kan inte läsas i den form som de lagras på databäraren. Ett meningsfullt innehåll skapas först när den fysiska representationen avkodas och tolkas i flera led och presenteras med hjälp av datorutrustning och program. Det är bara om det går att upprepa presentationen över tiden som man kan tala om ett bevarande i arkivförfattningarnas mening. För bevarande krävs att myndigheten har valt att lagra och representera data på ett sätt som med-

12 Se vidare RA-FS 1991:1 ändrad genom RA-FS 1997:4.

ger överföring till nya databärare, att det finns en teknisk miljö som möjliggör presentationen och att det finns dokumentation över lagrade data, rutiner i systemet m.m. Databärarnas beständighet har således inte samma betydelse som i traditionell miljö.

När det gäller upptagningar för automatiserad behandling har Riksarkivet utfärdat föreskrifter som omfattar krav vid systemutveckling, systemförvaltning, dokumentation och val av format m.m.[13] Av bestämmelserna framgår att myndigheten redan vid utveckling av ett system eller en applikation bör välja format i överensstämmelse med Riksarkivets tekniska krav. Skulle det bli nödvändigt att konvertera upptagningarna från ett format till ett annat skall myndigheten beskriva konsekvenserna av konverteringen, och ange vilka metoder som krävs för presentation av upptagningarna. En konvertering som medför informationsförlust innebär alltid gallring; se avsnitt 2.5.2.

Som tidigare påpekats har traditionella pappershandlingar i allt högre grad kommit att ersättas av elektroniska motsvarigheter, t.ex. e-brev, promemorior, protokoll och beslut i elektronisk form. Arbete pågår för närvarande med en översyn av Riksarkivets föreskrifter. Bestämmelserna anpassas till dagens IT-användning, med format för handlingar av dokumenttyp och elektroniska underskrifter m.m.

En tillämpning för inkomna handlingar

Riksarkivets föreskrifter avser i första hand handlingar som myndigheten själv upprättar, men de skall tillämpas även på inkommande handlingar i den mån myndigheten kan styra framställningen. Så är fallet beträffande t.ex. handlingar som överförs via telefax och skrivs ut på papper för bevarande i denna form. Liknande möjligheter att styra framställningen föreligger inom ramen för en myndighets e-tjänster; se avsnitt 5.2.

Det är av särskild betydelse för handlingar som skrivs under elektroniskt att välja ett lämpligt format från början. Ett olämpligt ursprungligt val för med sig att mottagande myndighet kan tvingas till en konvertering av handlingen som medför att underskriften till största delen förlorar sin funktion.

13 Se vidare Riksarkivets föreskrifter och allmänna råd (RA-FS 1994:2, ändrad genom RA-FS 2003:2) om upptagningar för automatiserad behandling, Riksarkivets föreskrifter och allmänna råd (RA-FS 1994:7, ändrad genom RA-FS 2003:3) om överlämnande av upptagningar för automatiserad behandling (ADB-upptagningar) till Riksarkivet och landsarkiven, samt Riksarkivets föreskrifter och allmänna råd (RA-FS 2003:1) om tekniska krav för ADB-upptagningar. Ett förslag till ändrade föreskrifter om tekniska krav för ADB-upptagningar beräknas träda ikraft under 2007.

2.5.2 Handlingarnas skydd

En myndighets handlingar skall, i enlighet med 6 § arkivlagen, skyddas mot förstörelse, skada, tillgrepp och obehörig åtkomst. Traditionellt handlar det om fysiska skydd såsom placering i aktomslag, arkivboxar, arkivlokaler och annan skyddad förvaring. I den elektroniska miljön räcker det emellertid inte med ett fysiskt skydd, t.ex. att servrar och bandrobotar finns i låsta och klimatreglerade utrymmen. Det krävs även brandväggar, behörighetssystem m.m. för att skydda handlingarna mot förvanskning, förstöring och obehörig åtkomst. En annan säkerhetsåtgärd är att framställa mer än ett exemplar av handlingar. När det gäller upptagningar för automatiserad behandling ställs krav på regelbunden säkerhetskopiering. Kopiorna skall omfatta samtliga uppgifter som utgör allmänna handlingar, även uppgifter som krävs för att sammanställa och förstå allmänna handlingar. Kravet på att bevara mer än ett exemplar gäller även efter det att upptagningarna har överförts för långtidslagring.[14]

2.5.3 Gallring

Föreskrifter om gallring

Huvudregeln är att myndigheter skall bevara sina allmänna handlingar. Enligt 10 § arkivlagen får gallring emellertid ske om de handlingar som återstår efter gallringen kan tillgodose de bevarandemål som nämns i 3 § arkivlagen.

Gallring får inte ske oreglerat. För statliga myndigheter följer av 14 § arkivförordningen att gallring får ske endast med stöd av föreskrifter eller beslut av Riksarkivet, om inte särskilda föreskrifter om gallring har meddelats i lag eller förordning; se nedan om gallring av personuppgifter.

Riksarkivet utfärdar dels gallringsbestämmelser som är generella och som avser handlingar som förekommer hos de flesta statliga myndigheter, dels myndighetsspecifika bestämmelser om gallring som skall tillämpas av en myndighet eller en grupp av myndigheter. Riksarkivet har utfärdat bl.a. generella gallringsföreskrifter för handlingar av tillfällig eller ringa betydelse. Dessa föreskrifter medger att en handling får gallras efter överföring till annan databärare om de förluster som uppkommer är ringa. Det kan gälla för t.ex. vissa e-postmeddelanden som skrivs ut på papper. De generella gallringsbestämmelserna kungörs i Riksarkivets författningssamling (RA-FS) och de myndighetsspecifika i en särskild publikationsserie (RA-MS).

14 4 kap 3 § RA-FS 2003:2.

Personuppgiftslagen (1998:204; PUL) har till syfte att skydda människor mot att deras personliga integritet kränks genom behandling av personuppgifter. PUL hindrar inte att en myndighet arkiverar och bevarar allmänna handlingar eller att arkivmaterial tas om hand av en arkivmyndighet. Finns det bestämmelser om gallring i annan lag eller förordning (s.k. registerförfattningar) så gäller dessa.[15]

Från det att en handling blivit allmän gäller att gallring får ske endast om åtgärden är tillåten enligt särskilda gallringsföreskrifter i lag eller förordning eller i enlighet med föreskrifter eller beslut av Riksarkivet.[16]

Vad är gallring

Med gallring avses i arkivförfattningarna att förstöra allmänna handlingar eller uppgifter i allmänna handlingar, eller att vidta andra åtgärder med de allmänna handlingarna som medför

- förlust av betydelsebärande data,
- förlust av möjliga sammanställningar,
- förlust av sökmöjligheter, eller
- förlust av möjligheter att bedöma handlingarnas autenticitet.

Alla åtgärder som medför informationsförlust utgör följaktligen gallring. Handlingens ursprungliga skick har därmed gått förlorat. Exempel på sådana åtgärder är överföring av handlingar till ett annat medium, t.ex. utskrift på papper från ett system för automatiserad behandling eller skanning av pappershandlingar. Även byte av format inom samma medietyp utgör gallring om åtgärden medför en irreversibel informationsförlust. Som gallring räknas också åtgärder som innebär att betydelsebärande element i en elektroniskt underskriven handling tas bort. Enligt arkivförfattningarna krävs det särskilda gallringsföreskrifter för att få förstöra de ursprungliga handlingarna efter åtgärder som medför informationsförlust.

15 Som exempel på gallringsbestämmelser i en registerförfattning kan nämnas 28 § lagen (2003:763) om behandling av personuppgifter inom socialförsäkringens administration. Där föreskrivs att personuppgifter som behandlas automatiserat skall gallras när de inte längre är nödvändiga för de avsedda ändamålen, dock att regeringen eller den myndighet regeringen bestämmer får meddela föreskrifter om bevarande för vetenskapliga ändamål. Riksarkivet har i flera fall föreskrivit om undantag från gallring i enlighet med bestämmelser i sådana registerförfattningar.

16 Se 10 § arkivlagen och 14 § arkivförordningen. Vad som sägs här avser i första hand statliga myndigheter.

Gallringsbara handlingar skall bevaras i ursprungligt skick under hela bevarandetiden, dvs. till dess att gallringsfristen har löpt ut.

Vilka bedömningar görs

När frågor om bevarande och gallring utreds inleds arbetet med en avgränsning av vad som utgör *handlingar* i det aktuella materialet, och därefter vilka handlingar som är *allmänna*, enligt bestämmelserna i 2 kap. TF.

Nästa steg är att kontrollera om det finns handlingar som är *gallringsbara* i enlighet med redan gällande författningar, dvs. i enlighet med

- Riksarkivets generella gallringsföreskrifter, rörande t.ex. räkenskapshandlingar och personalhandlingar,
- Riksarkivets myndighetsspecifika föreskrifter om gallring och annan arkivhantering, eller
- registerförfattningar.

Om gallringsföreskrifter saknas följer en värdering av de aktuella handlingarna med utgångspunkt från arkivlagens bevarandemål. De handlingar som bevaras skall tillgodose allmänhetens rätt till insyn, behovet av information för rättskipningen och förvaltningen samt forskningens behov; se avsnitt 2.4. Behovet av information för *rättskipning* och *förvaltning* avser handlingarnas betydelse som underlag för den dömande verksamheten, för att styrka rättigheter och skyldigheter, samt för att tillgodose rättssäkerhet, effektivitet och intern kontroll inom förvaltningen. Behovet av handlingarna för *offentlighetsinsyn* och *forskning* är svårare att förutse. I båda fallen avses möjligheter att använda handlingarna utan förutbestämda syften och utan begränsningar i tiden.

En myndighets handlingar härrör från dess verksamhet. Genom att bevara handlingarna i sitt sammanhang, skapas förutsättningar för insyn i myndighetens verksamhet, dvs. i hur myndigheten har arbetat och på vilket underlag som beslut har fattats. Vid prövning av frågor om bevarande och gallring måste en helhetsbedömning göras, där hänsyn inte bara tas till de aktuella handlingarna och deras *innehåll* utan även till deras *funktion* och *samband* med andra handlingar i handläggningsprocessen. Oftast görs därför bedömningar om bevarande och gallring i myndighetsspecifika gallringsföreskrifter.

> Vid en bedömning av bevarande och gallring av handlingarna inom en e-tjänst behöver samtliga handlingar med anknytning till e-tjänsten tas med i bedömningen, dvs. samtliga handlingar i den handläggningsprocess som e-tjänsten stödjer.

3 ELEKTRONISKA HANDLINGAR OCH INFRASTRUKTURER

3.1 VAD ÄR EN ELEKTRONISKT UNDERSKRIVEN HANDLING

För bedömning av vilka handlingar som bör bevaras respektive gallras, behövs en beskrivning av de handlingar som kommer in till myndigheten eller upprättas där inom ramen för en e-tjänst.[17]

Följande frågor behöver besvaras. Vad är en elektroniskt underskriven handling? Vilka är handlingens beståndsdelar, funktionellt och tekniskt? Vilka övriga handlingar kommer in och upprättas i anknytning till e-tjänster som stöds av ID-tjänster och hur används dessa? Vad är en myndighetsstämpel?

3.2 EN FÖRENKLAD BESKRIVNING

3.2.1 Text och underskrift

En elektroniskt underskriven handling består av flera delar. Data som representerar *texten* utgör endast en del av den färdiga handlingen.[18] När texten skrivs under elektroniskt kompletteras den med en *kontrollsumma* som krypteras med undertecknarens *privata nyckel* och knyts till texten. I funktionellt hänseende kan den krypterade kontrollsumman sägas utgöra e-underskriften genom att den knyter texten till en bestämd utställare.

Möjligheterna att kontrollera äktheten hos en elektroniskt underskriven handling är oberoende av databäraren. De är istället inbyggda i den elektroniska handlingen och i den infrastruktur som stödjer ID-tjänsten. Den elektroniska underskriften skiljer sig även från en traditionell underskrift genom att den inte presenteras för mottagaren i läsbar form. Den kan dock uppfattas indirekt när datorn presenterar resultatet av äkthetskontrollen. Vid en presentation visas även uppgifter ur undertecknarens e-legitimation.[19]

17 I denna rapport används uttrycken elektroniskt underskriven handling och elektronisk underskrift som en anpassning till e-nämndens vägledningar. I Riksarkivets föreskrifter används istället elektroniskt signerad handling och elektronisk signatur.

18 Med ”text” avses i denna rapport all slags information som kan förses med elektronisk underskrift, exempelvis även bilder.

19 I vissa programvaror finns funktioner för att presentera namnunderskriften i form av en bildfil tillsammans med uppgifter ur e-legitimationen.

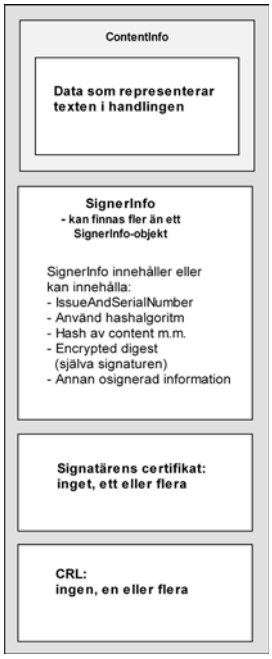
3.2.2 Format för underskrift

I de e-tjänster som myndigheterna tillhandahåller idag används något av följande två format:

- PKCS#7, Cryptographic Message Syntax Standard, eller
- XML-Signature, XML-Signature Syntax and Processing.

Vilket format som används beror på vilken ID-tjänst som utnyttjas. Formaten bygger på samma underliggande tekniker, bl.a. PKCS#1, RSA Encryption Standard.

Figur 1.



Förenklat kan en handling med elektronisk underskrift i formatet PKCS#7 beskrivas som ett paket innehållande ett eller flera mindre paket, som i sin tur kan innehålla ytterligare paket osv. Se figur 1. Det första av de inre paketen (ContentInfo) innehåller data som representerar texten i handlingen. I det andra (SignerInfo) finns bl.a. uppgifter om den metod som använts för att skapa kontrollsumman (hashalgoritmen), kontrollsumman (hashvärdet) och den krypterade kontrollsumma, dvs. underskriften. Det tredje paketet (Certificate eller signatärens certifikat) innehåller uppgifter ur den legitimation som stödjer underskriften, och i det fjärde (CRL eller CertificateRevocationList) kan finnas ingen, en eller flera spärrlistor.

Den elektroniskt underskrivna handlingen består således av en helhet som är definierad till innehåll och struktur. Alla delar behövs för att mottagaren skall kunna ta del av texten och kontrollera att uppgiften om utställare är riktig och att texten inte har förvanskats efter det att handlingen undertecknades.

De beskrivna delarna utgör tillsammans en handling, i enlighet med 2 kap. 3 § TF. Den del av handlingen som utgör underskriften kan visserligen inte presenteras i läsbar form men den kan uppfattas.

3.3 EN DETALJERAD BESKRIVNING

Som underlag för överväganden om bevarande och gallring behövs en mer detaljerad beskrivning av en elektroniskt underskriven handling och dess beståndsdelar. I detta avsnitt följer vi handlingen från utställarens framställning av text och underskrift till myndighetens äkthetskontroll och

dokumentation av utfallet. Här skisseras även hur en myndighetsstämpel kan utformas. Beskrivningen gör inte anspråk på att vara heltäckande.[20]

I beskrivningen används för ändamålet lämpliga format: PKCS#7-attached för den elektroniska underskriften och XML-Signature för myndighetens stämpel.

3.3.1 Handlingen före underskrift

Inom ramen för en e-tjänst kan myndigheten bestämma vilket format som skall användas. I detta fall utgår vi från ett elektroniskt formulär där uppgifterna skrivs in i en XML-struktur. Figur 2 visar uppgifter som har fyllts i och som skall skrivas under elektroniskt. I figur 3 visas några av blankettfälten i en deklaration på papper. Vid en jämförelse framgår hur pappersblankettens kodade fält motsvaras av XML-element.

Figur 2.

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<!DOCTYPE eink SYSTEM "system:eink.dtd">
- <eink>
  <idPers>700311-xxxx</idPers>
  <skm>01</skm>
  <skr>22</skr>
  <datum>20050501</datum>
  <inlamningstyp>C</inlamningstyp>
  <kvittens>20050501135008197003llxxxx</kvittens>
  <r03 status="f">102398</r03>
  <r43 status="f">2000</r43>
  <r53 status="n">9399</r53>
  <r102 status="f">0</r102>
</eink>
```

Figur 3.

Skatteverket

Senast måndagen den 2 maj 2005
ska deklarationen finnas hos Skatteverket.

OBS! Har du fått en förtryckt inkomstdeklaration ska du använda den när du deklarerar. Om du lämnar in denna manuella blankett måste du själv fylla i alla belopp.

Läs först i "Dags att deklarera" hur du ska fylla i blanketten.

Inkomstdeklaration 1 **2005**
Inkomståret 2004

Person-/Organisationsnummer: 700311-XXXX **M**

Namn och adress

OBS!
Denna blankett kan du bara använda för att räkna ut din skatt. När du deklarerar ska du använda den FÖRTRYCKTA deklarationsblanketten som du får hemskickad under perioden slutet av mars till början av april 2005.

① Inkomster - Tjänst

Lön, förmåner, sjukpenning m.m.	03	102398
Kostnadsersättningar	05	
Allmän pension och tjänstepension	14	

④ Kapital

Ränteinkomster, utdelningar m.m.	50	
Överskott vid uthyrning av privatbostad enligt blankett K3	51	
Avdrag för ränteutgifter m.m.	53	9399

20 Exemplen har hämtats från Skatteverket, till största delen från hanteringen av inkomstdeklarationer för år 2005. Exemplen är delvis avidentifierade.

3.3.2 Handlingen skrivs under

När blanketten har fyllts i undertecknas den med hjälp av ett program som knyter handlingen till utställaren. Som ett första steg beräknas en kontrollsumma baserad på texten. Kontrollsumman är ett för varje text unikt beräknat resultat, med fast längd. Därefter skapas underskriften genom att kontrollsumman krypteras med avsändarens privata nyckel.

Samtliga beståndsdelar bl.a. text, krypterad kontrollsumma, metodbeskrivning, uppgifter ur legitimationen (inkl. den publika nyckeln) och uppgifter om tidpunkten för undertecknande, sammanfogas till ett paket som kodas för att säkerställa överföringen till mottagaren. Därefter skickas den underskrivna handlingen till mottagningsfunktionen för aktuell e-tjänst, dvs. den funktion för automatiserad behandling som myndigheten har anvisat som mottagningsställe.

3.3.3 Den underskrivna handlingens format

Den underskrivna handling som skickas till myndigheten utgörs av en datamängd i PKCS#7-format. Formatet erbjuder två alternativa sätt att hantera den underskrivna handlingen. PKCS#7-attached innebär att underskriften och handlingen tekniskt hanteras som *en fil*, medan PKCS#7-detached innebär att underskriften och resten av handlingen hanteras som *två olika filer*. Skillnaden är rent teknisk och saknar betydelse för handlingens funktion och hur den uppfattas av mottagaren. Det påverkar inte heller möjligheterna till kontroll och bevarande. Det som visas i figur 4 är ett antal element i formatet PKCS#7-attached. Innehållet är inte direkt läsbart då det är kodat.[21] För att det skall förstås av mottagaren måste datamängden avkodas.

Vid avkodningen framträder den struktur enligt ASN.1 som utgör PKCS#7-paketet.[22] I figur 5 visas den första delen av strukturen. Där framgår bl.a. att metoden SHA-1 har använts när strukturen undertecknades.[23] Längre ner i figuren framträder det XML-dokument som har framställts och undertecknats. För att få en närmare förståelse av hur uppgifterna i pappersblanketten, XML-dokumentet och ASN.1-strukturen förhåller sig till varandra kan man jämföra figur 2, 3, och 5.

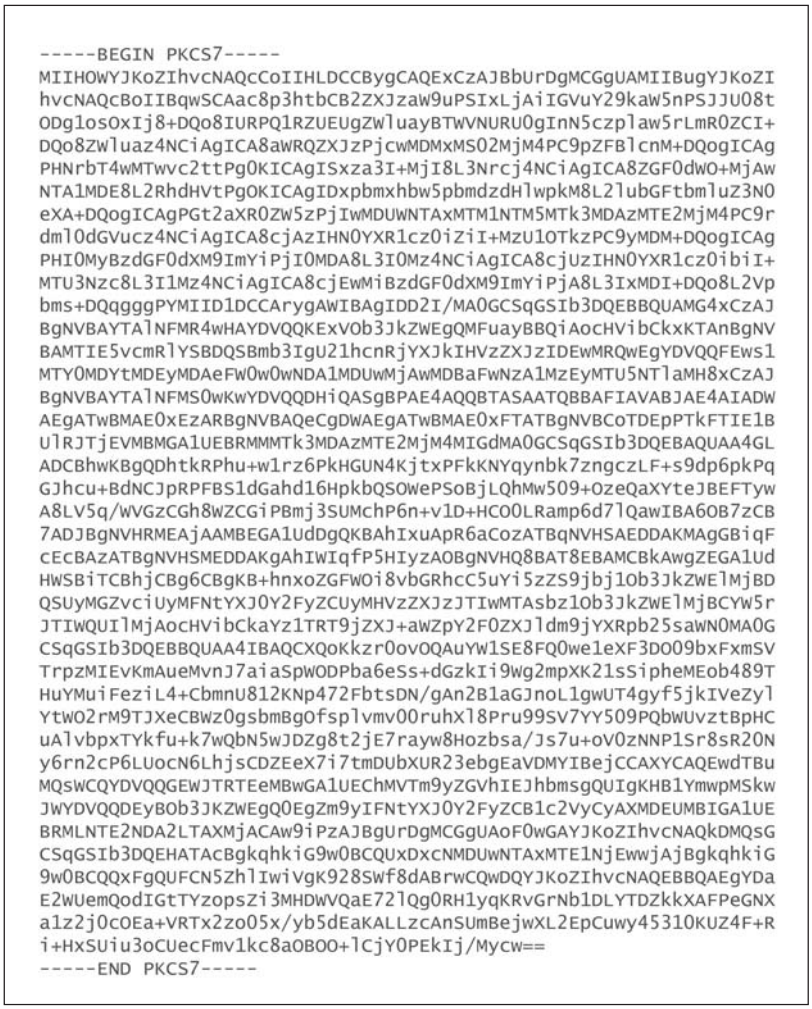
I figur 6 framträder ”signingTime”, dvs. uppgifter om att dokumentet undertecknats den 1 maj 2005 klockan 11:56:10, enligt undertecknarens dator. Där återfinns även ”messageDigest” (kontrollsumman) och ”rsaEncryption” (den krypterade kontrollsumman).

21 Kodningen är i detta fall i Base64-format.

22 ITU-T Recommendation X.208: Specification of Abstract Syntax Notation One (ASN.1)

23 SHA-1, Secure Hash Algorithm, är en metod för att en skapa en kontrollsumma.

Figur 4.



```
-----BEGIN PKCS7-----
MIIHOWYJKoZIhvcNAQcCoIIHLDCCBygCAQExCzAJBbUrDgMCGgUAMIIBugYJKoZI
hvcNAQcBoIIBqwSCAac8p3htbCB2ZXJzaW9uPSIxLjAiIGVuY29kaW5nPSJJU08t
ODg1osOxIj8+DQo8IURPQlRZUEUgZWluayBTWVNURU0gInN5czplaw5rLmR0ZCI+
DQo8ZWluaz4NCiAgICA8aWRQZXJzPjcwMDMxMS02MjM4PC9pZFBlcnM+DQogICAg
PHNrbT4wMTwvc2ttPg0KICAgISxza3I+MjI8L3Nrcj4NCiAgICA8ZGF0dWO+MjAw
NTA1MDE8L2RhdHVtPg0KICAgIDxpbmxhbw5pbmdzdHlwpkM8L2lubGFtbmluZ3N0
eXA+DQogICAgPGt2aXR0ZW5zPjIwMDUwNTAxMTM1NTM5MTk3MDAzMTE2MjM4PC9r
dml0dGVucz4NCiAgICA8cjAzIHN0YXR1cz0iZiI+MzU1OTkzPC9yMDM+DQogICAg
PHI0MyBzdGF0dXM9ImYiPjI0MDA8L3I0Mz4NCiAgICA8cjUzIHN0YXR1cz0ibiI+
MTU3Nzc8L3I1Mz4NCiAgICA8cjEwMiBzdGF0dXM9ImYiPjA8L3IxMDI+DQo8L2Vp
bms+DQqgggPYMIID1DCCArygAWIBAgIDD2I/MA0GCSqGSIb3DQEBBQUAMG4xCzAJ
BgNVBAYTAlNFMR4wHAYDVQQKExVOb3JkZWEgQMFuayBBQiAocHVibCkxKTAnBgNV
BAMTIE5vcmRlYSBDQSBmb3IgU21hcnRjYXJkIHVzZXJzIDEwMRQwEgYDVQQFEws1
MTY0MDYtMDEyMDAeFW0w0wNDA1MDUwMjAwMDBaFwNzA1MzEyMTU5NTlaMH8xCzAJ
BgNVBAYTAlNFMS0wKwYDVQQDHiQASgBPAE4AQQBTASAATQBBAFIAVABJAE4AIADW
AEgATwBMAE0xEzARBgNVBAQeCgDWAEgATwBMAE0xFTATBgNVBCoTDEpPTkFTIE1B
UlRJTjEVMBMGA1UEBRMMMTk3MDAzMTE2MjM4MIGdMA0GCSqGSIb3DQEBAQUAA4GL
ADCBhwKBgQDhtkRPhu+w1rz6PkHGUN4KjtxPFkKNYqynbk7zngczLF+s9dp6pkPq
GJhcu+BdNCJpRPFBS1dGahd16HpkbQSOWePSoBjLQhMw5O9+OzeQaXYteJBEFTyw
A8LV5q/WVGzCGh8WZCGiPBmj3SUMchP6n+v1D+HCO0LRamp6d7lQawIBA6OB7zCB
7ADJBgNVHRMEAjAAMBEGA1UdDgQKBAhIxuApR6aCozATBqNVHSAEDDAKMAgGBiqF
cEcBAzATBgNVHSMEDDAKgAhIWIqfP5HIyzAOBgNVHQ8BAT8EBAMCBkAwgZEGA1Ud
HWSBiTCBhjCBg6CBgKB+hnxoZGFWOi8vbGRhcC5uYi5zZS9jbj1Ob3JkZWElMjBD
QSUyMGZvciUyMFNtYXJ0Y2FyZCUyMHVzZXJzJTIwMTAsbz1Ob3JkZWElMjBCYW5r
JTIWQUIlMjAocHVibCkaYz1TRT9jZXJ+aWZpY2F0ZXJldm9jYXRpb25saWN0MA0G
CSqGSIb3DQEBBQUAA4IBAQCXQoKkzr0ovOQAuYW1SE8FQ0we1eXF3DO09bxFxmSV
TrpzMIEvKmAueMvnJ7aiaSpWODPba6eSs+dGzkIi9Wg2mpXK21sSipheMEob489T
HuYMuiFeziL4+CbmnU812KNp472FbtsDN/gAn2B1aGJnoL1gwUT4gyf5jkIVeZyl
YtWO2rM9TJXeCBWz0gsbmBgOfsplvmv00ruhXl8Pru99SV7YY509PQbWUvztBpHC
uAlvbpxTYkfu+k7wQbN5wJDZg8t2jE7rayw8Hozbsa/Js7u+oV0zNNP1Sr8sR20N
y6rn2cP6LUocN6LhjsCDZEeX7i7tmDUbXUR23ebgEaVDMYIBejCCAXYCAQEwdTBu
MQswCQYDVQQGEwJTRTEeMBwGA1UEChMVTm9yZGVhIEJhbmsgQUIgKHB1YmwpMSkw
JwYDVQQDEyBOb3JkZWEgQ0EgZm9yIFNtYXJ0Y2FyZCB1c2VyCyAXMDEUMBIGA1UE
BRMLNTE2NDA2LTAXMjACAw9iPzAJBgUrDgMCGgUAoF0wGAYJKoZIhvcNAQkDMQsG
CSqGSIb3DQEHATAcBgkqhkiG9w0BCQUxDxcNMDUwNTAxMTE1NjEwwjAjBgkqhkiG
9w0BCQQxFgQUFCN5ZhlIwivgK928Swf8dABrwCQwDQYJKoZIhvcNAQEBBQAEgYDa
E2WUemQodIGtTYzopsZi3MHDWVQaE72lQgORH1yqKRvGrNb1DLYTDZkkXAFPeGNX
a1z2j0cOEa+VRTx2zoO5x/yb5dEaKALLzcAnSUmBejwXL2EpCuwy45310KUZ4F+R
i+HxSUiu3oCUecFmv1kc8aOBOO+lCjY0PEkIj/Mycw==
-----END PKCS7-----
```

Figur 5.

```
  0:d=0  hl=4  l=1851  cons: SEQUENCE
  4:d=1  hl=2  l=   9  prim: OBJECT        :pkcs7-signedData
 15:d=1  hl=4  l=1836  cons: cont [ 0 ]
 19:d=2  hl=4  l=1832  cons: SEQUENCE
 23:d=3  hl=2  l=   1  prim: INTEGER       :01
 26:d=3  hl=2  l=  11  cons: SET
 28:d=4  hl=2  l=   9  cons: SEQUENCE
 30:d=5  hl=2  l=   5  prim: OBJECT        :sha1
 37:d=5  hl=2  l=   0  prim: NULL
 39:d=3  hl=4  l= 442  cons: SEQUENCE
 43:d=4  hl=2  l=   9  prim: OBJECT        :pkcs7-data
 54:d=4  hl=4  l= 427  cons: cont [ 0 ]
 58:d=5  hl=4  l= 423  prim: OCTET STRING  :<?xml version="1.0" encoding="ISO-8859-1" ?>
  <!DOCTYPE eink SYSTEM "system:eink.dtd">
- <eink>
   <idPers>700311-xxxx</idPers>
   <skm>01</skm>
   <skr>22</skr>
   <datum>20050501</datum>
   <inlamningstyp>C</inlamningstyp>
   <kvittens>20050501135008197003llxxxx</kvittens>
   <r03 status="f">102398</r03>
   <r43 status="f">2000</r43>
   <r53 status="n">9399</r53>
   <r102 status="f">0</r102>
  </eink>
```

Figur 6.

```
1618:d=7  hl=2  l=   9 prim: OBJECT        :contentType
1629:d=7  hl=2  l=  11 cons: SET
1631:d=8  hl=2  l=   9 prim: OBJECT        :pkcs7-data
1642:d=6  hl=2  l=  28 cons: SEQUENCE
1644:d=7  hl=2  l=   9 prim: OBJECT        :signingTime
1655:d=7  hl=2  l=  15 cons: SET
1657:d=8  hl=2  l=  13 prim: UTCTIME       :050501115610Z
1672:d=6  hl=2  l=  35 cons: SEQUENCE
1674:d=7  hl=2  l0   9 prim: OBJECT        :messageDigest
1685:d=7  hl=2  l=  22 cons: SET
1687=d=8  hl=2  l=  20 prim: OCTET STRING
     0000 - 14 23 79 66 19 48 c2 25-60 2b dd bc 49 67 fc 74    .#yf.H.%`+..Ig.t
     0010 - 00 6b c0 24                                        .k.$
1709:d=5  hl=2  l=  13 cons: SEQUENCE
1711:d=6  hl=2  l=   9 prim: OBJECT        :rsaEncryption
1722:d=6  hl=2  l=   0 prim: NULL
1724:d=5  hl=3  l= 128 prim: OCTET STRING
     0000 - da 13 65 94 7a 64 28 74 81 ad 4d 8c e8 a6 c6 62    .e.zd(t..M....b
     0010 - dc c1 c3 59 54 1a 13 bd a5 42 0d 11 1f 5c aa 29    ..YT....B...\.)
     0020 - 1b c6 ac d6 f5 0c b6 13 0d 99 24 5c 01 4f 78 63    ..........$\.Oxc
     0030 - 57 6b 5c f6 8f 47 0e 11 af af 45 3c 76 ce 8d 39    Wk\..G....E<v..9
     0040 - c7 fc 9b e5 d1 1a 28 02 cb cd c0 27 49 49 81 7a    ......(....II.z
     0050 - 3c 17 2f 61 29 0a ec 32 e3 9d f5 d0 a5 19 e0 5f    <./a)..2......_
     0060 - 91 8b e1 f1 49 48 ae de 80 94 79 c1 66 bf 59 1c    ....IH....y.f.Y.
     0070 - f1 a3 81 38 ef a5 0a 36 34 3c 49 08 8f f3 32 73    ...8...64<I...2s
```

Figur 7 visar kontrollsumman, och figur 8 den krypterade kontrollsumman (underskriften).

Figur 7.

```
14 23 79 66 19 48 c2 25-60 2b dd bc 49 67 fc 74 00 6b c0 24
```

Figur 8.

```
da 13 65 94 7a 64 28 74 81 ad 4d 8c e8 a6 c6 62
dc c1 c3 59 54 1a 13 bd a5 42 0d 11 1f 5c aa 29
1b c6 ac d6 f5 0c b6 13 0d 99 24 5c 01 4f 78 63
57 6b 5c f6 8f 47 0e 11 af af 45 3c 76 ce 8d 39
c7 fc 9b e5 d1 1a 28 02 cb cd c0 27 49 49 81 7a
3c 17 2f 61 29 0a ec 32 e3 9d f5 d0 a5 19 e0 5f
91 8b e1 f1 49 48 ae de 80 94 79 c1 66 bf 59 1c
f1 a3 81 38 ef a5 0a 36 34 3c 49 08 8f f3 32 73
```

3.3.4 Kontroll av den inkomna handlingen

Myndighetens kontroll av den elektroniskt underskrivna handlingen sker med stöd av en hel infrastruktur, en s.k. Public Key Infrastructure (PKI). Hur en PKI-struktur fungerar beskrivs inte närmare i denna rapport. Här fokuseras istället på den elektroniskt underskrivna handlingen.

Kontrollen omfattar följande moment. När paketet har mottagits upprepar myndigheten den beräkning som gjordes vid undertecknandet. Det sker genom att den angivna metoden (SHA-1) används för att framställa en ny kontrollsumma. Dessutom dekrypteras den krypterade kontroll-

summa som utgör underskriften så att den ursprungligen beräknade kontrollsumman framträder. Om kontrollsummorna inte överensstämmer betyder det att texten har förvanskats. Den mottagande myndigheten kontrollerar även att den e-legitimation som använts vid undertecknandet är utgiven av en ID-tjänst som myndigheten har valt att lita på, och att e-legitimationen inte är spärrad. Spärrkontrollen sker med hjälp av listor som inhämtas från den som har utfärdat e-legitimationen eller genom spärrkontrollfrågor och svar på spärrkontrollfrågor i realtid (OCSP).[24]

Om inget fel upptäcks vid kontrollen överförs de uppgifter som behövs för handläggningen till myndighetens verksamhetssystem. Den inkomna handlingen bevaras i ursprungligt skick, och utfallet av kontrollen dokumenteras.

3.3.5 Myndighetens stämpel och dess format

Att kontroll har skett kan dokumenteras på olika sätt, t.ex. genom att handlingen stämplas med myndighetens elektroniska stämpel. Stämpeln är ingen garanti för att handlingen skall förbli oförvanskad och bevarad i ursprungligt skick. Den kan däremot användas för att kontrollera om förvanskning har skett efter att den initiala kontrollen gjordes.

Myndighetens stämpel skulle kunna jämföras med en traditionell ankomststämpel. Att i IT-miljön återskapa motsvarigheter till företeelser i pappersmiljön är inte någon självklarhet. Det kan dock finnas ett värde i att även i fortsättningen kunna tala om att handlingar som kommer in till en myndighet ankomststämplas. Genom stämpeln skapas även förutsättningar för gallring av vissa andra handlingar, t.ex. spärrlistor och OCSP-svar.

När en handling stämplas skapas i praktiken en ny handling där den ursprungliga handlingen ingår tillsammans med andra uppgifter. Här avses uppgifter som hämtats ur den ursprungliga handlingen, från utfärdaren av certifikatet och från myndighetens IT-system, t.ex. uppgifter om

- ingivare,
- tidpunkt för inkommande,
- handlingens innehåll i klartext,
- utfallet av kontrollen, samt
- handlingen i sitt ursprungliga format.[25]

24 OCSP, Online Certificate Status Protocol, används för att verifiera giltigheten hos elektroniska underskrifter. OCSP ersätter spärrlistor, Certificate Revocation Lists (CRL).

25 Tidsangivelsen samordnas med tidpunkten för inkommande enligt 10 § FL; jfr e-nämndens vägledning för hantering av inkommande elektroniska handlingar (05:02).

Självfallet står det myndigheterna fritt att utforma XML-strukturen med utgångspunkt från den egna verksamhetens behov. Informationen fogas in i den XML-struktur som visas i figur 9.[26]

Figur 9.

```
- <Inkommen_e-handling>
  - <Ingivare>
      <Personnummer>700311-xxxx</Personnummer>
      <Namn>Jonas Martin Öholm</Namn>
    </Ingivare>
  - <Tid>
      <Datum>20050501</Datum>
      <Klockslag>135008</Klockslag>
    </Tid>
  - <Text_undertecknad_av _ingivaren>
      <Originalheader>?xml version="1.0" encoding="ISO-8859-1"</Originalheader>
    - <Ansökan_om_bostadsbidrag>
        <Personnummer>700311-xxxx</Personnummer>
        <Ansökningsdatum>20050501</Ansökningsdatum>
        <Inlämningstyp>e-legitimation</Inlämningstyp>
        <Kvittens>20050501135008197003llxxxx</Kvittens>
        <Årsinkomst>102398</Årsinkomst>
        <A-kassa>Nej</A-kassa>
        <Studiemedel>6300</Studiemedel>
      </Ansökan_om_bostadsbidrag>
    </Text_undertecknad_av_ingivaren>
   - <Utfall_av_äkthetkontroll_vid_inlämningen>
      <OK_eller_FALSK>OK</OK_eller_FALSK>
    </Utfall_av_äkthetskontroll_vid_inlämningen>
   + <Handlingen_i_sitt_ursprungliga_format>
  </Inkommen_e-handling>
```

I figur 10 visas innehållet i hela XML-strukturen. I strukturen återfinns elementet <Handlingen_i_sitt_ursprungliga_format> som innehåller den underskrivna Base64-kodade handlingen. Den finns således bevarad i ursprungligt skick, samtidigt som uppgifterna lagras i klartext i den nya handlingen.

3.4 VAL AV FORMAT FÖR UNDERSKRIFT OCH STÄMPEL

I de exempel som redovisats används formatet PKCS#7-attached för underskriften och formatet XML-Signature för myndighetens stämpel. Formaten utgör som framgått endast två av flera standardiserade format. Att PKCS#7 används för underskriften och XML-Signature för myndighetens stämpel, beror på att PKCS#7 har bedömts vara ett bättre alternativ för masshantering vid inkommandetidpunkten medan XML-Signature ger bättre läsbarhet över tiden.

En vidareutveckling av XML-Signature är XML Advanced Electronic Signatures (XAdES), som tagits fram för att anpassa XML-Signature till krav i Europeiska Unionens direktiv, Directive 1999/93/EC of the Euro-

26 Exemplet i figur 10 har hämtats från en bostadsansökan, till skillnad från tidigare figurer som hämtats från en inkomstdeklaration.

Figur 10.

```
<?xml version="1.0" encoding="UTF-8" ?>
- <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
- <SignedInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
  <CanonicalizationMethod
Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments"
xmlns="http://www.w3.org/2000/09/xmldsig#" />
  <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"
xmlns="http://www.w3.org/2000/09/xmldsig#" />
- <Reference URI="#signedObject"
xmlns="http://www.w3.org/2000/09/xmldsig#">
  <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"
xmlns="http://www.w3.org/2000/09/xmldsig#" />
  <DigestValue
xmlns="http://www.w3.org/2000/09/xmldsig#">hGkEDlCYBn6gMFgeOWNP4k7K2aA=</DigestValue>
  </Reference>
  </SignedInfo>
  <SignatureValue
xmlns="http://www.w3.org/2000/09/xmldsig#">S1MvzeurOTJYqdbBZZXl+A+f5OuBls5acrISYaZY4Jsb6xrVqT6I+pRlDlHz7v0G
sa2aHqvx65FMZCNV/lnVWg==</SignatureValue>
- <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
- <X509Data xmlns="http://www.w3.org/2000/09/xmldsig#">
  <X509Certificate>MIIC1TCCAT2hhk</X509Certificate>
  </X509Data>
  </KeyInfo>
- <Object Id="signedObject" xmlns="http://www.w3.org/2000/09/xmldsig#">
- <Inkommen_e-handling xmlns="http://www.bidragsverket.se/bostad">
- <Ingivare>
  <Personnummer>700311-xxxx</Personnummer>
  <Namn>Jonas Martin Öholm</Namn>
  </Ingivare>
- <Tid>
  <Datum>20050501</Datum>
  <Klockslag>135008</Klockslag>
  </Tid>
- <Text_undertecknad_av_ingivaren>
  <Orginalheader>?xml version="1.0" encoding="ISO-8859-1"?</Orginalheader>
- <Ansökan_om_bostadsbidrag>
  <Personnummer>700311-6238</Personnummer>
  <Ansökningsdatum>20050501</Ansökningsdatum>
  <Inlämningstyp>e-legitimation</Inlämningstyp>
  <Kvittens>20050501135008197003116238</Kvittens>
  <Årsinkomst>102398</Årsinkomst>
  <A-kassa>Nej</A-kassa>
  <Studiemedel>6300</Studiemedel>
  </Ansökan_om_bostadsbidrag>
  </Text_undertecknad_av_ingivaren>
- <Utfall_av_äkthetskontroll_vid_inlämningen>
  <OK_eller_FALSK>OK</OK_eller_FALSK>
  </Utfall_av_äkthetskontroll_vid_inlämningen>
- <Handlingen_i_sitt_ursprungliga_format>
  <PKCS7>MIIHOwYJCjYOPEkIj/MyCw==</PKCS7>
  </Handlingen_i_sitt_ursprungliga_format>
  </Inkommen_e-handling>
  </Object>
  </Signature>
```

pean Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, och för att implementera ETSI-standarden TS 101 733.

3.5 HUR MYNDIGHETERNA GÖR

En genomgång har gjorts av hanteringen hos ett par myndigheter som har inrättat e-tjänster. Myndigheterna kontrollerar omedelbart efter ankomsten handlingens äkthet i enlighet med standardiserade rutiner för PKI.[27] Om inget fel upptäcks förses handlingen med en tidsangivelse och myndighetens elektroniska stämpel. Uppgifterna i handlingen kopieras till myndighetens verksamhetssystem, medan det stämplade PKCS#7-paketet bevaras i en särskild funktion.

Trots att myndigheterna har gjort initiala äkthetskontroller och dessa har dokumenterats har inget av det ursprungliga kontrollmaterialet raderats

27 Det sker i en teknisk funktion som inom standardiseringsarbetet kallas för notariattjänst.

hos myndigheterna. Även inkomna spärrlistor och svar på spärrfrågor m.m. har bevarats. Ett bevarande stämmer också överens med vad som gäller i enlighet med arkivförfattningarna, om det inte finns gallringsföreskrifter för de aktuella handlingarna.

Sammanfattningsvis har myndigheterna gjort vissa val utifrån den syn som vuxit fram i arbetet med internationell standardisering, nämligen att göra kontroller av äkthet i ett tidigt skede och att förse handlingen med en elektronisk stämpel, dvs. en ny ”elektronisk underskrift” som är knuten till myndigheten, inte till en viss individ, och som bygger på en annan kontrollstruktur än den för e-underskriften.

4 ETT KOMPLEXT OMRÅDE

4.1 OLIKA UPPFATTNINGAR

Frågor som rör myndigheternas hantering av elektroniskt underskrivna handlingar är såväl tekniskt som juridiskt komplexa. Under de diskussioner som har förts med jurister, säkerhetsarkitekter, IT-arkitekter, arkivarier m.fl. har följaktligen många olika uppfattningar kommit till uttryck. I detta avsnitt behandlas några av de frågor som har diskuterats.

4.2 FRÅGOR SOM HAR AKTUALISERATS

En uppfattning som har framförts är att den elektroniska underskriften innefattar en uppsättning av kontrollfunktioner som inte kan långtidslagras då de mister sin styrka i takt med ökad processorkraft och matematiska genombrott. Med en sådan utgångspunkt kan det förefalla mest rationellt att enbart bevara texten i den underskrivna handlingen. Mot detta står lagstiftningens krav på ett bevarande i ursprungligt skick.

Vad är det då som skall bevaras? En första åtgärd har varit att analysera vad som avses med en elektroniskt underskriven handling. En teknisk analys har redovisats i avsnitt 3. Det har konstaterats att hela PKCS#7-paketet utgör den elektroniskt underskrivna handlingen. Att underskriften inte är läsbar på traditionellt sätt saknar betydelse i sammanhanget.

Finns det några krav i arkivförfattningarna som säger att elektroniska underskrifter skall användas? Frågan besvaras i avsnitt 5.1. En annan fråga rör de upptagningar och den infrastruktur som finns utanför myndighetens gränser, och som används som stöd för äkthetskontrollerna. Bör sådana handlingar hämtas in för att möjliggöra en fullständig upprepning av den initiala kontrollen? Se avsnitt 5.2.

Myndighetens ansvar för att skapa säkra kommunikations- och handläggningsrutiner övergår efter den initiala kontrollen i ett ansvar för förvaltning och skydd av den elektroniskt underskrivna handlingen. Även efter att den initiala kontrollen har skett skall handlingen kunna tillgodose allmänhetens, förvaltningens, rättskipningens och forskningens behov av oförvanskad information. I avsnitt 5.3 behandlas skillnaden mellan begreppen ursprungligt skick och äkthet.

En vanlig uppfattning är att det inte går att påverka de inkomna handlingarnas format, och att de därför måste konverteras för att kunna läsas på sikt. En konvertering innebär att den elektroniska underskriften till störs-

ta delen förlorar sin funktion. En fråga har därför varit i vilken omfattning en myndighet kan säkerställa att handlingar med e-underskrift redan från början ges det format de skall ha när de långtidslagras. Se avsnitt 6.

Är det tillräckligt med säkra processer för att skydda de elektroniskt underskrivna handlingarna efter ankomsten till myndigheten, eller behövs det även myndighetsstämplar? Krävs det ytterligare åtgärder? I avsnitt 7 behandlas flera åtgärder som krävs för ett bevarande.

5 ÄKTHET OCH URSPRUNGLIGT SKICK

5.1 VERKSAMHETENS BEHOV

Av e-nämndens vägledning för hantering av inkommande elektroniska handlingar (05:02) framgår hur infrastrukturer för e-legitimationer och ID-tjänster bör användas när en myndighet kontrollerar om den som framstår som utställare av en handling verkligen har undertecknat den och om texten har ändrats. Motsvarande kontroller av pappersurkunder görs först när någon har ifrågasatt handlingens äkthet. Analyser kan i sådana fall göras vid kriminaltekniska laboratorier.

Det är denna fråga om äkthet som avses när en tillämpning övervägs av 10 § tredje stycket förvaltningslagen (1986:223; FL), där det föreskrivs att ett meddelande som inte är underskrivet skall bekräftas av avsändaren genom en egenhändigt undertecknad handling, om myndigheten begär det. För att skydda allmänhetens tillit till elektroniskt underskrivna handlingar och att undgå falska utsagor finns vidare regler om kvalificerade elektroniska signaturer, om straffansvar för urkundsförfalskning[28] och om form för vissa rättshandlingar, t.ex. att ansökan i mål eller ärenden eller utsagor av särskilt känsligt slag skall vara egenhändigt undertecknade.[29] Det är således verksamhetens krav och straff- och näringsrättsliga skyddsregler m.m. som ligger till grund för myndigheternas införande och användning av elektroniska underskrifter med anknytande funktioner för spärrkontroll m.m.

I arkivförfattningarna ställs inga krav på användning av elektroniska underskrifter. Där finns inte heller några bestämmelser om att det bästa bevismaterialet, t.ex. ett original, inte en kopia, skall användas vid en bevisupptagning inför domstol. Detta regleras i processuella regler.[30] I praktiken ges vanligtvis ovidimerade fotokopior in så länge en handlings äkthet inte ifrågasätts av part.

28 Se lagen (2000:832) om kvalificerade elektroniska signaturer och 14 kap. brottsbalken.

29 Se bl.a. 3 § förvaltningsprocesslagen (1971:291) där det föreskrivs att en ansöknings- eller besvärshandling från en enskild skall vara egenhändigt undertecknad och bestämmelsen i 10 kap. 1 § ärvdabalken om att testator skall skriva under sin testamentshandling och att vittnena skall bestyrka handlingen.

30 Se t.ex. 35 kap. 8 § rättegångsbalken.

Det är i första hand verksamhetens behov som avgör vilka rutiner för kontroll av äkthet som skall införas för myndigheternas handläggning av ärenden och för myndigheternas informationssäkerhet.

Arkivförfattningarna ställer inte krav på att kontroller av inkomna handlingars *äkthet* skall utföras. Krav på kontrollrutiner och dokumentation av utfallet kan dock ställas som en förutsättning för gallring av andra handlingar i en e-tjänst.

5.2 INHÄMTANDE AV REFERENSMATERIAL

När en elektroniskt underskriven handling kommer in till en myndighet och äkthetskontrolleras sker det med stöd av en hel infrastruktur. Av förklarliga skäl kan inte hela denna struktur och varje uppgift med anknytning till strukturen inhämtas för att bevaras hos myndigheten. En annan sak är att myndigheter utifrån verksamhetens krav ser till att den som tillhandahåller en ID-tjänst bevarar handlingar under den tid som de kan behövas hos myndigheten.

Arkivförfattningarna ställer inga krav på vilka handlingar som myndigheten skall inhämta från andra aktörer för att säkerställa möjligheterna till kontroll på kort och lång sikt. Däremot följer det av arkivförfattningarna att handlingar som faktiskt har kommit in till en myndighet inom ramen för en e-tjänst, t.ex. handlingar som har inhämtats för äkthetskontrollen, bevaras om det inte följer av föreskrifter eller beslut att gallring får ske.

Krav på att hämta in handlingar från andra aktörer följer inte av arkivförfattningarna. Om så sker får handlingarna inte gallras utan föreskrifter eller ett beslut om gallring.

5.3 ÄKTHET OCH URSPRUNGLIGT SKICK ÄR INTE DETSAMMA

Det finns en skillnad mellan vad som avses med äkthet enligt brottsbalken och 10 § tredje stycket FL respektive ursprungligt skick på det sätt som förutsätts i TF och arkivförfattningarna. Med *äkthet* avses att en handling omanipulerat härrör från den som framstår som utställare. I denna rapport används begreppet i en sådan betydelse.

Med bevarande i *ursprungligt skick* avses att handlingar bevaras så som de var när de kom in till eller upprättades hos myndigheten. Alla åtgärder som vidtas med handlingarna och som leder till informationsförlust utgör gallring, enligt arkivförfattningarna; se avsnitt 2.5.2. Även om en handling skulle visa sig vara förfalskad skall den bevaras i ursprungligt skick, och får inte gallras utan stöd i föreskrifter av Riksarkivet. Det är en annan sak att en upptäckt av en förfalskning skall dokumenteras och att åtgärden att förfalska kan föranleda rättsliga åtgärder.

När en myndighet överväger hur elektroniskt underskrivna handlingar skall hanteras bör frågor om äkthet och ursprungligt skick inte blandas samman. Behovet av att bevara handlingarna i ursprungligt skick står emellertid inte i motsättning till behovet av att kunna bedöma deras äkthet. Möjligheterna till äkthetsbedömning tillhör de förutsättningar som beaktas när bevarande och gallring utreds.

6 LÄMPLIGT FORMAT FÖR BEVARANDE

6.1 FORMAT SOM KAN BEVARAS

Som tidigare framgått skall myndigheterna vid framställning av handlingar välja ett format som gör det möjligt att bevara handlingarna i ursprungligt skick. Valet av ursprungligt format är av stor betydelse när det gäller elektroniskt underskrivna handlingar då underskriften till största delen förlorar sin funktion om handlingarna konverteras; se avsnitt 2.5.1.

Riksarkivet föreskriver för statliga myndigheter om materiel och metoder för framställning av handlingar. Kraven är tillämpliga även på inkomna handlingar i den mån myndigheten kan styra i vilket format handlingarna framställs. Rätten att föreskriva gäller emellertid inte i förhållande till privaträttsliga aktörer eller kommuner.[31]

Till detta kommer att myndigheternas serviceskyldighet numera innefattar att se till att det är möjligt för enskilda att kontakta myndigheten med hjälp av telefax och elektronisk post och att svar kan lämnas på samma sätt; 5 § andra stycket FL. För utvecklingen av e-förvaltningen är det en viktig fråga om serviceskyldigheten medför att myndigheter som tillhandahåller e-tjänster måste ta emot handlingar i alla format.

Det är allmänt vedertaget att e-tjänster bygger på webbformulär och liknande tekniska lösningar. Det innebär att e-post med bilagor och andra liknande handlingar inte kan ges in till den mottagningsfunktion som myndigheten tillhandahåller som ”postbox” för handlingar som upprättats med stöd av en e-tjänst. I e-tjänsterna styrs alltså format m.m. så att myndigheten får in handlingarna utformade på lämpligt sätt, i det format de skall granskas och långtidslagras. Sådana begränsningar torde inte strida mot reglerna om service i 5 § andra stycket FL. I lagmotiven anfördes bl.a. att andra kommunikationssätt än telefax och e-post inte kunde anses vara så etablerade att det fanns anledning att införa dessa metoder i förvaltningslagens serviceregler.[32]

Bestämmelsen i 5 § FL utgör emellertid en minimiregel. De begränsningar som en myndighet inför beträffande möjligheterna till ingivning via en e-tjänst måste vara förenliga med god förvaltningsrättslig praxis;

31 Jfr 8 kap. 3 och 5 §§ regeringsformen.

32 Begreppet e-post, som inte preciseras närmare i lagmotiven, torde inte innefatta insändande av handlingar med stöd av en e-tjänst.

jfr 7 § andra stycket 5 verksförordningen (1995:1322). Här bör noteras att e-tjänsterna typiskt sett ger medborgarna en betydande service i form av hjälp och stöd för att fylla i uppgifter i inlagor och att enkelt och billigt ge in dessa via nät, utan tidsutdräkt. Denna service går betydligt längre än den miniminivå som föreskrivs i 5 § FL, en bestämmelse som inte innebär att användaren måste få välja format för sina inlagor. Skulle någon ha behov av att välja ett annat format, som e-tjänsten och mottagningsfunktionen för e-tjänsten inte förmår att hantera, kan denne alltjämt ge in en försändelse via e-post, telefax eller som vanlig post.

Sakligt grundade begränsningar av vilka format som en myndighet godtar vid ingivning till en mottagningsfunktion för en e-tjänst – t.ex. med stöd av föreskrifter som Riksarkivet utfärdat om format – kan knappast stå i strid med en myndighets serviceskyldighet. Här bör också uppmärksammas de hot och risker för bl.a. datavirus och intrång som uppkommer om myndigheterna inte kan begränsa sin hantering till handlingar med format som det finns tekniska och administrativa förutsättningar att kunna behandla på ett säkert sätt.

6.2 KAN KRAV STÄLLAS PÅ LÄMPLIGT FORMAT

För kommunikation med enskilda kan noteras att 5 § andra stycket FL gäller för telefax och elektronisk post. Där regleras inte på vilket sätt och i vilken omfattning en myndighet som tillhandahåller en e-tjänst skall vara tillgänglig för enskilda via just den kanalen. Det finns inte heller några andra regler om service som ålägger en myndighet att tillhandahålla *e-tjänster* där tjänsten och dess mottagningsfunktion kan hantera alla format. Varje myndighet får bedöma i vilken utsträckning myndigheten bör begränsa sin tillgänglighet. Styrande är t.ex. verksamhetens art, e-tjänsternas art och funktionalitet, arbets- och resurssituationen och den grundlagsstadgade rätten att ta del av allmänna handlingar.

För handlingar som ges in till en myndighet inom ramen för en e-tjänst kan myndigheten i praktiken bestämma vilket format som skall väljas, oberoende av om det rör sig om kommunikation med andra myndigheter eller med enskilda. Det bör säkerställas att handlingarna redan från början ges det format som skall användas för att bevara handlingarna.

7 HANDLINGARNAS SKYDD ÖVER TIDEN

Myndighetens handlingar måste skyddas mot förstörelse, skada, tillgrepp och obehörig åtkomst. I den elektroniska miljön är det inte tillräckligt att servrar och bandrobotar förvaras i låsta och klimatreglerade utrymmen. Det krävs även behörighetssystem, brandväggar och andra åtgärder för att handlingarna skall vara skyddade mot förvanskning och obehörig åtkomst; se avsnitt 2.5.2.

7.1 UNDERSKRIFT FÖR ÄKTHET, STÄMPEL FÖR URSPRUNGLIGT SKICK

Skydd och kontroller av elektroniskt underskrivna handlingar bygger på automatiserade processer och handlingar som delvis finns utanför myndighetens gränser. En myndighet kan inte hämta in, bevara och upprätthålla hela den ursprungliga infrastruktur som behövs för att kontrollera e-underskrifterna. Myndigheterna har hanterat denna fråga genom rutiner för att göra en PKI-kontroll genast när en handling kommer in och att stämpla den mottagna handlingen och därvid intyga hur resultatet av kontrollen har utfallit. Efter att den initiala kontrollen har genomförts skyddas den inkomna handlingen mot förvanskning genom en elektronisk stämpel

Det har tidigare konstaterats att en elektronisk stämpel inte kan säkerställa att en handling förblir oförvanskad och bevarad i ursprungligt skick. Stämpeln utgör *ett* av flera sätt att möjliggöra upptäckt av förvanskning.

> Förenklat kan sägas att den elektroniska underskriften gör det möjligt att kontrollera handlingens *äkthet*, dvs. att uppgiften om utställare är riktig och att texten inte förvanskats.
>
> Myndighetens elektroniska stämpel gör det möjligt att bedöma om handlingen alltjämt är i *ursprungligt skick*, dvs. har samma innehåll som när den kom in till myndigheten och kontrollerades där.

7.2 ÅTGÄRDER FÖR ATT BEVARA OCH SKYDDA

Att särskilda skydd har skapats för elektroniskt underskrivna handlingar betyder inte att andra åtgärder är överflödiga. Som för övriga handlingar i elektronisk miljö krävs att det skall finnas *två (arkiv-)exemplar* av handlingarna. Handlingarna skall som i traditionell miljö vara skyddade genom att databärare och servrar förvaras säkert i *låsta utrymmen*. De två exemplaren bör vidare förvaras på skilda platser. Kompletterande skydd kan även skapas genom lagring på *beständiga databärare* (t.ex. vissa typer av worm-skivor) eller genom att så få personer som möjligt ges *tillgång* till funktioner som möjliggör förvanskning eller förstöring av handlingar. En annan möjlighet som har diskuterats är att ett exemplar av handlingarna omedelbart efter den initiala PKI-kontrollen överförs till arkivmyndighet eller annan tredje part.

Antagandet att det med tiden går att knäcka all kryptering har använts som argument mot ett bevarande av elektroniskt underskrivna handlingar. Mot detta kan anföras att handlingarna skyddas på *flera* sätt. En kombination av åtgärder krävs oavsett om det rör sig om elektroniskt underskrivna handlingar eller övriga handlingar. Utan sådana skyddsåtgärder som beskrivits ovan skulle handlingarna inte bara riskera att förvanskas. De skulle till och med riskera att helt förstöras. De nya möjligheter som elektroniska underskrifter och stämplar erbjuder när det gäller att upptäcka förvanskning bör ses som ett kompletterande skydd.

> För att bevara och skydda elektroniskt underskrivna handlingar behövs det en kombination av åtgärder.

8 BEVARANDE OCH GALLRING

8.1 VILKA HANDLINGAR MEDTAS I BEDÖMNINGEN

De handlingar som berörs av gallringsövervägandena är samtliga handlingar som har anknytning till den aktuella e-tjänsten, och som faktiskt finns inom myndighetens gränser, dvs. åtminstone följande

- den elektroniskt underskrivna handlingen, normalt omfattande text, kontrollsumma, krypterad kontrollsumma, den publika nyckeln och uppgifter ur undertecknarens e-legitimation, och
- kontrollmaterial, dvs. spärrlistor, eller uppgifter som härrör från OCSP-rutiner.[33]

En myndighet kan givetvis i kontrollsyfte inhämta ytterligare handlingar från den som har utfärdat legitimationen. Om så sker blir handlingarna allmänna och skall medtas i bedömningen. Även övriga handlingar som kommer in till myndigheten eller upprättas där med anknytning till handläggningsprocessen skall medtas. Det gäller oberoende av medium och kommunikationskanal.

8.2 VILKA FÖRUTSÄTTNINGAR FINNS FÖR GALLRING

8.2 1 Den elektroniskt underskrivna handlingen

Den elektroniskt underskrivna handlingen har som framgått flera beståndsdelar. Samtliga delar behövs för att mottagaren skall kunna ta del av texten, kontrollera att uppgiften om utställare är riktig och att texten inte har förvanskats efter det att handlingen undertecknades. Det har också konstaterats att de beskrivna delarna tillsammans utgör en handling, i enlighet med 2 kap. 3 § TF.

Myndigheternas allmänna handlingar skall som huvudregel bevaras i ursprungligt skick. Som gallring räknas inte bara förstöring av allmänna handlingar utan även avlägsnande av delar av allmänna handlingar. Även andra åtgärder som medför informationsförlust utgör gallring, t.ex. att förstöra handlingar efter skanning, eller att konvertera elektroniskt underskrivna handlingar så att underskriftens funktion försämras eller går förlorad.[34] I båda fall medför åtgärderna att möjligheterna att bedöma handlingarnas autenticitet försämras.[35] Sådan gallring medges endast om

33 Som tidigare nämnts avses med ”text” (första punkten) all slags information som kan förses med elektronisk underskrift, exempelvis även bilder.

34 Se avsnitt 2.5.3 om gallring.

35 Möjligheterna att bedöma autenticiteten försämras även om operatören övervakar och dokumenterar överföringen, i enlighet med Riksarkivets bestämmelser.

informationsförlusten vägs upp av betydande vinster, t.ex. med avseende på effektivisering av handläggningsprocessen eller förbättrad tillgänglighet till handlingarna. Att avlägsna delar av en elektroniskt underskriven handling ger obetydliga vinster.

Det kan sammanfattningsvis konstateras att det i praktiken föreligger två alternativ när det gäller bevarande och gallring av de elektroniskt underskrivna handlingarna. Antingen bevaras handlingarna i sin helhet, i ursprungligt skick, eller så gallras de efter det att relevanta uppgifter har överförts till verksamhetssystemet. För gallring av elektroniskt underskrivna handlingar krävs en utredning i varje enskilt fall där hänsyn tas till samtliga handlingar inom e-tjänsten och den handläggningsprocess som denna stödjer.

8.2.2 Kontrollmaterialet

En del av de uppgifter som behövs för kontroll av en elektroniskt underskriven handling utgör delar av handlingen själv, medan andra ingår i det kontrollmaterial som kommer in till eller upprättas hos myndigheten. Vid ett bevarande av den inkomna handlingen i ursprungligt skick kan man även fortsättningsvis kontrollera om handlingen är förvanskad. För kontroll av uppgiften om utställare är det däremot nödvändigt att ha tillgång till spärrlistor eller motsvarande. Behovet av att bevara kontrollmaterialet för att kunna upprepa den initiala kontrollen är till stor del beroende av om den har utförts noggrant och korrekt, och om utfallet av kontrollen har dokumenterats på ett tillfredställande sätt.

8.2.3 En diskussion om bevarandenivåer

När frågan om bevarande och gallring behandlades inom SAMSET gjordes en bedömning av vilka möjligheter till äkthetskontroll som föreligger vid olika bevarandenivåer. Ett exempel konstruerades där omkontroller företas efter ett antal år, hos ett tänkt Statens e-Kriminaltekniska Laboratorium (SeKL). Där medtogs även handlingar som kan, men inte behöver, finnas hos myndigheten. Exemplet har bifogats rapporten för att illustrera en del av de diskussioner som fördes i SAMSET:s juristgrupp; se bilaga 1.

8.2.4 Förutsättningar för gallring

Det har tidigare konstaterats att arkivförfattningarna inte reglerar vilka handlingar som skall inhämtas från andra aktörer för att säkerställa möjligheterna till kontroll. Det är oklart vilka rättsliga och andra krav som i framtiden kommer att ställas på inhämtande av kontrollmaterial och eventuell upprepning av den initiala kontrollen. Det går inte heller att förutsäga i vilka sammanhang elektroniska underskrifter kommer att användas.

Även om förutsättningarna för gallring delvis är desamma för flera av de myndigheter som har infört e-tjänster, så saknas tillräckligt underlag för att besluta generella gallringsföreskrifter. Underlag för diskussionerna inom SAMSET och för denna rapport har varit masshanteringen av elektroniskt underskrivna handlingar hos ett antal större myndigheter. Det är för närvarande inte möjligt att bedöma om resonemangen är tillämpliga i andra sammanhang.

Så länge som det är oklart i vilka sammanhang elektroniska underskrifter kommer att användas och vilka handlingar som faktiskt kommer att finnas hos myndigheterna, bedöms gallringsfrågan i varje enskilt fall. Eventuell gallring regleras tillsvidare i myndighetsspecifika föreskrifter.

9 SLUTORD

Arkivfrågorna har i praktiken ofta skjutits på framtiden, trots att de tekniska och administrativa lösningarna för att hantera elektroniskt underskrivna handlingar blir avgörande för möjligheterna att tillgodose arkivlagens bevarandemål.

I traditionell miljö kan avvägningar mellan olika intressen göras allt eftersom frågorna aktualiseras. I IT-miljö måste ett antal frågor lösas redan i utvecklingsskedet. Det gäller bl.a. den elektroniskt underskrivna handlingens format. Beslut som fattas i ett tidigt skede kan bli avgörande för möjligheten att på sikt kontrollera handlingarnas äkthet och ursprungliga skick och att gallra delar av materialet.

BILAGA 1 – BEVARANDENIVÅER

Sparat material	SeKL:s utlåtande
1. Endast själva ”texten”	1. Då någon ursprunglig handling ej hittats kan SeKL inte uttala sig om till vilken medborgare den aktuella ”texten” är eller har varit kopplad till.
2. ”Texten” samt hashvärde och krypterat hashvärde	2. Fragment av den inkomna handlingen har hittats och hashvärdet och texten matchar varför SeKL bedömer att ingen förvanskning har skett[36]. Värdet av detta är dock högst tvivelaktigt då SeKL *inte* kan koppla detta fragment till någon specifik undertecknare.
3. ”Texten” samt e-legitimationen	3. Fragment av den inkomna handlingen har hittats. En e-legitimation utställd till medborgare X finns bland fragmenten men SeKL kan *inte* på något sätt koppla texten till denne medborgare. Den e-legitimation som hittats *tycks* vara utgiven av Bank Y men det finns inga bevis för att det verkligen är så.
4. Hela den inkomna handlingen	4. Den inkomna handlingen *tycks* vara utställd av medborgare X och är oförvanskad men SeKL kan inte uttala sig om handlingens äkthet. Den e-legitimationen som handlingen undertecknats med *skulle kunna* vara utgiven av banken Y men det kan vara en falsk bank.
5. Hela den inkomna handlingen samt det korresponderande rotcertifikatet	5. Den inkomna handlingen *tycks* vara utställd av medborgare X och är oförvanskad men SeKL kan inte uttala sig om handlingens äkthet. Den e-legitimation som handlingen undertecknats med *skulle kunna* vara utgiven av banken Y men det kan vara en falsk bank, då rotcertifikatets äkthet inte kan bevisas.
6. Hela den inkomna handlingen samt a) det korresponderande rotcertifikatet b) den vid tiden gällande spärrlistan, eller c) realtidsspärrfrågan och svaret d) Policydokument	6. SeKL håller det för *sannolikt* att den inkomna handlingen är undertecknad av medborgare X. Handlingen är oförvanskad. E-legitimationen *skulle kunna* vara utgiven av banken Y men det kan vara en falsk bank. E-legitimationen var giltig vid tiden för undertecknandet. Denna äkthetsbedömning gäller dock under förutsättning att utgivningen av e-legitimationen skett i enlighet med policyn och att medborgare X sett till att e-legitimationens hemliga del inte har kommit i orätta händer.
7. Hela den inkomna handlingen samt a) det korresponderande rotcertifikatet b) den vid tiden gällande spärrlistan, eller c) realtidsspärrfrågan och svaret d) Policydokument e) Material från bank Y:s ID-tjänst, certifikat, loggar m.m.	7. SeKL håller det för *ytterst sannolikt* att den inkomna handlingen är undertecknad av medborgare X. - Handlingen är oförvanskad - E-legitimationen var giltig vid undertecknandet - E-legitimationen är utgiven av bank Y - Utfärdandet har gått korrekt till Denna äkthetsbedömning gäller dock under förutsättning att medborgare X sett till att e-legitimationens hemliga del inte har kommit i orätta händer.

36 Detta förutsätter dock att myndigheten vet vilken hashalgoritm som har använts och har tillgång till den.

RAPPORTER

I denna rapport behandlas frågor som är av betydelse för bevarande och gallring av elektroniskt underskrivna handlingar och andra handlingar som kommer in till eller upprättas inom ramen för myndigheternas e-tjänster. Rapporten har tagits fram av Riksarkivet i samverkan med SAMSET-projektets juristgrupp som är ett forum för samverkan mellan myndigheter som har kommit långt i arbetet med att införa e-tjänster och som har ställts inför dessa frågor.

RIKSARKIVET
Box 12541, 102 29 Stockholm
Telefon 08 - 737 63 50

Fritzes
ett Wolters Kluwer-företag

106 47 Stockholm Tel 08-690 91 90 Fax 08-690 91 91 order.fritzes@nj.se www.fritzes.se

ISBN 91-38-32325-7 ISSN 1402-9685
ISBN 978-91-38-32325-0