Juridisk vägledning för införande av

e-legitimering och e-underskrifter

eSam

INNEHÅLL

Vägledningen är framtagen av eSam i samarbete med E-legitimationsnämnden och Myndigheten för samhällsskydd och beredskap

SAMMANFATTNING

E-legitimering och e-underskrift är komplexa funktioner som behöver omhändertas från såväl juridiska som tekniska och administrativa utgångspunkter. Vägledningen förklarar

- hur dessa funktioner är uppbyggda,
- vilka rättsregler som aktualiseras och
- vilka säkerhetsåtgärder som behöver vidtas.

Vägledningen ger stöd i arbetet med informationssäkerhet och innehåller juridiskt anpassade beskrivningar för att

a) *använda* elektroniska
   - identitetshandlingar (e-legitimationer), och
   - intyg om vem som legitimerat sig (identitetsintyg),

b) identifiera den som har legitimerat sig,

c) ställa ut elektroniska urkunder,
   - elektroniskt underskrivna (e-underskrivna) av en fysisk person, eller
   - elektroniskt stämplade (e-stämplade) av en organisation,

d) kontrollera om en e-urkund är äkta, och

e) bevara och gallra e-urkunder och handlingar för att styrka sådana handlingars ursprungliga skick och äkthet.

Kapitel 1 beskriver syfte och målgrupp.

Allt fler organisationer står i begrepp att eller har redan börjat erbjuda tjänster som bygger på e-legitimering och e-underskrifter. Genom att skapa en samsyn bland samhällets aktörer, särskilt inom offentlig sektor, om funktion, juridik och säkerhet för e-legitimering och e-underskrifter uppnås flera syften. Kravställningen förenklas och harmoniseras vilket ger leverantörer möjlighet att erbjuda standardiserade tjänster av hög kvalitet. Funktionerna för att legitimera sig och skriva under ser likadana ut från tjänst till tjänst vilket underlättar för användarna att förstå hur de ska hanteras. Säkerhetsbehoven blir också analyserade och beaktade på ett enhetligt sätt vilket förenklar för organisationerna att erbjuda robusta och säkra tjänster. En sådan samordning är avgörande för att användarna ska känna förtroende för och vilja använda de erbjudna tjänsterna.

Sammantaget är denna samsyn en förutsättning för att effektivt kunna bygga vidare på de möjligheter som digitaliseringen erbjuder.

Vägledning ska kunna användas på tre sätt:

dels som stöd för den som behöver en övergripande bild av de rättsfrågor och säkerhetsfrågor som uppkommer vid e-legitimering och e-underskrift,
dels som en praktisk handledning där konkreta råd ges om införande och utformning,
dels som en informationskälla om dessa frågor och var ytterligare information finns.

Vägledningen är i centrala delar främst skriven för myndigheternas jurister. Den kan emellertid också användas av andra som arbetar med eller annars berörs av frågor om elektronisk legitimering och elektronisk underskrift.

Kapitel 2 handlar om att inför e-legitimering i verksamheten.

En organisation som ska införa e-legitimering och e-underskrift i sin verksamhet behöver vara förberedd för att kunna hantera dessa funktioner och att göra en korrekt kravställning och upphandling av tjänsterna. Under drift måste säkerhetsnivån bibehållas. Informationen behöver också hanteras på ett korrekt sätt över tid, även efter att systemen avvecklats.

Kapitel 3 beskriver hur hanteringen av e-legitimering och e-underskrift har förändrats över tid.

Kapitel 4 beskriver e-legitimering.

Beskrivningen är inriktad på vilken information som hanteras och innebörden av åtgärderna. I detta ingår även att tydliggöra vad den som erbjuder en e-tjänst (förlitande part), användaren, leverantören av identitetsintyg och eventuella underleverantörer, vidtar för åtgärder i de olika stegen. Även hanteringen av utländska e-legitimationer berörs. Kapitlet vänder sig i första hand till de som behöver fördjupa sig i bakomliggande procedurer för att kunna förstå de tekniska och juridiska förutsättningarna och utforma dem så att avsedda rättsverkningar uppkommer när e-legitimationer används och att ansvar kan inträda för den som missbrukar dessa funktioner.

Kapitel 5 beskriver e-underskrifter.

E-underskrifter används bland annat för att en identifierad användare på ett juridiskt bindande sätt ska kunna utföra rättshandlingar inom ramen för en e-tjänst. Kapitlet inleds med en beskrivning av den juridiska funktionen hos en e-underskrift. Därefter följer en redogörelse från ett juridiskt perspektiv för de olika stegen vid e-underskrift. Där tydliggörs också vad olika parter vidtar för åtgärder i olika steg. Även hanteringen av utländska e-underskrifter berörs. Kapitlet vänder sig även här i första hand till de som behöver fördjupa sig i de bakomliggande procedurerna för att kunna förstå de tekniska och juridiska förutsättningarna och utforma dem så att avsedda rättsverkningar uppkommer när e-legitimationer används för underskrift.

Även hanteringen av utländska e-underskrifter berörs

Kapitel 6 berör formkrav förknippade med underskrifter.

När en organisation överväger att börja använda e-underskrifter i sina e-tjänster är det av vikt att veta vilka formkrav som finns kopplade till olika förfaranden. Vissa formkrav hindrar att e-underskrifter används medan andra formkrav tillåter det. I kapitlet tydliggörs vilka regler som finns och när e-underskrifter får användas.

Kapitel 7 beskriver parter, roller och civilrättsligt ansvar.

Användningen av e-legitimationer och e-underskrifter regleras i en rad olika avtal mellan olika aktörer. Det är viktigt att avtalen utformas korrekt så att det civilrättsliga ansvaret fördelas på ett balanserat sätt mellan berörda aktörer. Kapitlet beskriver vilka aktörerna är, de olika typer av avtal som behövs på området och vad de kan behöva innehålla, de frågor om ansvar som aktualiseras och de risker som respektive aktör kan behöva beakta.

Kapitlet ger stöd både åt organisationer som står i begrepp att utforma och teckna avtal på området och åt organisationer som redan ingått avtal och behöver kontrollera utformningen av dem. En skillnad som blir av betydelse från avtalssynpunkt är den som beskrivs mellan direkt och indirekt legitimering respektive direkt och indirekt underskrift.

Kapitel 8 beskriver det straffrättsliga ansvaret vid användning av e-legitimationer.

Samhället ger straffrättsligt skydd när e-legitimering och e-underskrifter används. Kapitlet beskriver vissa manipulationer med och missbruk av e-legitimationer som börjat förekomma, vilka bestämmelser om straffansvar som kan bli tillämpliga och vad en myndighet kan behöva vidta för åtgärder när missbruk uppdagas.

Kapitel 9 handlar om hur informationen säkras.

Förtroendet för att en e-tjänst där e-legitimering och e-underskrift används är säker blir av central betydelse för att tjänsten ska nyttjas i önskad utsträckning. Detta förtroende bygger i grunden på att obehöriga inte får tillgång till informationen, informationen inte ändras på ett obehörigt sätt, tjänsten är tillgänglig för användaren, och att det är spårbart vem som har gjort vad och när. För att kunna uppfylla dessa krav behövs ett systematiskt informationssäkerhetsarbete så att det inte uppstår luckor som kan nyttjas för missbruk och manipulationer.

I detta kapitel beskrivs hur ett sådant arbete kan bedrivas med stöd av ett Ledningssystem för informationssäkerhet (LIS).

Kapitel 10 handlar om bevarande och gallring.

I kapitlet beskrivs de frågor om bevarande och gallring som aktualiseras när e-legitimering och e-underskrift används. I samband med att e-tjänster införs, används, förändras och avvecklas, behöver det bedömas vilken information om e-legitimationer och e-underskrifter som ska bevaras och vilken information som får tas bort från systemen. Frågan är av såväl juridisk som säkerhetsmässig betydelse.

En organisations behov av att spara valideringsdata behöver analyseras av organisationen. Denna reglering gäller visserligen för myndigheter men bakomliggande överväganden är av intresse också för andra organisationer.

Kapitel 11 berör skyddet för enskildas personliga integritet.

E-legitimationer och e-underskrifter bygger på behandling av personuppgifter. För organisationer är det viktigt att säkerställa att behandlingen inte bara utförs i enlighet med gällande regelverk utan även tar höjd för den reglering som införs när Dataskyddsförordningen träder ikraft år 2018.

I detta kapitel redovisas översiktligt de frågor om persondataskydd som aktualiseras inom ramen för e-legitimationssystemet och hur dessa frågor bör hanteras.

Kapitel 12 handlar om EU:s förordning om gränsöverskridande elektronisk legitimering (eIDAS)

I kapitlet redogörs för EU:s förordning om gränsöverskridande elektronisk legitimering (eIdas-förordningen) och hur kraven på ömsesidigt erkännande av anmälda e-legitimationer från och med den 29 september 2018 påverkar myndigheterna.

Kapitel 13 innehåller praktiska råd och rekommendationer om införandet.

I kapitlet ges råd och rekommendationer för att samordna och underlätta införandet av e-legitimationer och e-underskrifter.

Kapitlet är indelat i tre delar med checklistor som stöd för

- införande av e-legitimering,
- införande av e-underskrifter, och
- hantering av bevarande och gallring.

I råden och rekommendationerna har såväl de juridiska som de säkerhetsmässiga perspektiven beaktats. Grunden för råden och rekommendationerna presenteras i vägledningens tidigare kapitel. Checklistorna kan användas både av den som står i begrepp att införa e-legitimationer och e-underskrifter och den som vill kontrollera att de redan införda tjänsterna har utformats på ett korrekt och säkert sätt.

INLEDNING

Digitaliseringen av det offentliga Sverige går snabbt och ska fördelarna med den tekniska utvecklingen kunna tas tillvara krävs tillgång till ett antal grundfunktioner. En viktig sådan är möjligheten att på ett säkert sätt kunna identifiera användare av e-tjänster och att kunna kontrollera att elektroniskt underskrivna handlingar är äkta. E-legitimering och e-underskrift är därför en nödvändig del av den grundläggande infrastrukturen för såväl e-förvaltningen som för kommersiella aktörer.

Förtroendet för de funktioner som används vid e-legitimering och e-underskrift förutsätter en stabil och säker teknisk lösning, rättssäkra avtalslösningar och att det är möjligt att med bland annat straffrättsliga medel motverka missbruk. Det finns också ett behov av att göra användningen av begrepp och beskrivningar inom området enhetlig för att berörda aktörer ska kunna bygga en gemensam plattform för utveckling och användning av e-legitimering, e-underskrift och e-tjänster.

Utmaningarna är dock flera och det behöver inledningsvis betonas att det handlar om tjänster och funktioner som är såväl tekniskt som juridiskt komplexa. Detta ställer höga krav på beställarkompetens hos myndigheter och andra organisationer för att införa säkra, robusta och juridiskt anpassade e-legitimerings- och e-underskriftslösningar. Användningen av e-legitimering och e-underskrift har ökat successivt genom att myndigheter i allt större utsträckning kommit att lägga ut funktioner på underleverantörer för identifiering av användare som

legitimerat sig och för kontroll av om e-underskrivna handlingar är äkta.[1] Någon samordning för att bibehålla ett enhetligt e-legitimationssystem har dock inte ägt rum. Den stegvisa utvecklingen har istället fört med sig att olika begrepp och beskrivningar används och att nya avtal tecknas med olika strukturer, ansvarsförhållanden och krav. Inte sällan har upphandlingar av e-legitimerings- och e-underskriftsfunktioner resulterat i funktioner som inte varit helt transparenta och i att avtal tecknats som inte varit heltäckande, vilket försvårat bedömningen av säkerheten för informationen och fördelningen av ansvar.

Samtidigt har förfaranden börjat förekomma där e-legitimationer och andra intyg missbrukas i strid mot den straffrättsliga regleringen[2], på ett sätt som inte heller kan förenas med reglerna om persondataskydd. Här behöver säkerställas att e-legitimationer och e-tjänster inte tillåts bli ett laglöst land. Jurister och verksamhetsansvariga vid berörda myndigheter behöver därför kunna förstå hur hanteringen går till och samordna sina insatser mot alla former av missbruk av e-legitimations- och underskriftssystem.

Jurister och verksamhetsansvariga behöver därför kunna förstå hur hanteringen går till

För att förtroendet ska kunna upprätthållas för e-tjänster där e-legitimering och e-underskrifter behövs krävs dessutom ett systematiskt informationssäkerhetsarbete. Brister avseende tillgänglighet, riktighet och konfidentialitet kan få allvarliga konsekvenser och även nyttjas vid missbruk. Det blir därför viktigt för jurister och verksamhetsansvariga att tillsammans med informationssäkerhetsansvariga bygga upp en gemensam förståelse för informationssäkerhetsarbetet som en grundläggande förutsättning för att kunna erbjuda olika typer av e-tjänster.

Efter en inledning med en allmän beskrivning av utgångspunkter och bakgrund ges den egentliga vägledningen i kapitel 4-12. Därefter beskrivs vad myndigheter och andra organisationer kan behöva göra för att etablera en rättsligt och informationssäkerhetsmässigt fungerande hantering av e-legitimering och e-underskrifter.

[1] Se vidare avsnitt 3.
[2] Enligt ett beslut av Åklagarmyndigheten skulle det inte vara brottsligt att utge sig för att vara någon annan efter en legitimering på internet (Åklagarkammarens ärende AM-61001-16).

1. SYFTE OCH MÅLGRUPP

1.1. Vägledningens syfte

1.1.1. Att övergripande underlätta förståelse och samsyn

E-legitimering och e-underskrift är komplexa funktioner där flera aspekter behöver omhändertas. Vägledningen har till syfte att förklara

- hur dessa funktioner är uppbyggda,
- vilka rättsregler som aktualiseras och
- vilka säkerhetsåtgärder som behöver vidtas.

Allt fler organisationer står i begrepp att eller har redan börjat erbjuda tjänster med behov av elektronisk identifiering och underskrift. Genom att skapa en samsyn bland samhällets aktörer, särskilt inom offentlig sektor, rörande funktion, juridik och säkerhet för e-legitimering och e-underskrifter uppnås flera syften. Kravställningen förenklas och harmoniseras vilket ger leverantörer möjlighet att erbjuda samordnade tjänster av hög kvalitet. Funktionerna för att legitimera sig och skriva under ser likadana ut från tjänst till tjänst vilket underlättar för användarna att förstå hur de ska hanteras. Säkerhetsbehoven blir också analyserade och beaktade på ett enhetligt sätt vilket förenklar för organisationerna att erbjuda robusta och säkra tjänster. En sådan samordning är avgörande för att användarna ska känna förtroende för och vilja använda de erbjudna tjänsterna.

Sammantaget är denna samsyn en förutsättning för att effektivt kunna bygga vidare på de möjligheter som digitaliseringen erbjuder.

1.1.2 Att underlätta införande

Införandet av tjänster som nyttjar e-legitimering och e-underskrifter får följdverkningar inom olika delar av en organisation och flera olika yrkeskategorier måste vara involverade i arbetet. Vägledningen syftar till att förenkla detta arbete och utgöra ett stöd för organisationen i varje steg i processen. Här behandlas förberedelser, kravställning, upphandling, införande, förvaltning, drift och avveckling.

Vägledningen vänder sig huvudsakligen till de organisationer som har infört eller ska införa den här typen av tjänster. De organisationer som redan har infört tjänster som nyttjar e-legitimering och e-underskrift kan ha nytta av vägledningen för att ytterligare utveckla och skydda sina tjänster. Den kan även användas som en kontroll av att den rättsliga och säkerhetsmässiga plattformen för tjänsten har utformats på ett ändamålsenligt sätt.

1.1.3 Att underlätta hantering av e-underskrivna handlingar över tid

E-legitimationer, identitetsintyg och e-underskrifter ska inte bara vara äkta vid det tillfälle då de skapas, kontrolleras och inledningsvis används. Det kan också, i särskilda fall, finnas ett behov av att i efterhand kunna gå tillbaka och verifiera vem som har gjort vad och om en e-underskriven handling fortfarande är äkta. Vidare behöver det klargöras vad som ska bevaras och gallras när e-underskrivna

handlingar ska tillgodose en organisations behov över tid. Säkerställs inte hela processen genom lämpliga val av skyddsmetoder, format, metadata och valideringsdata kan information som behövs för validering i efterhand ha gått förlorad. I andra fall kan ett kostsamt bevarande ske i onödan. Vägledningen kan underlätta organisationens arbete också inom detta område.

1.1.4 Att fördjupa den juridiska förståelsen

Från juridiska utgångspunkter finns även ett behov av samordning när det ska bedömas vem det är som tillhandahåller en viss funktion, vilka avtal eller föreskrifter som gäller mellan parterna, vilket civilrättsligt och straffrättsligt ansvar som kommer i fråga vid ett missbruk samt vilka handlingar som bör åberopas när någon behöver styrka sin rätt; är det en e-legitimation, ett identitetsintyg eller någon annan elektronisk handling, med eller utan urkundskvalitet? Dessa frågor ställs som, framgått på sin spets, inte bara på grund av nya funktioner utan också som en följd av ökad kriminalitet genom id-kapningar och liknande i ett alltmer digitaliserat samhälle. De grundläggande funktioner som införts för att upprätthålla förtroendet för en digitaliserad förvaltning måste värnas. Sådana samhällsbärande funktioner som e-legitimations- och underskriftssystemet får inte uppfattas som laglöst område där oseriösa aktörer kan bereda sig åtkomst till sekretessbelagda uppgifter eller förfalska och missbruka handlingar.

Därför behöver de system som numera används för legitimering och underskrift beskrivas på ett enhetligt sätt, med utgångspunkt i tydliga begrepp och beskrivningar som är baserade på allmänt vedertagna juridiska gränser.

1.1.5 Att säkerställa informationssäkerheten

Användarnas förtroende för de tjänster som erbjuds är av avgörande betydelse för att de ska få önskat genomslag. På senare tid har dock flera brister och möjligheter till missbruk uppmärksammats.

Även om en ny tjänst har en hög potential att skapa ökad effektivitet och att underlätta för såväl användare som den organisation som erbjuder tjänsten, kan bristande säkerhet och därpå följande förtroendebrister påtagligt påverka hur mycket tjänsten används eftersom frågan om förtroende och därmed informationssäkerheten är av stor betydelse för användarna av tjänsten. De förutsätter att personuppgifter inte hanteras på ett felaktigt sätt, att obehöriga inte kan ta del av inlämnade uppgifter och framförallt att andra inte kan missbruka en persons e-legitimation eller e-underskrift så att innehavaren lider skada. En annan aspekt, lika viktigt för organisationen som för användaren, är att e-legitimationen och e-underskriften är utformad på ett sådant sätt att det med tillräckligt hög säkerhet går att identifiera den som ska använda exempelvis en e-tjänst.

Hög potential att skapa ökad effektivitet

Säkerhetsaspekterna är också en angelägenhet för samhället i stort. Regeringen har vid flera tillfällen uttalat sitt stöd för en ökad digitalisering av offentlig sektor. Byggs en sådan digitalisering på en osäker identifiering finns det emellertid risk att satsningen inte ger önskat resultat. Därför behöver säkerheten byggas in från början.

1.2 Målgrupp

Denna vägledning vänder sig i första hand till offentlig sektor. Den kan användas såväl internt för att till exempel införa e-underskrift av myndighetens beslut som externt för att göra det möjligt för enskilda och befattningshavare inom det allmänna att legitimera sig och skriva under handlingar i sina kontakter med myndigheter.

Även andra organisationer som överväger att börja använda e-legitimationer och e-underskrifter och organisationer som redan har sådana tjänster kan använda vägledningen som stöd vid uppföljning och utvärdering av tjänster, med avseende på till exempel avtal, säkerhet, persondataskydd, gallring och straffrättsligt skydd. Den kan även användas vid misstänkt missbruk av e-legitimationer eller e-underskrifter. Mycket i vägledningen är dessutom giltigt för såväl privata som offentliga organisationer. Några delar gäller dock främst offentliga aktörer, till exempel reglerna om gallring.

En organisation som erbjuder användare att använda e-legitimation och e-underskrift kallas i vägledningen ”förlitande part” eftersom organisationen förlitar sig på att kedjan mellan utfärdare, användare och eventuell intygsutställare är korrekt.

Ett framgångsrikt införande av funktioner för e-legitimering och e-underskrift förutsätter inte bara ett nära samarbete mellan organisationens jurister, och informationssäkerhetsansvariga utan även mellan verksamhetsutvecklare, it-arkitekter, arkivarier, kommunikatörer och upphandlare med flera som är involverade i att ta fram en lösning. Alla dessa yrkeskategorier är därför i någon mån målgrupp för denna vägledning och vägledningen är tänkt att underlätta samarbetet dem emellan. Vissa delar i vägledningen är dock skrivna främst med jurister i åtanke.

1.3 Omfattning och avgränsning

En rad olika frågor aktualiseras i samband med e-legitimering och e-underskrift. Denna vägledning tar emellertid sikte på frågor som är av direkt betydelse för de myndigheter och andra organisationer som

- står i begrepp att införa e-legitimationer och e-underskrifter, eller
- redan tillhandahåller den möjligheten men behöver kontrollera hur lösningen förhåller sig avtalsmässigt och säkerhetsmässigt till de krav som måste ställas.

Vägledningen ger stöd i arbetet med informationssäkerhet och innehåller juridiskt anpassade beskrivningar för att

a) *använda* elektroniska
   – identitetshandlingar (e-legitimationer), och
   – intyg om vem som legitimerat sig (identitetsintyg),
b) *identifiera* den som har legitimerat sig,
c) *ställa ut* elektroniska urkunder (e-urkunder; se 8.1),
   – elektroniskt underskrivna (e-underskrivna) av en fysisk person, eller
   – elektroniskt stämplade (e-stämplade) av en organisation,
d) *kontrollera* om en e-urkund är äkta, och

e) *bevara och gallra* e-urkunder och handlingar för att styrka sådana handlingars ursprungliga skick och äkthet. Vägledningen tar inte upp frågor om juridisk behörighetskontroll, i tekniska sammanhang ofta kallat auktorisation.

Vägledningen ger inte ensamt stöd för att avgöra om det för en viss tjänst är lämpligt eller tillräckligt säkert att använda e-legitimationer eller e-underskrift. För att kunna fatta ett sådant beslut behöver respektive organisation först ha genomfört en riskanalys (se 2.1.2).

1.4 Hur ska vägledningen användas

Målet är att denna vägledning ska kunna användas på tre sätt:

dels som stöd för den som behöver en övergripande bild av de rättsliga och säkerhetsrelaterade frågor som aktualiseras vid införande och användning av e-legitimering och e-underskrifter,

dels som en praktisk handledning där konkreta råd ges om införande och utformning,

dels som informationskälla för var ytterligare information om dessa frågor kan hämtas och om innebörden i olika begrepp.

Vägledningen är i delar främst är skriven för jurister. Den innehåller emellertid även en genomgång och en inkludering av tekniska rutiner och tekniska förutsättningar. Detsamma gäller informationssäkerhet. Utan en genomgång av dessa områden skulle vägledningen inte kunna tas fram. Arbetet med att införa e-legitimationer och e-underskrifter förutsätter att olika yrkesgrupper involveras och samarbetar. Därför rekommenderas att organisationen sätter samman en grupp för att genomföra det aktuella arbetet där alla berörda discipliner finns representerade.

I de flesta arbeten av denna typ uppstår frågor som kan vara svåra att besvara. Att delta i ett nätverk för att kunna utbyta erfarenheter och kunskap kring e-legitimering och e-underskrift är därför av vikt. Ett komplement till vägledningen kan vara att delta i något nätverk eller samverkansprojekt för e-legitimering och e-underskrift. Det finns även andra nätverk som kan vara till stor hjälp, exempelvis finns en rad nätverk på informationssäkerhetsområdet för både offentlig och privat sektor samt nätverk med koppling till e-förvaltning.[3]

1.5 Medverkande

Arbetet med att ta fram vägledningen har genomförts av eSams rättsliga expertgrupp. Ledamöter i expertgruppen är *Johan Bålman, Per Furberg, Sven Granlund, Gustaf Johnssén, Sara Markstedt, Jan Sjösten, Gunnar Svensson, Mikael Westberg, Staffan Wikell, Tomas Öhrn och Christina Wikström*. Adjungerade ledamöter i expertgruppen är *Maria Sertcanli och Nils Fjelkegård*. I arbetet har även eSams rättsliga referensgrupp deltagit.

Myndigheten för samhällsskydd och beredskap, Verksamheten för cybersäkerhet och skydd av samhällsviktig verksamhet, har bidragit aktivt med texter och annat stöd gällande vägledningens utformning, upplägg och säkerhetsfrågor. Från MSB har *Helena Andersson, Carl Önne och Anders Östgaard* deltagit.

Arbetet har bedrivits i nära samarbete med E-legitimationsnämnden. Från nämnden har *Oskar Öhrström och Eva Sartorius* deltagit.

[3] Kontakta eSam för ytterligare information om tillgängliga nätverk med koppling till e-förvaltning. Bland annat E-legitimationsnämnden, MSB och eSam tillhandahåller olika nätverk.

2. ATT INFÖRA E-LEGITIMERING I VERKSAMHETEN

En organisation som ska införa e-legitimering och e-underskrift i sin verksamhet behöver vara förberedd för att kunna hantera en infrastruktur för detta och göra en korrekt kravställning och upphandling av tjänsterna. Under drift måste säkerhetsnivån bibehållas. Informationen behöver också hanteras på korrekt sätt över tid, även efter att systemen avvecklats. Detta kapitel beskriver de olika stegen i processen för att införa e-legitimering och e-underskrift och hur hanteringen förändrats över tid. Beskrivningen riktar sig främst till dem som ska förbereda för, och införa, sådana tjänster.

2.1 Förberedelser

Under en förberedande fas när en organisation planerar att införa e-legitimering och e-underskrift, vanligtvis i sin externa kommunikation, till exempel i e-tjänster, aktualiseras ett antal frågor som beskrivs i detta avsnitt.

2.1.1 Omfattning

Att e-legitimationer och e-underskrifter ska införas och användas inom en organisation, kan vara ett resultat av en kravställning av en viss e-tjänst som ska erbjudas för en kategori av användare. Det blir viktigt att göra ett gediget förarbete så att tjänsten inte riskerar att bli udda inom organisationen eller får brister så att den inte kan användas inom andra områden.

Även om det ofta är samma typ av e-legitimation en användare brukar för e-legitimering och e-underskrift (till exempel BankID eller Telia e-legitimation), skiljer sig hanteringen för e-identifiering från den vid e-underskrift. Under förberedelsefasen behöver frågan om vilken tjänst, e-legitimering eller e-underskrift, som ska användas besvaras. Stöd för detta beslut ges i kapitel 6, se även kapitel 4 och 5. Båda tjänsterna kan införas, samtidigt eller vid olika tidpunkter, se vidare kapitel 13.

En organisation kan ha egna e-legitimationer utgivna till sina anställda.[4] Organisationen behöver därför ta ställning till om dessa e-legitimationer bör få användas för e-legitimering och e-underskrift utanför den egna organisationen.

2.1.2 Riskanalys

För att få ett underlag för arbetet med arkitektur, infrastruktur och säkerhetsåtgärder behöver riskerna analyseras. Som exempel på hot mot systemet kan nämnas att

- utfärdare upphör med sina tjänster,
- leverantör av identitetsintyg drabbas av ett intrång,
- den egna organisationens underlag för spårbarhet skadas,

[4] Som exempel kan nämnas Försäkringskassan som förser anställda med e-legitimation.

- någon del i den kedja av tjänster som används upphör att fungera, till exempel att en aktör blir utsatt för en överbelastningsattack.

En riskanalys går ut på att besvara ”vad kan hända”, ”hur sannolikt är det” och ”vilka blir konsekvenserna”. I en analysfas handlar det om att förfina beskrivningar av riskscenarier och att bedöma hur troligt det är att de inträffar. Därefter bedöms konsekvenserna och värderas utifrån alternativa metoder för att möta dem. Det kan göras genom att

- acceptera – låta risken finnas kvar och godta att den inte hanteras,
- minimera – minska risken genom att till exempel införa skyddsåtgärder,
- transferera – låta risken föras över på en annan aktör,
- undvika – avgöra om en annan lösning för med sig att risken inte ens uppstår.

För att prioritering och val av metod och säkerhetsåtgärd ska kunna ske görs en informationsklassificering utifrån behovet av konfidentialitet, riktighet, tillgänglighet och, för de organisationer som så anser, spårbarhet. I ett sådant ledningssystem för informationssäkerhet som beskrivs i kapitel 9 ingår informationsklassificering och riskanalys som en del i processen.

Ett av resultaten från riskanalysen är också ett val av tillitsnivå för inloggning i en tjänst.[5]

2.1.3 Kravställning

Kraven vid införande av e-legitimering och e-underskrifter ska ställas utifrån dels de juridiska förutsättningar och risker som beskrivs i detta dokument, dels de risker för informationssäkerheten som identifieras vid en riskanalys och den strategi och arkitektur som organisationen arbetar efter. Kravställningen ska ske i förhållande till alla berörda aktörer, bland annat

- utfärdare av e-legitimation,
- leverantör av identitetsintyg,
- leverantör av underskriftstjänst,
- underleverantörer, såsom vid utlokaliserad tjänst eller molntjänst,
- den egna verksamheten (till exempel organisation, verksamhetssystem och e-arkiv).

Utöver detta behöver säkerhetsåtgärder införas för att en e-urkunds äkthet ska kunna kontrolleras över tid och ledas i bevis vid en rättslig prövning (se kapitel 9).

2.1.4 Upphandling

Upphandling av tjänster för e-legitimering och e-underskrift kan ske på olika sätt. E-legitimationsnämnden har regeringens uppdrag att stödja och samordna elektronisk identifiering och underskrift i den offentliga förvaltningens e-tjänster och ska tillhandahålla och administrera system för säker elektronisk identifiering enligt lagen (2013:311) om valfrihetssystem i fråga om tjänster för elektronisk identifiering. Fram till den 31 december 2016 har det varit möjligt att ansluta till E-legitimationsnämndens övergångstjänst, och nämnden arbetar vidare med en mer långsiktig försörjningslösning för offentlig sektor. Utöver den samordning som erbjuds av E-legitimationsnämnden, kan även Kammarkollegiets ramavtal ”Programvaror och tjänster 2014” användas. Det är också möjligt för en myndighet att göra en egen upphandling.

[5] Se vidare www.elegnamnden.se där olika e-legitimationer och tillitsnivåer finns beskrivna.

Oavsett vilken form för upphandling som väljs måste de juridiska kraven och kraven på informationssäkerhet klargöras så att utfärdare, leverantörer, underleverantörer och återförsäljare levererar det som behövs. Som tidigare redovisats är det viktigt att en samsyn finns så att ställda krav kan samordnas och att fördyrande speciallösningar kan undvikas.

2.2 Införande

När tjänster för e-legitimering och e-underskrift införs är det viktigt att tillitskedjan bibehålls på ett dokumenterat sätt. Exempel på detta är att kryptografiska nycklar skapas under kontrollerade och dokumenterade förhållanden och att eventuella utbyten av autentiseringsinformation mellan aktörer utförs på motsvarande säkra vis. Vid integration mellan de olika systemen ska gränssnitten vara definierade och validerade. Eventuella tester ska inte göras i produktionsmiljö utan hanteras i därför avsedda miljöer. Endast godkänd och granskad kod får installeras i produktionsmiljö och behörigheterna bör vara åtskilda mellan utvecklare, testare och driftpersonal.

Viktigt att tillitskedjan bibehålls på ett dokumenterat sätt

Alla dessa krav har räknats upp för att påvisa vikten av att ha kontroll över hela kedjan av inblandade system, informationsflöden och aktörer.

2.3 Förvaltning och drift

Under den period tjänsterna för e-legitimering och e-underskrift är i drift gäller i allt väsentligt samma krav som vid införandet. Vid felsökning och behov av att använda externa resurser måste risker vid fjärråtkomst och behovet av loggar beaktas. Loggarna används för att visa en påstådd händelsekedja. Skadas loggars integritet minskar deras bevisvärde.

Säkerhetskopior ska hanteras på samma säkra sätt som produktionssystemet och återläsning ska kunna ske enligt strikta rutiner.

2.4 Avveckling

När en tjänst för e-legitimering eller e-underskrift avvecklas måste information som behövs över tid för att bevisa äkthet m.m. bevaras på ett säkert sätt. Information som inte behöver sparas över tid (till exempel i ett e-arkiv) ska gallras (se kapitel 10).

3. E-LEGITIMERING OCH E-UNDERSKRIFTER I FÖRÄNDRING

Myndigheternas e-tjänster och användningen av e-legitimering och e-underskrifter tog sin början under 2000-talets första år. Under hand har rutiner, parter m.m. ändrats. Kapitlet beskriver denna förändring fram till nu.

3.1 Samhällets behov

Digitala tjänster ska, så långt det är möjligt och relevant, vara förstahandsval i den offentliga sektorns kontakter med medborgare, organisationer och företag.[6] Med hjälp av innovativa sådana lösningar kan ytterligare effektivitetsvinster uppnås samtidigt som de kan bidra till att stärka förvaltningens öppenhet.[7] E-legitimering och e-underskrifter är fundamentala tjänster för att kunna uppnå en verklig digitalisering, både för den offentliga sektorn men också för näringslivet. Det är betydelsefullt att veta vem som är part vid till exempel en rättshandling eller annars agerar i ett för en enskild eller en myndighet betydelsefullt sammanhang.[8]

3.2 E-legitimering och e-underskrifter i förändring

Myndigheternas e-tjänster[9] och användningen av e-legitimering och e-underskrifter kan utformas på många olika sätt.[10] I samband med att e-legitimationssystemet infördes under 2000-talets första år etablerade myndigheterna därför ett juridiskt synsätt för de funktioner och rutiner som då tillämpades.[11] Det är från dessa utgångspunkter som den juridiska förklaringsmodell som etablerades på 2000-talet ska förstås.

Ett omfattande förändringsarbete har emellertid bedrivits under senare år för att införa ett modernt e-legitimationssystem. I denna vägledning beskrivs hur dessa funktioner numera är utformade och hur de kan förenas med gällande rätt.

3.3 Första versionen av e-legitimationssystemet

Redan när e-legitimationssystemet infördes fanns olika *utfärdare av e-legitimation* som hade till uppgift att ge ut e-legitimationer åt *användare*.[12] De kryptografiska

---

[6] Budgetpropositionen 2015/16:1, utgiftsområde 22, s. 120.

[7] E-delegationen har i sitt slutbetänkande (SOU 2015:66) konstaterat att offentlig sektor behöver mobilisera samverkan kring gemensamma digitala lösningar. Delegationen pekade på att utvecklingen i andra länder i hög grad bygger på gemensamma identifieringslösningar, säker infrastruktur för kommunikation, registerhantering och lagstiftning kopplad till dessa lösningar.

[8] Det kan vara för att bereda åtkomst till en sjukjournal som kan nås via en e-tjänst eller att ett köpeavtal ingås. I det första fallet är det ett krav från lagstiftaren att den som tillhandahåller e-tjänsten endast tillhandahåller journalinnehållet för behörig och för att kunna avgöra att någon är behörig krävs en säker identifiering. I det andra fallet har säljaren ett behov av att kunna lita på att den e-underskrift som anknyts till köpeavtalet har skapats av just den köparen.

[9] Se vidare E-delegationens juridiska vägledning för verksamhetsutveckling inom e-förvaltningen (mars 2015).

[10] Detta har beskrivits av E-delegationen i en juridisk vägledning för verksamhetsutveckling inom e-förvaltningen (mars 2015) och en vägledning för Elektroniska original, kopior och avskrifter (juni 2012). Utformningen av e-tjänster och e-underskrifter har också beskrivits av Sveriges kommuner och landsting i en Rapport till en vägledning vid införandet av e-tjänster (oktober 2011).

[11] Se Riksskatteverkets beslut om riktlinjer för myndigheternas användning av elektroniska signaturer och certifikattjänster m.m. (RSV M 2001:35), E-nämndens grundläggande vägledning för myndigheternas användning av e-legitimationer och elektroniska underskrifter och E-nämndens vägledning för användargränssnitt som uppfyller legala krav (båda från juni 2004). Frågor om bevarande och gallring har dessutom redovisats i Riksarkivets rapport (2006:1) Elektroniskt underskrivna handlingar, med utgångspunkt från den teknik som då användes. Riksarkivet har utarbetat ett utkast till vägledning för bevarande och gallring av elektroniska underskrifter (december 2015).

[12] Avser enskilda som använder myndigheters e-tjänster – beroende på sammanhanget även kallade innehavare eller undertecknare.

processerna för att legitimera sig och skriva under ägde då huvudsakligen rum utan att utfärdaren av e-legitimationen eller någon särskild leverantör genomförde automatiserade kontroller och ställde ut intyg om vem som legitimerat sig. Utfärdaren tillhandahöll – utöver det som hör till utfärdandet av e-legitimationer – tjänsten för spärr och för kontroll av att använd e-legitimation inte var spärrad.

En förlitande part – till exempel en myndighet som infört legitimering och underskrift i en e-tjänst – fick därmed själv genomföra de kryptografiska kontrollerna innan tillträde gavs till en e-tjänst.[13] På samma sätt fick den som mottagit en e-underskriven handling själv kontrollera om den var äkta.[14] Tre aktörer deltog således – utfärdare av e-legitimation, förlitande part och användare – och utfärdarens roll var begränsad. Medan utfärdare av e-legitimation slöt avtal med användare om att utfärda e-legitimation och tillhandahålla anknytande tjänster för spärr slöt samma utfärdare ett s.k. förlitandeavtal med förlitande part. Enligt det senare avtalet skulle utfärdaren på vissa villkor ansvara för att utfärda e-legitimationer och för tillhörande funktioner för spärr och spärrkontroll. Förlitande part fick i enlighet med avtalet tillgång till en tjänst för att kontrollera om e-legitimationen var spärrad. I övrigt fick förlitande part utföra de kryptografiska kontrollerna själv.

Infratjänst 2003 och eID 2008

Ramavtalen för Infratjänst 2003 och eID 2008 resulterade i att e-legitimations- och e-underskrifttjänsterna kunde avropas från återförsäljare (Logica/CGI, Sirius IT/Visma och Cybercom) som agerade för utfärdarna så att förlitande part endast behövde sluta ett avtal med en leverantör som denne gett fullmakt att rättshandla gentemot utfärdarna.

Detta underlättade för förlitande parter som bara behövde bygga ett tekniskt gränssnitt[15] gentemot återförsäljaren för att kunna nyttja spärrtjänsterna och istället låta integrationen mot respektive utfärdare utföras av återförsäljaren. Större förlitande parter tecknade dock normalt avtal direkt med utfärdarna och integrerade spärrkontrollfunktionen mot dessa.

Nuvarande versioner av e-legitimationssystemet

Arbetet med ett nytt e-legitimationssystem har delvis ändrat dessa förutsättningar. Förändringarna har skett successivt för att närmare uppmärksammas i E-legitimationsnämndens arbete med Svensk e-legitimation. Utfärdare av e-legitimation tillhandahåller nu även funktioner för att, genom automatiserade kontroller online, granska vem som har legitimerat sig, ställa ut ett svar där det framgår vem som har legitimerat sig (identitetsintyget) och sända det till förlitande part. Förlitande part ska därför inte längre behöva kontrollera om den använda e-legitimationen är spärrad och inte heller göra de kryptografiska kontrollerna av vem som legitimerat sig. Det är tillräckligt att ta del av intyget[16], som levereras i ett överenskommet format, oberoende av hur en användares e-legitimation utformats. Dessa förändringar har underlättat för myndigheter att införa funktioner för e-legitimering och e-underskrift även om ett ansvar och viss risk alltjämt vilar på den förlitande parten.

---

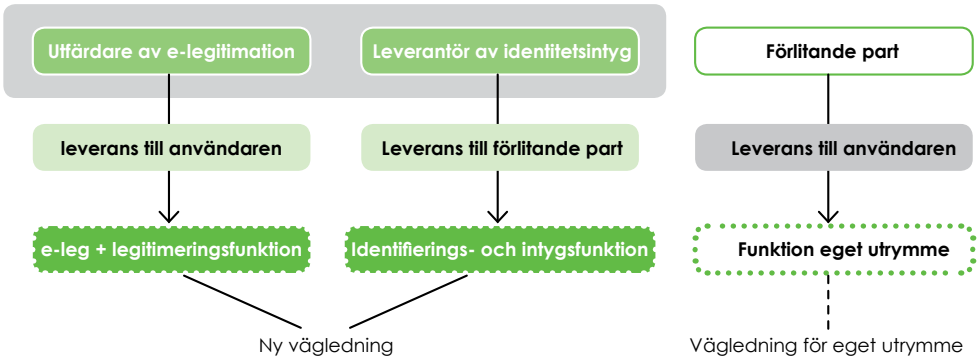
[13] Förlitande part använde härvid en av BankID certifierad kontrollprogramvara (BICS).
[14] Visserligen kom myndigheter att i allt högre grad anlita underleverantörer för dessa kontroller, men i juridisk mening utförde myndigheten kontrollen.
[15] Detta hanterades genom ett webservice-gränssnitt kallat OSIF (Offentlig sammanhållen identifieringsfunktion) som nu förvaltas av Kammarkollegiet.
[16] Detta intyg skickas oftast i formatet SAML (Security Assertion Markup Language), ett XML-baserat protokoll där innehållet kryptografiskt signeras av utfärdaren av intyget och där mottagaren av intyget kontrollerar att intyget är korrekt vid mottagandet.

Med utgångspunkt i det arbete som har bedrivits för Svensk e-legitimation har detta beskrivits så att en ny aktör, *leverantör av identitetsintyg*[17], har tillkommit. Denne tillhandahåller en funktion för att identifiera den som legitimerat sig och utfärda identitetsintyg.

I praktiken sluts emellertid de avtal enligt vilka identitetsintyg levereras i många fall antingen direkt mellan förlitande part och en utfärdare av e-legitimation, som samverkar med andra utfärdare (till exempel en bank som levererar BankID), eller med en leverantör till förlitande part (till exempel CGI, Visma och Cybercom), som inte själv utfärdar e-legitimationer men som har slutit förlitandeavtal med en utfärdare. – Ytterligare tjänster tillhandahålls alltså numera åt förlitande part.[18]

Detta kan sammanfattas så att

- *utfärdare av e-legitimation* förser användaren med en e-legitimation och stödfunktioner för att användaren ska kunna bruka e-legitimationen för att legitimera sig,[19]
- *leverantör av identitetsintyg* utför en e-identifiering, dvs. en kryptografisk kontroll av vem som legitimerat sig, ställer ut ett identitetsintyg och sänder det till förlitande part (en roll som utfärdare av e-legitimation ofta tar på sig), och
- *förlitande part* släpper in användaren i e-tjänsten och förser denne vanligtvis med ett eget utrymme i enlighet med eSams publikation från april 2016 ”Eget utrymme – en vägledning”, jämför följande figur.



Till detta kommer den ovan beskrivna nya rollfördelningen, de nya aktörer som tillhandahåller underskriftstjänster i anknytning till myndigheters e-tjänster och de frågor om upphandling som har berörts i avsnitt 2.1.4. Där framgår att myndigheter har kunnat välja olika sätt att upphandla. De som valt en annan form för upphandling än e-legitimationsnämndens övergångstjänst måste i hög grad själva precisera vad som upphandlas och vilka krav som ställs. Dessa val blir betydelsefulla av många skäl, till exempel för informationssäkerheten.

[17] E-legitimationsnämnden hade föreslagit en avtalsstruktur där en motsvarighet till dagens förlitandeavtal skulle slutas med leverantör av identitetsintyg, inte med utfärdare av e-legitimation. En leverantör av identitetstyg skulle istället knyta en eller flera utfärdare till sig och ta visst ansvara för de åtgärder som de utför. Detta avtalspaket för svensk e-legitimation har dock inte tagits i bruk.

[18] Inom de e-legitimationssystem som beskrevs under 2000-talets första år försåg förlitande part vanligtvis användare också med delar av det användargränssnitt och tekniska stöd i övrigt som användaren nyttjar när han eller hon legitimerar sig. I och med att utfärdare av e-legitimation eller en särskild leverantör av identitetsintyg börjat förse förlitande part med identitetsintyg har det emellertid blivit naturligt för utfärdaren att av till exempel säkerhetsskäl förse användaren även med en legitimeringsfunktion.

[19] Som exempel kan nämnas den app som banker tillhandahåller för Mobilt BankID. – Utfärdaren förser naturligtvis som tidigare innehavare av e-legitimation även med vissa tjänster för spärr och annan administration av dennes e-legitimation.

4. HUR FUNGERAR E-LEGITIMERING?

I detta kapitel beskrivs från ett juridiskt perspektiv de olika stegen vid e-legitimering och efterföljande identifiering av individ. Beskrivningen är inriktad på vilken information som hanteras och innebörden av åtgärderna. I detta ingår även att tydliggöra vad den som erbjuder en e-tjänst (förlitande part), användaren, leverantören av identitetsintyg och eventuella underleverantörer, vidtar för åtgärder i de olika stegen. Även hanteringen av utländska e-legitimationer berörs. Kapitlet vänder sig i första hand till de som behöver fördjupa sig i bakomliggande procedurer för att kunna förstå och utforma dem på ett sådant sätt att e-legitimationen kan användas korrekt.

4.1 Efter e-legitimering sker alltid en e-identifiering i ett tänkt flöde för att verifiera att den påstådda identiteten (till exempel ett angivet personnummer) tillhör den användare som har legitimerat sig. I det följande beskrivs hur detta numera görs med hjälp av en e-legitimation.

Definitioner

4.2 Med e-legitimering menas att innehavaren av en e-legitimation använder den för att visa vem han eller hon är.

4.3 Med e-identifiering menas en kontroll[20] av vem som legitimerat sig.

4.4 Med identitetsintyg menas en elektronisk handling, som kan användas endast vid ett visst tillfälle, där utställaren intygar vem som har legitimerat sig.[21]

E-legitimering för olika syften

4.5 E-legitimering kan ske för till exempel

1. tillträde, i syfte att elektroniskt få tillgång till uppgifter som får lämnas ut till den person som legitimerat sig och få skydd mot att någon annan släpps in under sken av att vara den som legitimerat sig,
2. uppgiftslämnande, för att lämna uppgifter elektroniskt och få skydd mot att någon annan lämnar uppgifter under sken av att vara uppgiftslämnaren, eller
3. indirekt underskrift, för att ställa ut en elektronisk handling som är skyddad mot förfalskning och förnekande av underskrift på motsvarande sätt som om handlingen hade undertecknats på papper (se 5.9).

Beroende på den typ av e-tjänst användaren nyttjar och informationsinnehållet i tjänsten kan en viss minsta skyddsnivå krävas för e-legitimationen och tillhörande identifiering.

[20] Som synonym används ofta ”autentisering” vilket är samma sak. Dessutom används e-legitimering och e-identifiering i vanligt språkbruk ofta synonymt.

[21] Av denna definition framgår att begreppet identitetsintyg här fyller en juridisk funktion och därmed inte tar sikte på vilka tekniska lösningar som används i det enskilda fallet; jfr kap. 8 om skyddet enligt 14 och 15 kap. brottsbalken för urkunder och andra handlingar.

Åtgärder av användare och förlitande part – för e-legitimering

4.6 En användare kan ha en eller flera e-legitimationer, utställda av olika utfärdare. Vilken e-legitimation som ska användas avgör användaren själv genom att välja en åt denne redan utfärdad e-legitimation. Vanligtvis sker det hos den förlitande part som användaren besöker. Förlitande part sänder då en begäran till en legitimeringsfunktion för den e-legitimation som användaren har valt. Av begäran framgår normalt vilken förklarande text som ska visas (till exempel ”Jag legitimerar mig mot x-myndigheten”).

4.7 Därefter förs användaren till legitimeringsfunktionen som normalt tillhandahålls av utfärdare av e-legitimation.

4.8 I legitimeringsfunktionen

1. ser användaren för vem (dvs. vilken förlitande part) han eller hon är på väg att legitimera sig (till exempel en viss myndighet i en e-tjänst), och
2. uppger användaren, automatiserat eller via formulär, vem han eller hon är, samt
3. startar proceduren för att användaren ska kunna identifieras (till exempel genom att ange sin kod).

Åtgärder av leverantör av identitetsintyg – för e-identifiering

4.9 Leverantör av identitetsintyg genomför automatiserade kontroller i en identifierings- och intygsfunktion (i tekniska sammanhang kallat ”autentiserar användaren”).

4.10 Bekräftar kontrollerna uppgiften om vem som har legitimerat sig ställer leverantören ut ett identitetsintyg och sänder det till den som har begärt intyget.

4.11 En identifierings- och intygsfunktions leverans till den som beställt intyget kan ske

– *direkt*, från den aktör som utfärdar e-legitimationer,[22] eller
– *indirekt*, från en underleverantör som mottagit ett intyg direkt från en utfärdare och konverterat uppgifterna till ett intyg som är anpassat för den förlitande partens it-miljö.[23]

När identitetsintyg levereras indirekt till förlitande part kontrollerar den leverantör av identitetsintyg som förlitande part anlitat först den direkta leveransen (från en aktör som utfärdar e-legitimationer). Därefter konverterar leverantör av identitetsintyg uppgifterna till ett intyg, förser intyget med sin e-stämpel och inkluderar de uppgifter som behövs för att validera intygets äkthet.

[22] Leverans sker vanligtvis i samverkan med andra utfärdare av e-legitimation och med intyg som har ett format som inte är anpassat till myndighetens tekniska miljö.
[23] E-legitimationsnämnden har föreslagit en avtalsstruktur där en motsvarighet till dagens förlitandeavtal sluts med leverantör av identitetsintyg, inte med utfärdare av e-legitimation. En leverantör av identitetsintyg avsågs istället knyta en eller flera utfärdare till sig och ta visst ansvar för de åtgärder som de utför.

Exempel 1 – direkt leverans: Myndighet X, som tillhandahåller en e-tjänst där e-legitimering krävs, har slutit förlitandeavtal med banken B (ansluten till BankID) genom avrop av den särskilda övergångstjänst som E-legitimationsnämnden annonserat. När användare A har legitimerat sig, med en e-legitimation utfärdad av B (eller annan bank inom BankID-samarbetet) och B har identifierat A, levererar B i enlighet med parternas avtal styrkande urkunder direkt till X. Den information som X i praktiken litar på har varken skrivits under eller stämplats av leverantörens intygsfunktion.[24]

Exempel 2 – indirekt leverans: Myndighet Y tillhandahåller också en e-tjänst där e-legitimering krävs. Y har emellertid slutit avtal med CGI som är återförsäljare av legitimeringstjänster med BankID. När användare A har legitimerat sig för tillträde till myndighet Y:s e-tjänst sänder bank B intyget till CGI. CGI konverterar intyget till ett intyg som myndighet Y använder i sin it-miljö. Leveransen sker indirekt men som en obruten kedja av åtgärder och kontroller. Översänt intyg är e-stämplat av CGI.

Åtgärder av förlitande part – för kontroll av vem som legitimerat sig

4.12 Den förlitande part som mottagit identitetsintyget (dvs. den förlitande part som begärt intyget) kontrollerar att identitetsintyget är

- äkta (dvs. utställt av den leverantör av identitetsintyg som framstår som utställare),
- utställt av en leverantör som förlitande part godtar, och
- baserat på en e-legitimation som förlitande part godtar för den aktuella tjänsten.

Efter att dessa kontroller ägt rum sker andra automatiserade procedurer, anpassade till respektive e-tjänst, till exempel för att användaren ska styras till rätt eget utrymme, i it-miljö ofta beskrivet som ”auktorisation” eller ”teknisk behörighetskontroll”; jämför behörighetskontrollsystem. Förlitande parts behov av att utföra kontroller blir beroende av hur säkert svaret levereras till den som avses lita på det.

Underleverantörer

4.13 Förlitande parter, utfärdare av e-legitimationer och leverantörer av identitetsintyg anlitar som framgått ofta underleverantörer för att utföra de beskrivna funktionerna.

Berörd aktör bör svara för sina tjänsteleverantörer som om aktören hade utfört åtgärden själv (se till exempel eSams publikation, Outsourcing – en vägledning om sekretess och persondataskydd).

Åtgärder vid legitimering med en utländsk e-legitimation

4.14 De europeiska e-legitimationer som anmälts enligt eIDAS-förordningen måste från och med den 29 september 2018 införas som möjligt val för legitimering i svenska myndigheters e-tjänster (se 12.15).

[24] Se de förändringar som gjordes år 2013 av BankID-tjänsten så att förlitande part får ett intyg om vem som har legitimerat sig – en kontroll som tidigare gjordes lokalt av förlitande part. Förlitande part kan kontrollera dels att en av spärrkontrollfunktionen stämplad urkund med svar på en spärr fråga är äkta, dels att en urkund som undertecknats med stöd av användarens privata nyckel för legitimering är äkta. Dessa urkunder och övrig information sänds över via en säker kanal.

Det är E-legitimationsnämnden som tillhandahåller den svenska nod, till vilken myndigheter ansluter sig, för att få stöd för denna alternativa metod för identifiering.

Legitimering och identifiering via den svenska noden går till på samma sätt som vid användning av en svensk e-legitimation, med undantag för att det inte är säkert att den som legitimerar sig i en utländsk legitimeringsfunktion kan se för vilken förlitande part han eller hon är på väg att legitimera sig (jfr 4.8). Den förlitande parten erhåller inte heller något identitetsintyg från en utländsk leverantör utan från E-legitimationsnämnden (jfr 4.10), som fungerar som indirekt leverantör, efter att ha mottagit ett intyg från en utländsk nod och vid behov konverterat uppgifterna till ett intyg som är anpassat för den förlitande partens it-miljö (jfr 4.11).

En sammanställning av vad som sker vid e-legitimering

4.15 Följande sammanställning ger en förenklad bild av hur hanteringen vanligtvis sker.

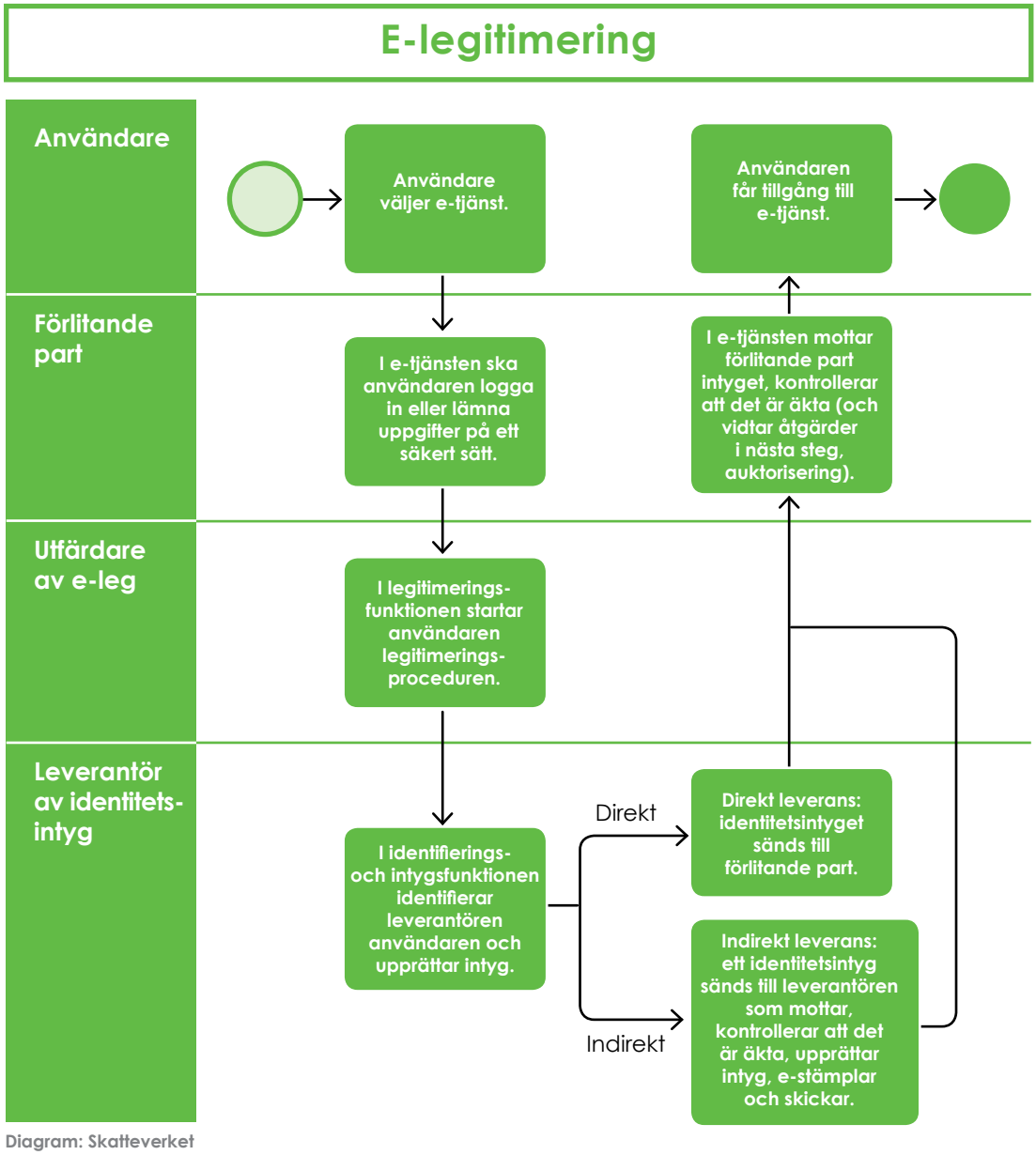


Diagram: Skatteverket

5. HUR FUNGERAR E-UNDERSKRIFT?

E-underskrifter har flera syften och används bland annat för att en identifierad användare på ett juridiskt bindande sätt ska kunna uttrycka sin vilja inom ramen för en e-tjänst. Detta kapitel inleds med en beskrivning av den juridiska funktionen hos en e-underskrift. Därefter följer en redogörelse för de olika stegen vid e-underskrift från ett juridiskt perspektiv. Det tydliggörs också vad den som erbjuder en e-tjänst (förlitande part), användaren, leverantören av identitetsintyget och eventuella underleverantörer vidtar för åtgärder i de olika stegen. Även hanteringen av utländska e-underskrifter berörs. Kapitlet vänder sig i första hand till de som behöver fördjupa sig i de bakomliggande procedurerna för att kunna förstå och utforma dem så att e-underskrifter kan användas på rätt sätt.

5.1 I detta kapitel finns definitioner och en beskrivning från en juridisk utgångspunkt av hur användare numera skriver under elektroniskt inom e-legitimationssystem som används i anknytning till de e-tjänster som tillhandahålls av myndigheter.

Definitioner

5.2 Med e-underskrift menas uppgifter i elektronisk form som är fogade till eller logiskt knutna till andra uppgifter i elektronisk form för att säkerställa de senares ursprung och dataintegritet.[25]

5.3 Med e-urkund avses en elektronisk handling som har en utställarangivelse som kan kontrolleras på ett tillförlitligt sätt.[26]

5.4 Med särskilt underskriftscertifikat menas en identitetshandling i elektronisk form, utställd automatiserat efter att en användare har legitimerat sig och som endast används för att skapa en indirekt underskrift (se 5.9) och knuten till en privat nyckel som kan användas för att framställa en underskrift endast vid ett tillfälle.[27]

Underskrifters juridiska funktioner

5.5 Handlingar skrivs under elektroniskt för att ge skydd mot förfalskning och förnekande på motsvarande sätt som när handlingar undertecknas på papper. Underskriftens funktion är främst säkerhetsrelaterad, såsom att ge underlag för

[25] Jfr däremot eIDAS-förordningen där det sista ledet ”för att säkerställa de senares ursprung och integritet” ersatts med ”och som används av undertecknaren för att skriva under”. Eftersom detta kan föra tanken fel (till den s.k. privata nyckeln, inte till själva underskriften) har vi gjort en mindre språklig justering. Någon materiell skillnad är inte avsedd. Något förenklat kan en e-underskrift beskrivas som en motsvarighet till en traditionell underskrift på papper. I 15 kap. 13 § brottsbalken beskrivs detta som en utställarangivelse avseende en urkund, när angivelsen är sådan att den kan likställas med en underskrift.

[26] Till definitionen i 14 kap. 1 § andra stycket 2 BrB hör också att handlingen ska ha upprättats till bevis eller annars vara av betydelse som bevis. Så är fallet med här berörda handlingar.

[27] Den privata nyckeln förstörs genast efter underskrift. Ett sådant särskilt underskriftscertifikat kan dock användas flera gånger för att kontrollera vem som har skrivit under handlingen och att dess innehåll inte har manipulerats.

- äkthetsprövning (kontroll av vem som skrivit under och att handlingens innehåll inte har ändrats),
- bevissäkring (ett skriftligt bevis skapas), och
- originalkvalitet (det blir möjligt att skilja handlingar som kan kontrolleras på ett tillförlitligt sätt från oskyddade handlingar),[28]

När handlingens äkthet inte måste skyddas genom en underskrift kan andra skyddsfunktioner som underskrifter erbjuder föra med sig krav på undertecknande, såsom

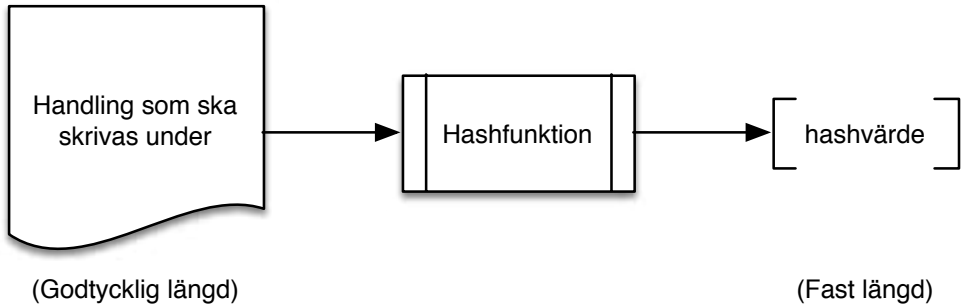
- avslutningsfunktionen (att innehållet är fullständigt och förenligt med utställarens avsikt), och
- varningsfunktionen (att tänka sig för och förstå åtgärdens innebörd).

Ett utkast innan underskrift sker

5.6 En användare upprättar ett utkast till en handling, granskar utkastet och väljer att skriva under. Utkastet kan finnas lokalt i användarens egen miljö eller i ett eget utrymme som tillhandahålls åt användaren i anknytning till en e-tjänst, se vidare eSams publikation Eget utrymme hos myndighet – en vägledning.

Förfarandet för att producera det underlag som tekniskt skrivs under

5.7 I användarens egen miljö eller i dennes eget utrymme produceras normalt ett underlag (kryptografiskt kondensat eller s.k. hashvärde), som ned till minsta tecken representerar den handling som ska undertecknas,[29] se följande figur.



Underlaget förmedlas[30] till en underskriftsfunktion som en begäran om en underskrift. [31] Av begäran framgår normalt vilken förklarande text som ska visas (till exempel ”Jag skriver under [min ansökan till x-myndigheten]”).

Förfarandet när en handling skrivs under, ges in och mottas

Åtgärder av användaren för att skriva under

5.8 I den följande användardialogen ser användaren för vem (vilken förlitande part) han eller hon är på väg att skriva under och ombeds att starta proceduren för underskrift genom att till exempel ange koden för sin e-legitimation.

---

[28] Se vidare E-delegationens vägledning Elektroniska original, kopior och avskrifter.
[29] Funktionens egenskaper innebär vidare att den inte kan ge samma hashvärde för två olika handlingar och att den bara fungerar en väg – det går inte att utifrån ett hashvärde finna den ursprungliga handlingens innehåll. Hashvärden har dessutom en fast längd så att de blir mera lätthanterliga samtidigt som handlingars innehåll inte avslöjas.
[30] För att skydda undertecknaren från kartläggning eller övervakning bör den handling som ska skrivas under inte finnas med (jfr 2 kap. 6 § andra stycket regeringsformen).
[31] Vad som ingår tekniskt är information om vad som omfattas av underskriften (hela eller delar av en handling), information om underskriften (tidpunkt, algoritmer etc.), hashvärde för data som ska skrivas under och eventuellt andra data knutna till använda standarder.

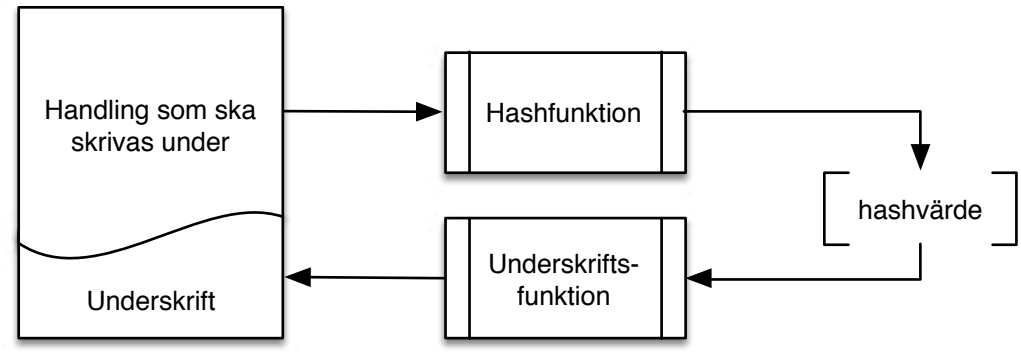
5.9 Underskriften kan produceras på två olika sätt,

- direkt med den e-legitimation som redan är utfärdad åt användaren, eller
- indirekt genom att användaren legitimerar sig för underskrift (se 4.5 p. 3 och 4.6-4.11) så att ett särskilt underskriftscertifikat ställs ut och används för att producera underskriften (se 5.15 och 5.16).[32]

Vid såväl direkt som indirekt underskrift startar användaren förfarandet i en funktion (ett användargränssnitt) som utfärdare av e-legitimation tillhandahåller åt användaren.[33] Där bör åtgärder vidtas så att användaren förstår när underskrift sker och inte vilseleds att tro att något annat äger rum än en legitimering för indirekt underskrift (jfr 5.5).

Åtgärder för att fullborda upprättandet och ge in urkunden

5.10 När underskriften framställts förs den till användarens egen miljö eller till användarens eget utrymme och fogas till den handling som skrivits under, se följande figur.



5.11 Om användaren inte redan har begärt att den färdiga urkunden ska ges in till den förlitande parten startar användaren funktionen för att skicka.[34]

Som en service åt användare kan automatiserade kontroller göras i eget utrymme av vem som har undertecknat urkunden och att innehållet inte ändrats (en s.k. äkthetsprövning). Om något har fallerat får användaren ett felmeddelande.

Åtgärder av förlitande part

5.12 Den förlitande part som tar emot urkunden gör en automatiserad äkthetskontroll (dvs. en kontroll av att handlingen skrivits under av den som anges vara utställare och att innehållet inte har ändrats).

---

[32] En viktig anledning till varför detta till synes komplicerade indirekta förfarande tillkommit är att det möjliggör ett större mått av frihet i förhållande till den tekniska lösningen för e-legitimationen, som vid indirekt underskrift inte behöver inneha egen förmåga att producera underskriften. Detta blir extra viktigt vid exempelvis gränsöverskridande e-underskrift, då det är svårt för förlitande parter att förhålla sig till olika tekniska format och processer för äkthetskontroll för olika former av e-underskrifter. Med stöd av det standardiserade identitetsintyget kan alla e-legitimationer genom det indirekta förfarandet användas för att producera e-underskrifter i myndighetens e-tjänst.

[33] Jfr den app som utfärdare av e-legitimation tillhandahåller åt den som har mobilt BankID. Aktivering vid indirekt underskrift har likheter med legitimering för uppgiftslämnande, dock att identitetsintyget skapas för att leverantör av underskriftstjänst ska identifiera undertecknaren.

[34] Se om anvisat mottagningsställe i avsnitt 4.1.1 E-delegationens juridiska vägledning för verksamhetsutveckling inom e-förvaltningen (mars 2015) och i E-nämndens vägledning från år 2005 för service och hantering av inkommande handlingar m.m.

Närmare om direkt underskrift

5.13 När användaren startar förfarandet för att producera underskriften, direkt med en e-legitimation som redan har utfärdats åt honom eller henne, t.ex. med BankID, inleds en automatiserad procedur i en tjänst som en leverantör av underskriftstjänst tillhandahåller för att framställa en underskrift med stöd av användarens privata nyckel för underskrift, som hör till e-legitimationen, och det översända underlag som tekniskt ska skrivas under (5.7).[35]

Leverantör av underskriftstjänst kan genomföra automatiserade jämförande kontroller av underskriften, med den e-legitimation[36] som är utfärdad till användaren. Visar kontrollerna att allt fungerat korrekt kan leverantör av underskriftstjänst ställa ut ett intyg i ett överenskommet format om att underskriften är äkta[37] och foga det till underskriften. Underskriften och det eventuella intyget sänds till användarens eget utrymme.

5.14 Undertecknaren skickar urkunden till förlitande part (5.11), som tar emot urkunden och gör en äkthetskontroll (jfr 5.12). Förlitande parts behov av att utföra kontroller blir beroende av hur säkert svaret levereras till den som avses lita på det.

Närmare om indirekt underskrift

5.15 Användaren förs till en sådan legitimeringsfunktion som beskrivits i 4.7 och 4.8 och undertecknar genom att legitimera sig för indirekt underskrift (se 4.5 p. 3 och 7.9).[38]

Leverantör av identitetsintyg genomför automatiserade kontroller av vem som legitimerat sig (4.9), ställer ut ett identitetsintyg för den som skriver under och sänder intyget till den leverantör av underskriftstjänst som har begärt intyget (4.10).

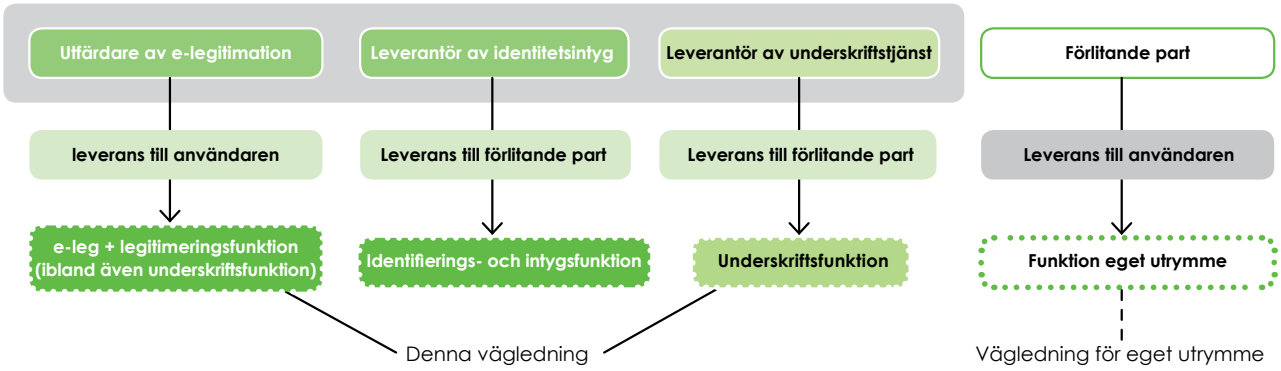
5.16 Leverantör av underskriftstjänst

- tar emot identitetsintyget och kontrollerar att det är äkta (4.12),
- ställer ut ett särskilt underskriftscertifikat (5.4) för undertecknaren,
- startar en automatiserad procedur för att framställa en underskrift med stöd av det särskilda underskriftscertifikatet och det underlag som tekniskt skrivs under (se 5.7),[39]
- kontrollerar automatiserat, med stöd av det särskilda underskriftscertifikatet, att underskriften är äkta,
- ställer ut ett intyg om att underskriften är äkta, om kontrollerna visat att underskriftsproceduren fungerat korrekt, och
- sänder intyget och underskriften till användarens eget utrymme.

---

[35] Av persondataskyddsskäl är den juridiska huvudlinjen att inte skicka in hela handlingen utan bara det underlag som tekniskt skrivs under. I tillämpningar där BankID används förekommer det visserligen att data som representerar hela handlingen sänds in till den centrala tjänsten, men dessa data raderas genast efter att en underskrift har producerats.
[36] I praktiken sker kontrollen med stöd av en certifierad publik nyckel, ett s.k. certifikat, som är till för underskrift. Här begränsas beskrivningen emellertid till det som krävs för att förstå de juridiskt relevanta delarna.
[37] När inte hela handlingen (utan bara ett hashvärde, se 5.7 och not 29) sänds till den tjänst där underskriften framställs måste det som intygas av tjänsteleverantören begränsas till vem det är som har skrivit under. För att det ska kunna granskas om innehållet har ändrats efter undertecknandet krävs tillgång till hela den underskrivna handlingen.
[38] Proceduren för att upprätta ett identitetsintyg kan grundas på direkt eller indirekt leverans av ett identitetsintyg (se 4.11).
[39] I samma skede förstörs det särskilda underskriftscertifikatets nyckel för att skriva under medan nyckeln för att kontrollera underskriftens äkthet bevaras.

5.17 Undertecknaren skickar urkunden till förlitande part (5.11), som tar emot urkunden och gör en äkthetskontroll (5.12; jfr följande översiktliga figur där det av det grå fältet framgår att samma juridiska person kan ha flera roller).



Underleverantörer

5.18 Om utfärdare av e-legitimation, leverantör av identitetsintyg, leverantör av underskriftstjänst eller förlitande part anlitar en underleverantör svarar den som anlitat underleverantören för tillhandahållen funktion som om denne hade utfört åtgärden själv.

5.19 Den kedja av automatiserade procedurer, som leder fram till att en underskriven handling kommer in till en myndighet, behöver hållas samman både tekniskt och juridiskt. Myndigheter bör överväga om underleverantörer kan underlätta tillgången till en sammanhängande kedja av bevis om äkthet och ursprungligt skick.

Åtgärder vid underskrift med en utländsk e-legitimation

5.20 Genom att ett alternativ för europeiska e-legitimationer införs (se 4.14) i myndigheters e-tjänster blir det också möjligt att skriva under med en utländsk e-legitimation. Underskrift bör ske indirekt genom att användaren legitimerar sig för underskrift (jfr 5.9) med sin utländska e-legitimation. En sådan underskrift produceras i allt väsentligt på samma sätt som vid indirekt underskrift med en svensk e-legitimation.

Eftersom det inte är säkert att den som legitimerar sig för underskrift i en utländsk legitimeringsfunktion får information där om att han eller hon skriver under – det går inte att styra den förklarande text som visas i ett annat land – har ett till led införts efter legitimeringen, där undertecknaren måste klicka på en knapp med texten ”Jag skriver under”, för att den elektroniska underskriften ska produceras.

En sammanställning av vad som sker vid e-underskrift

5.21 Följande sammanställning förenklar en överblick av hanteringen för e-underskrift.

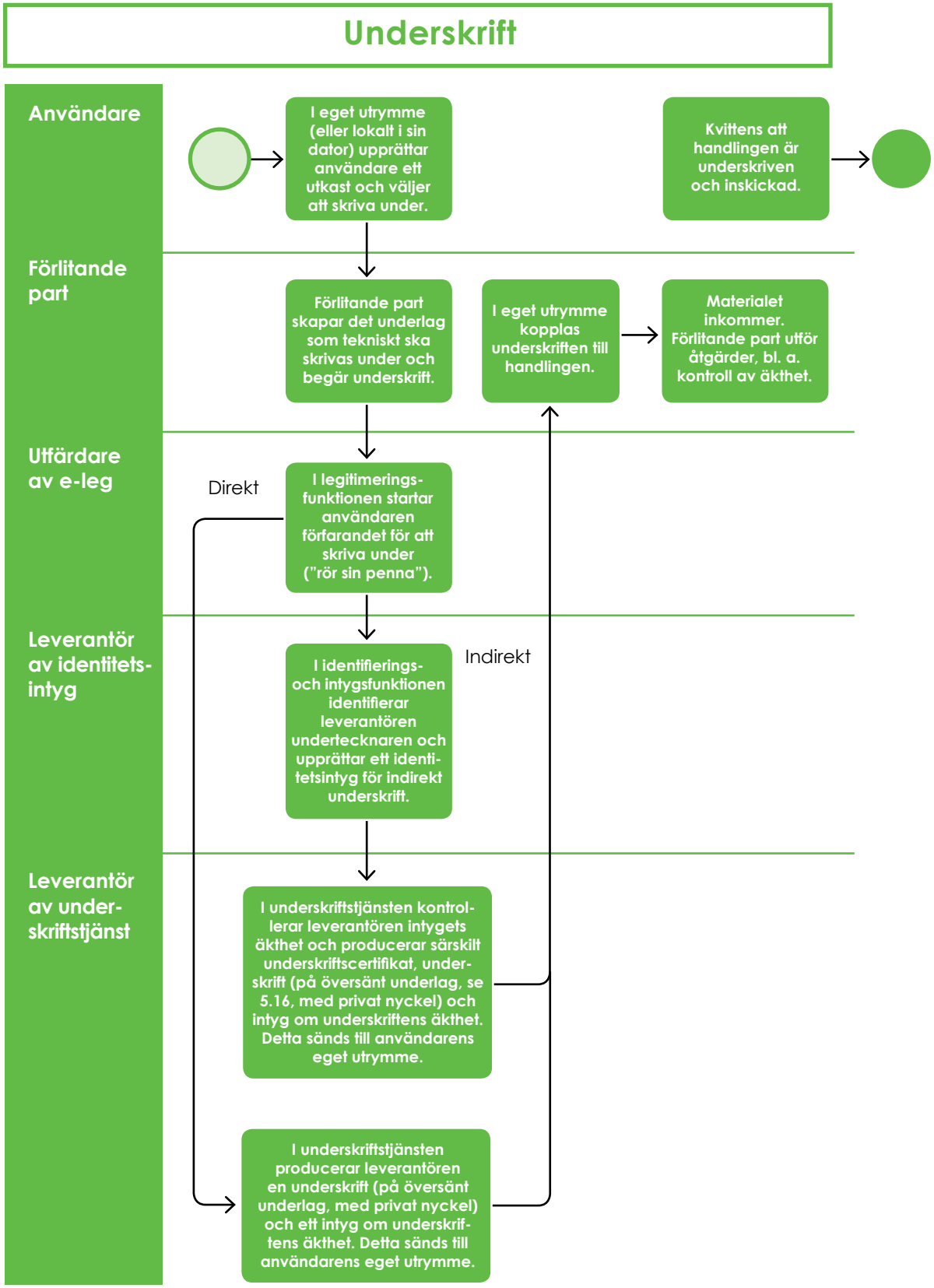


Diagram: Skatteverket

6. NÄR FÅR E-UNDERSKRIFTER ANVÄNDAS?

När en organisation överväger att börja använda e-underskrifter i sina e-tjänster är det av vikt att veta vilka formkrav som finns kopplade till olika förfaranden. Vissa formkrav hindrar att e-underskrifter används medan andra formkrav tillåter det. I det här kapitlet tydliggörs vilka regler som finns och när e-underskrifter får användas.

Formkrav

6.1 Med formkrav menas att en handling, för att ha en viss rättsverkan, ska ha viss form eller visst innehåll eller ska tillkomma eller annars hanteras på visst sätt. Vid elektronisk hantering av handlingar består formkravens styrande effekt vanligtvis i att vissa termer eller uttryck betecknar åtgärder som inte kan utföras elektroniskt.[40]

6.2 Om en handling enligt en formföreskrift i lag, förordning eller myndighetsföreskrifter ska vara försedd med underskrift, namnteckning, undertecknande eller liknande, kan detta krav inte uppfyllas med elektroniska rutiner.[41] Sådana formföreskrifter är emellertid inte särskilt vanliga. E-underskrifter kan därför normalt användas.

Krävs underskrift på beslutshandlingar?[42]

Skyddsbehoven kan normalt tillgodoses utan underskrift

6.3 Krav på att en myndighets beslut ska vara underskrivna gäller endast om det föreskrivs i lag, förordning eller myndighetsföreskrifter.[43] Sådana krav är ovanliga.[44]

De skyddsbehov som ligger till grund för att en myndighets beslut upprättas skriftligt kan normalt tillgodoses i elektronisk miljö, utan underskrift, om förfarandet har utformats så att kraven på äkthet, informationssäkerhet och tydliga användargränssnitt tillgodoses.[45]

---

[40] För vissa bestämmelser gäller emellertid att det inte är formkraven i sig som är det egentliga hindret för elektroniska rutiner, utan den process som formkravet är en del av. I till exempel en ansökningssituation kan det finnas krav på att det skall fogas bilagor till ansökan eller deklarationen, som inte finns tillgängliga elektroniskt och som kan vara svåra att digitalisera. – Följderna av att ett formkrav inte uppfylls varierar. Inom flera rättsområden finns bestämmelser om att en rättshandling som brister i form är ogiltig – helt eller delvis.

[41] Se den s.k. FORMEL-gruppens (Ju 2002:D) ställningstaganden (Ds 2003:29 s. 87 ff.). Gruppens bedömning torde alltjämt utgöra gällande rätt, dock att begreppet undertecknad i 38 kap. 1 och 2 §§ skatteförfarandelagen (2011:1244) används teknikneutralt så att kravet kan uppfyllas både genom undertecknande på papper och med elektroniska medel (prop. 2010/11:165 s. 857).

[42] Redovisningen i 6.3-6.7 tar sikte på myndighetsintern användning. Det tekniska och administrativa förfarandet kan här ofta vara ett annat än när enskilda skriver under elektroniskt i anknytning till de e-tjänster som vägledningen i övrigt tar sikte på.

[43] Se till exempel 17 kap. 10 § rättegångsbalken.

[44] Krav på undertecknande av beslut följer inte av förvaltningslagen och inte heller av myndighetsförordningen, där det däremot i 21 § föreskrivs att det för varje beslut i ett ärende ska upprättas en handling som visar dagen för beslutet, beslutets innehåll, vem som har fattat beslutet, vem som har varit föredragande och vem som har varit med vid den slutliga handläggningen utan att delta i avgörandet. Inte heller termen ”beslut” anses, när den används i lag eller författning, hindra elektroniska rutiner, se Ds 2003:29 s. 98.

[45] Ds 2003:29 s. 100. Se även Förvaltningslagsutredningen som år 2010, i anknytning till bedömningen av reglerna om överklagande, anfört att den tekniska utvecklingen och därmed möjligheten att på ett bättre och säkrare sätt kunna verifiera att ett meddelande verkligen härrör från den uppgivne avsändaren, nu kommit därhän att kravet på egenhändigt undertecknande mera allmänt kan ifrågasättas i lagstiftningen (SOU 2010:29 s. 668).

Vad beslutsfattaren ser och förstår

6.4 Beträffande vissa av de funktioner som en underskrift fyller kan tydliga användargränssnitt ge samma distinkta och tydliga resultat som en underskrift på papper. Detta gäller för avslutningsfunktionen (att innehållet är fullständigt och förenligt med undertecknarens vilja) och varningsfunktionen (att utställaren tänker sig för och förstår åtgärdens innebörd).

Att utställaren tänker sig för och förstår

Bevis om att beslutshandlingen är äkta

6.5 Beträffande andra funktioner som underskrifter fyller och som tar sikte på att kunna kontrollera att en handling är äkta[46] kan kontrollerna vanligtvis införas på enklare sätt när handlingarna produceras inom myndigheten. Myndigheten har kontroll över hela det automatiserade förfarandet; jfr däremot handlingar som skrivs under och ges in av utomstående.

En metod kan vara att förse besluten med myndighetens elektroniska stämpel (e-stämpel)[47] efter att beslutsfattaren identifierats på ett säkert sätt och klickat på en knapp med texten ”Jag beslutar” i stället för ”Jag skriver under” (jfr 6.9).

6.6 Vid bedömningen av vilka rutiner som är lämpliga behöver också beaktas om beslutet blir att anse som en urkund, så att straffrättsligt skydd ges mot förfalskning av e-urkunden (dvs. av den e-underskrivna eller e-stämplade handlingen i kontrollerbar form). Har en handling urkundskvalitet ges samtidigt straffrättsligt skydd mot att sanningslöst utge en handling för att vara en riktig kopia[48] av urkunden (till exempel en manipulerad kopia i pdf-format som varken är e-stämplad eller e-underskriven).

Här leder alltså tekniska och administrativa val till olika resultat med avseende på det straffrättsliga skyddet.[49] Dessa val blir särskilt viktiga när beslut ska spridas externt till aktörer som avses lita på innehållets ursprung.

Särskilt om kommunala protokoll

6.7 Ett protokoll ska enligt 5 kapitel 61 § kommunallagen (1991:900) justeras senast fjorton dagar efter sammanträdet på det sätt som fullmäktige har bestämt. Enligt Kammarrätten i Göteborgs dom den 24 september 2014 (mål nr 3459-14) finns inte hinder mot att justera kommunala sammanträdesprotokoll med elektronisk signatur.[50]

Krävs underskrift på ansökningshandlingar och liknande skrifter till myndighet?

6.8 Handlingar som ges in till en myndighet måste vara underskrivna på papper eller elektroniskt endast om sådan form krävs enligt lag, förordning eller myndighetsföreskrifter. Föreskrivs det att en handling ska vara underskriven – utan något tillägg för elektroniska förfaranden – uppfyller en elektronisk underskrift inte kravet.[51]

---

[46] Med att beslutshandlingen är äkta menas att det verkligen är angiven befattningshavare som är utställare och att innehållet inte har ändrats.
[47] Med elektronisk stämpel menas enligt eIDAS-förordningen (art. 3.25) uppgifter i elektronisk form som är fogade till eller logiskt knutna till andra uppgifter i elektronisk form för att säkerställa de senares ursprung och integritet.
[48] Se E-delegationens vägledning Elektroniska original, kopior och avskrifter.
[49] Om en myndighet upprättar beslut så att de har urkundskvalitet kan den som åberopar en obestyrkt kopia av beslutet och har manipulerat innehållet ha gjort sig skyldig till missbruk av handling (15 kap. 12 § tredje stycket BrB).
[50] Numera används vanligtvis e-underskrift i stället för uttrycket elektronisk signatur. Här kan antas att förfaranden med e-stämplar också kan komma i fråga om funktionerna utformas på ett ändamålsenligt sätt.
[51] Ett undantag i skatteförfarandelagen har redovisats i not 41. Se även kap. 12 där det framgår att eIDAS-förordningen inte föranleder annan bedömning.

Regler om att handlingar ska skrivas under, elektroniskt eller på papper, finns i till exempel rättegångsbalken, fastighetsbildningslagen, aktiebolagslagen, socialförsäkringsbalken, tullagen och fastighetstaxeringslagen m.fl. författningar.[52] Finns en regel om underskrift i myndighetens egna föreskrifter kan myndigheten välja att ta bort detta hinder om de funktioner som underskriften fyller tillgodoses på annat sätt.[53]

6.9 De skyddsbehov som har föranlett att ansökningshandlingar och andra handlingar som ges in till en myndighet ska skrivas under bör i många fall – med beaktande av skyddsvärde och risk – kunna tillgodoses i elektronisk miljö, utan underskrift, om förfarandet utformas ändamålsenligt (jfr fotnot 45). Vid bedömningen av vilka rutiner som är lämpliga bör också beaktas om handlingarna får sådan form att de blir att anse som urkunder.

6.10 När det inte finns någon formföreskrift som kräver att en handling skrivs under (elektroniskt eller på papper) får myndigheten göra en bedömning utifrån vilken kategori av handling det är fråga om och vilka av underskriftens funktioner som behöver ersättas av annat tekniskt eller administrativt skydd.

När en handlings äkthet inte måste skyddas genom en underskrift är det normalt tillräckligt att underskriftens avslutnings- och varningsfunktion (se 4.6) tillgodoses på annat sätt, till exempel genom tydliga användargränssnitt och förklarande texter så att användaren får motsvarande tydliga uppfattning om åtgärdens betydelse och rättsverkningar.

Är det huvudsakliga syftet, bakom att en viss kategori av handlingar skrivs under, istället att få skydd mot förfalskning och förnekande på motsvarande sätt som när handlingar undertecknas på papper, kan underskrifter emellertid behövas – elektroniskt eller på papper (se 4.6 om äkthetsprövning, bevissäkring och originalkvalitet). Här får en juridisk och teknisk bedömning göras beträffande varje kategori av handlingar och e-tjänster. Kan kompenserande tekniska och administrativa åtgärder och tydliga användargränssnitt ge motsvarande bevisvärde som en underskrift och utgör avsaknaden av straffrättsligt skydd inte ett hinder mot att avstå från underskrift bör alternativa förfaranden kunna införas.

6.11 En myndighet som tar emot handlingar elektroniskt bör genom en riskanalys klarlägga vilka av underskriftens funktioner som är centrala för berörda förfaranden och i vilken mån tekniskt, administrativt och rättsligt skydd kan ges med andra metoder.

Ett ökat behov av det straffrättsliga skyddet för e-urkunder

De särskilda risker som numera framträtt för att obehöriga utför rättshandlingar i annans namn har fört med sig ett ökat behov av att tillvarata det straffrättsliga skyddet för e-urkunder (se kap. 8). För vissa myndigheter och tillämpningar kan detta innebära att e-underskrifter behövs, även när sådana inte krävs enligt lag, förordning eller myndighetsföreskrifter, jfr kap. 12 om de krav som följer av Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden (eIDAS).

[52] Se vidare till exempel prop. 2015/16:72 och Ds 2003:29. Här bör nämnas att ett uppgiftslämnande ”på heder och samvete” inte måste vara förenat med underskrift (se 8.4).
[53] För inkommande handlingar gäller emellertid enligt 10 § tredje stycket förvaltningslagen att ett meddelande som kommit in till en myndighet och som inte är underskrivet ska bekräftas av avsändaren genom en egenhändigt undertecknad handling, om myndigheten begär det. Här ges myndigheten utrymme att laga efter läglighet.

7. AVTAL, ROLLER OCH CIVILRÄTTSLIGT ANSVAR

Användningen av e-legitimationer och e-underskrifter regleras i en rad olika avtal mellan olika aktörer. Det är viktigt att avtalen utformas korrekt så att det civilrättsliga ansvaret fördelas rätt mellan olika aktörer. Det här kapitlet beskriver

- **vilka aktörerna är**
- **olika typer av avtal som behövs på området och vad de kan behöva innehålla**
- **frågor om ansvar som aktualiseras**
- **risker som respektive aktör kan behöva beakta.**

Kapitlet ger stöd både åt organisationer som står i begrepp att utforma och teckna avtal på området och organisationer som redan ingått avtal och behöver kontrollera utformningen av dem. En skillnad som blir av betydelse från avtalssynpunkt är den som finns mellan direkt och indirekt legitimering respektive direkt och indirekt underskrift.

En reglering genom avtal

Parter

7.1 Aktörernas mellanhavanden vid legitimering och underskrift regleras genom avtal.[54] Följande aktörer kan vara parter i dessa avtal:

1) Användare.[55]
2) Förlitande part.[56]
3) Utfärdare av e-legitimation.
4) Leverantör av identitetsintyg.[57]
5) Leverantör av underskriftstjänst.
6) Myndigheter med en samordnande roll.[58]
7) Underleverantörer till 2-6.

Grundläggande typer av avtal

7.2 Genom följande typer av avtal etablerar parterna de e-legitimations- och underskriftssystem som numera används på myndighetsområdet:

a) Användare (1), som upprättar utkast i eget utrymme, sluter avtal om eget utrymme med förlitande part (2).
b) Användare (1), som legitimerar sig och skriver under elektroniskt, sluter e-legitimationsavtal med utfärdare av e-legitimation (3).

---

[54] Den författningsreglering som finns inom området rör främst formkrav och liknande som inte tar sikte på själva e-legitimations- och e-underskriftssystemet.
[55] Beroende på sammanhanget även kallad innehavare eller undertecknare.
[56] Exempelvis en myndighet som tillhandahåller en e-tjänst där legitimering och underskrift krävs.
[57] Kan i förhållande till förlitande part antingen leverera en tjänst i eget namn eller agera i egenskap av underleverantör för att hantera leveranser från en aktör som agerar självständigt. I underleverantörsfallet kan denna aktör även kallas integratör eller återförsäljare.
[58] Exempelvis E-legitimationsnämnden, Kammarkollegiet och Internetstiftelsen i Sverige.

c) Förlitande part (2), som identifierar användare och kontrollerar om underskrifter är äkta, sluter förlitandeavtal med leverantör av identitetsintyg (4).
d) Förlitande part (2), som beställer underskrifter, sluter avtal om underskriftstjänst[59] med leverantör av underskriftstjänst (5).

Kombinationer av beskrivna avtal

7.3 Den redovisade indelningen i olika avtalstyper förenklar juridiska beskrivningar av roller och förpliktelser inom de e-legitimations- och underskriftssystem som numera används. I praktiken är det emellertid vanligt att en leverantör (någon av 3-5) tillhandahåller kombinationer av tjänster och ikläder sig flera av de beskrivna rollerna.

Det är dessutom vanligt att en part (någon av 2-5) sluter avtal med en underleverantör (7) som parten svarar för i förhållande till annan part (någon av 2-5) som om den första parten hade utfört åtgärden själv (jfr 4.13 och 5.18-19).

> För att förtydliga detta kan noteras att en och samma juridiska person kan vara såväl utfärdare av e-legitimation (3) som leverantör av identitetsintyg (4) och leverantör av underskriftstjänst (5). En sådan part med flera roller sluter både förlitandeavtal och avtal om underskriftstjänst med förlitande part (2). Samtidigt kan denna part i rollen som utfärdare av e-legitimation (3) sluta e-legitimationsavtal med användare. Det förekommer också att en part som slutit förlitandeavtal eller avtal om underskriftstjänst samtidigt tillhandahåller funktioner i egenskap av underleverantör (7). Ett sådant kombinerat avtal kan innefatta såväl förlitandeavtal som avtal om underskriftstjänst och avtal om vissa andra tjänster, medan de e-legitimationer som används kan vara utfärdade av en annan part. Exempelvis kan en bank, till exempel Nordea, som tecknar förlitandeavtal och avtal om underskriftstjänst med en förlitande part förse denna förlitande part med avtalade funktioner både beträffande de e-legitimationer Nordea själv har utfärdat och e-legitimationer som utfärdats av andra banker. I ett sådant fall sluter inte förlitande part avtal direkt med alla berörda utfärdare av e-legitimation. Här finns ett behov av att uppmärksamma hur ansvaret för de tjänster en utfärdare av e-legitimation tillhandahåller är reglerat gentemot förlitande part.

Myndigheter med en samordnande roll

7.4 En myndighet som ingår förlitandeavtal och avtal om direkt underskriftstjänst med en leverantör efter avrop av den särskilda övergångstjänsten sluter dessutom avtal eller träffar en överenskommelse med E-legitimationsnämnden.[60] På motsvarande sätt reglerar Kammarkollegiets ramavtal de villkor som tillämpas på avrop av tjänster för e-legitimering och e-underskrifter.[61]

---

[59] Här är det viktigt att skilja mellan tjänster där underskriften produceras direkt med en e-legitimation som redan utfärdats åt undertecknaren (5.13) respektive indirekt genom att användaren legitimerar sig för underskrift (5.15) eftersom avtalen ska reglera förfaranden som skiljer sig åt och normalt berör olika parter.

[60] E-legitimationsnämnden har enligt 1 a § förordningen (2010:1497) med instruktion för E-legitimationsnämnden i uppdrag att efter överenskommelse med upphandlande myndigheter tillhandahålla system för säker elektronisk identifiering enligt 1 § andra stycket 2 lagen (2013:311) om valfrihetssystem i fråga om tjänster för elektronisk identifiering. Därför kan även E-legitimationsnämnden vara part (i avtal mellan 2 och 4-5), men i en särskild roll som följer av författning.

[61] Om den som avropar är en myndighet under regeringen är denne en del av samma juridiska person som E-legitimationsnämnden respektive Kammarkollegiet. Överenskommelsen kan därmed inte prövas i domstol eller av skiljemän. Därför används inte begreppet avtal för mellanhavandet med nämnden resp. kollegiet.

Avtalens innehåll

Avtalens reglerande funktion vid rättshandlingar

7.5 När avtal ingås enligt 7.2 tillhandahåller leverantörerna inte bara en viss funktionalitet. E-legitimeringar och e-underskrifter för med sig rättsverkningar i enlighet med vedertagna juridiska synsätt och tolkningsmetoder och resulterar i skriftliga bevis. Även dessa verkningar och bevis behöver i vissa delar regleras genom avtal.[62]

Avtal om eget utrymme (A)

7.6 En användare som upprättar utkast i eget utrymme har ett civilrättsligt mellanhavande med den förlitande part som förser användaren med utrymmet. Se eSams publikation, Eget utrymme hos myndighet – en vägledning, beträffande avtalsvillkor som kan behöva införas mellan förlitande part och användare av eget utrymme.

E-legitimationsavtal (B)

7.7 Parter i ett e-legitimationsavtal är användare och utfärdare av e-legitimation. Av betydelse blir de villkor som gäller för användare om att hantera e-legitimation och kod aktsamt, så att ingen annan kan legitimera sig eller underteckna under sken av att vara användaren. Att utfärdaren utför uppgifterna fackmannamässigt, till exempel vid identifiering av den som ansöker om e-legitimation, blir också av betydelse.

Att hantera e-legitimation och kod aktsamt

7.8 Utfärdaren av en e-legitimation tillhandahåller normalt även den legitimeringsfunktion som användaren nyttjar (se 4.8). Eftersom rättshandlingar som utförs med stöd av en e-legitimation avses bli juridiskt bindande är det av betydelse hur användargränssnitt i en legitimeringsfunktion utformas, vilka verkningar som anges i e-legitimationsavtalet av att bruka en e-legitimation[63] och vilka handlingar för validering som upprättas i bevissyfte.

7.9 Användarens faktiska handlande för att starta processen i en legitimerings- respektive underskriftsfunktion utgör själva e-legitimeringen respektive e-undertecknandet. Av e-legitimationsavtalet bör följa att rättshandlingar som utförs på detta sätt juridiskt ska jämställas med legitimering och underskrift i traditionell fysisk miljö.[64] Vid underskrift med en utländsk e-legitimation kan ett särskilt led krävas för att säkerställa att användaren tydligt får veta att han eller hon skriver under en handling (se 5.20).

Förlitandeavtal (C)

7.10 Parter i ett förlitandeavtal är förlitande part och leverantör av identitets-

[62] Förlitandeavtal och avtal om underskriftstjänst är vanligtvis fåordiga (utöver att det tillhandahålls en teknisk funktion) när det gäller vem som utför och svarar för vad (till exempel vem som i juridisk mening ställer ut det särskilda underskriftscertifikatet vid indirekt underskrift).

[63] Exempelvis har en utfärdare i sina e-legitimationsavtal infört ett villkor om att kunden, innan denne undertecknar elektroniskt, noga måste granska det som presenteras för underskrift och ta ställning till om kunden vill skriva under samt att det – om kunden undertecknar elektroniskt – innebär att denne vill att e-underskriften ska få samma verkan som om underskrift skett på papper.

[64] I elektronisk miljö utförs detta normalt genom att skriva sin kod och klicka på ”Jag legitimerar mig” eller ”Jag skriver under”. Undertecknarens åtgärd för att skriva under viss handling utförs alltså redan när denne, vid direkt underskrift startar sin e-legitimation för underskrift, respektive vid indirekt underskrift legitimerar sig för indirekt underskrift; jfr att visa upp sitt körkort och att hålla i en penna och röra handen över ett pappersark med text för att skriva under.

intyg, som utför vissa kontroller för att identifiera användaren och lämna intyg om vem användaren är (se 4.9-4.11).[65]

Förlitandeavtal utformas olika när identitetsintyg ska sändas direkt till förlitande part från en aktör som utfärdar e-legitimationer respektive indirekt från en aktör som tar emot intyg från en bakomliggande aktör som utfärdar e-legitimationer.

Den som enligt ett förlitandeavtal om indirekt leverans tar emot ett intyg från en bakomliggande direkt leverantör av identitetsintyg, anpassar vanligtvis uppgifternas format till förlitande parts it-miljö samt upprättar, e-stämplar och sänder ett identitetsintyg (se 4.11).

7.11 En *direkt* leverantör av identitetsintyg bär ett ansvar gentemot förlitande part för den e-identifiering som gjorts av användaren och för den bakomliggande hanteringen av e-legitimationer, till exempel att samtliga krav för aktuell tillitsnivå är uppfyllda.

En indirekt leverantör av identitetsintyg svarar för kontrollerna av att mottagna intyg från en bakomliggande direkt leverantör av identitetsintyg är äkta, för den anpassning av innehållet som sker ska göras till det format som förlitande part krävt och för att ett intyg ställs ut, e-stämplas och översänds på specificerat sätt. Här utförs således både de kontroller som en mottagare gör vid en direkt leverans av identitetsintyg och de ytterligare åtgärder och kontroller som krävs för den indirekta leveransen av identitetsintyg.

7.12 Vid *direkt* leverans av intyg behöver parterna avtala om ansvar, risker och vilket bevismaterial som produceras och tillhandahålls. Villkoren vid direkt leverans behöver bara omfatta *ett* led.

Avser ett förlitandeavtal i stället indirekt leverans behövs regler om ansvar, risker och bevis i flera led. Parterna behöver genom avtal kunna följa kedjan bakåt så att ansvar kan fördelas för fel i ett konverterat intyg utställt av en indirekt leverantör, som har sin grund i fel gjorda av en bakomliggande direkt leverantör eller utfärdaren av den e-legitimation som använts.[66] För alla dessa olika fall är villkor av betydelse om till exempel fackmannamässigt utförande[67] och vilka skriftliga bevis som levereras så att de kan åberopas vid en tvist.[68]

7.13 Villkoren i förlitandeavtal ska stödja juridiskt korrekta

- kontroller av vem som utför en rättshandling genom att legitimera sig, och
- begränsningar, så att någon annan än den som anges i ett identitetsintyg och använd e-legitimation inte ges tillträde eller annars får del av uppgifter, under sken av att vara den i identitetsintyg och e-legitimation angivna personen.

Villkoren i förlitandeavtal bör därför reglera hur e-legitimationer och identitetsintyg ska brukas och äkthetskontrolleras och förbjuda att någon annan än den

[65] När e-legitimationssystemet infördes under 2000-talets början fick förlitande part däremot, som framgår av avsnitt 3,3, själv utföra de kryptografiska kontrollerna innan tillträde gavs. Det fanns således endast utfärdare av e-legitimation som part (3). Den roll som leverantör av identitetsintyg (4) numera fyller utfördes av underleverantörer (7). Avtalen har endast delvis anpassats till de ändrade juridiska förutsättningar som blivit följden av att leverantörer av identifierings- och intygsfunktioner etablerats inom de e-legitimations- och underskriftssystem som numera används.

[66] Förlitandeavtal har ofta ett knapphändigt innehåll såvitt avser ansvaret för de delar som rör utfärdande av e-legitimationen eller identifiering och uppgiftslämnande om resultatet.

[67] Detta gäller särskilt för de höga krav på informationssäkerhet som är en nödvändighet för att tilliten till systemet ska kunna upprätthållas.

[68] Det är för närvarande i många fall oklart vilka urkunder som upprättas och bevaras så att de kan åberopas i händelse av en tvist.

som anges i e-legitimationen, eller en robot, ges tillgång till någon annans eget utrymme eller information under sken av att vara den som anges i e-legitimationen och identitetsintyget.[69]

Se vidare den juridiska checklistan för förlitandeavtal i kapitel 13.

Avtal om underskriftstjänst (D)

7.14 Parter i ett avtal om underskriftstjänst är den förlitande part som kräver underskrift och berörd leverantör av underskriftstjänst. Avtal om underskriftstjänst utformas olika när underskrift sker

- direkt med en e-legitimation som redan är utfärdad åt användaren (5.13), respektive
- indirekt genom att en leverantör av identitetsintyg identifierar användaren, intygar vem denne är och sänder intyget till leverantören av underskriftstjänst (4.5 p. 3 och 4.9-4.11) som utfärdar ett särskilt underskriftscertifikat (se 5.15-16).[70]

7.15 En leverantör av underskriftstjänst som skapar direkta underskrifter, med den e-legitimation som redan är utfärdad åt undertecknaren, svarar gentemot förlitande part för e-identifieringen av undertecknaren, den underskrift leverantören producerar på grundval av översänt underlag (5.7) och det intyg som leverantören ställer ut om den översända underskriftens äkthet. Leverantören bör gentemot förlitande part svara även för den bakomliggande hanteringen av e-legitimationen (för spärrkontroll etc.).[71]

Vid direkt underskrift behöver parterna avtala om ansvar, risker och vilket bevismaterial som produceras. Villkoren i ett förlitandeavtal för direkt underskrift behöver bara omfatta ett led och bakomliggande hanteringen av e-legitimation och intyg.

7.16 Skapar leverantören av underskriftstjänst istället indirekta underskrifter utför leverantören inte e-identifieringen av undertecknaren. Istället kontrollerar leverantören att mottaget intyg från en bakomliggande leverantör är äkta.

En leverantör av indirekta underskrifter avses däremot, gentemot förlitande part, svara för dels det särskilda underskriftscertifikat som denne ställer ut, dels den underskrift denne producerar på grundval av översänt underlag (5.7), dels det intyg som denne ställer ut om den översända underskriftens äkthet.

Leverantör av underskriftstjänst kan, gentemot förlitande part, svara även för den bakomliggande hanteringen av e-legitimationen och e-identifieringen efter e-legitimering för underskrift, i de fall där leverantören av underskriftstjänst fungerar som återförsäljare av den bakomliggande leverantörens e-identifieringar och intyg.[72]

Den bakomliggande hanteringen av e-legitimationen

[69] Jfr hur användaren i en banks e-legitimationsavtal förbinder sig att endast använda sin e-legitimation direkt i bankens tjänster och inte använda den när inloggning till bankens tjänster sker indirekt genom ett annat företags tjänst.
[70] Ett sådant utfärdas genast efter legitimering för underskrift och används endast en gång för indirekt underskrift (det lämnas således aldrig ut till undertecknaren för att innehas av denne så som en e-legitimation som används för direkt underskrift).
[71] Sker underskriften direkt levererar samma juridiska person både identifierings- och underskriftsfunktionerna och kan i många fall även vara utfärdaren av e-legitimationen. Ett exempel på detta är de underskrifter som levereras av en utfärdare av e-legitimation under varumärket BankID. – Förlitandeavtal som samtidigt innefattar ett avtal om underskriftstjänst där aktivering sker direkt är vanliga. De har emellertid ofta ett knapphändigt innehåll såvitt avser den juridiska rollfördelningen rörande hanteringen av det underlag som skrivs under, produktion av underskrift, leverans av resultatet samt vilka bevis som lämnas i form av e-urkunder så att de kan åberopas vid en tvist.
[72] Här ställs den myndighet som tillhandahåller e-tjänsten inför en kedja av funktioner där olika parter utför delar av hanteringen och ställer ut olika bevis. Det blir även av betydelse vilket ansvar leverantörerna har för e-legitimationen, underskriften och de bevis som levereras i form av e-urkunder för att kunna åberopas vid en tvist. Här är mellanhavandena emellertid komplexa.

Vid indirekt underskrift behöver parterna avtala om ansvar, risker och vilket bevismaterial som produceras. Villkoren i ett förlitandeavtal för indirekt underskrift behöver omfatta två led (dels äkthetskontroll av identitetsintyg och utfärdandet av ett särskilt underskriftscertifikat,[73] dels produktion av underskrift och intyg om underskriftens äkthet), samt den bakomliggande hanteringen av e-legitimationen.

7.17 Vid både direkt och indirekt underskrift är villkor om fackmannamässigt utförande av betydelse[74] samtidigt som det tydligt behöver regleras vilka skriftliga bevis som levereras eller kan begäras utlämnade så att de kan åberopas vid en tvist.[75] Parterna behöver genom avtal kunna följa kedjan bakåt så att ansvar kan fördelas för fel gjorda av en bakomliggande leverantör eller utfärdaren av den e-legitimation som använts. Det är också av vikt att leverantören av identitetsintyg i avtalet tar på sig ett rimligt felansvar i förhållande till förlitande part för e-identifieringen i dess helhet.

Parterna behöver kunna följa kedjan bakåt

7.18 Avtal om underskriftstjänst bör ge stöd för juridiskt korrekta kontroller av vem som har skrivit under en handling. Även i övrigt behöver hanteringen skyddas genom villkor i avtalet. Detta gäller till exempel för hur e-legitimationer och identitetsintyg för underskrift får brukas och äkthetskontrolleras och hur förfalskningar och andra missbruk ska förhindras. I avtalen behöver också beaktas att e-legitimationer utfärdas för olika tillitsnivåer och att det normalt visserligen är tillräckligt med en avancerad e-underskrift men att en kvalificerad eunderskrift undantagsvis kan krävas.

Avtal om underskriftstjänst för indirekta underskrifter behöver också innehålla villkor om vem som ansvarar för det särskilda underskriftscertifikatet och vilka som avses lita på det. Hit hör också hur och mellan vilka avtal sluts om särskilda underskriftscertifikat.

Se vidare den juridiska checklistan i kapitel 13 för avtal om underskriftstjänst.

Offentlig upphandling

Integratörer, återförsäljare och andra underleverantörer

7.19 Förlitandeavtal (C) och avtal om underskriftstjänst (D) med tillhörande reglering av särskilda underskriftscertifikat för indirekt underskrift har av många förlitande parter upphandlats genom avrop från ett ramavtal som Kammarkollegiet slutit med vissa leverantörer. Kammarkollegiets ramavtal är emellertid inte specifikt inriktade på de e-legitimations- och underskriftssystem som numera används och de är inte heller avgränsade till funktioner för e-legitimering och e-underskrift. Det aktuella ramavtalet (se nedan PT14-IF) är mycket brett till sitt omfång och utgör i många hänseenden mer ett kommersiellt ramverk än en konkret kravställning av specifika tjänster. Även om det finns exempelavrop och specifikationer, ställer avrop på ramavtalet således höga krav på förlitande part att själv konkretisera och specificera kravställningen, även

[73] Aktörer som tidigare agerat endast som underleverantör åt förlitande part träder här in i en roll som ansvarig för underskriftscertifikatet. Avtalen reglerar ofta knapphändigt vem som, gentemot förlitande part, svarar för den e-legitimation som använts för aktivering och det identitetsintyg som leverantör av identitetsintyg utfärdat åt leverantören av underskriftstjänst.

[74] Detta gäller särskilt för de höga krav på informationssäkerhet som är en nödvändighet för att tilliten till systemet ska kunna upprätthållas.

[75] Det är för närvarande i många fall oklart vilka urkunder som upprättas och bevaras så att de kan åberopas i händelse av en tvist.

med avseende på hur tjänsterna ska fungera juridiskt vid e-legitimering eller e-underskrift. Se följande sammanställning av E-legitimationsnämnden av vad ramavtalen täcker och hur de kombineras.

1. E-tjänst/er	2. Integrations-tjänst/er	3. eID-tjänst/er	Kommentar
E-tjänst /id-portal (internt eller externt förvaltad)	Intygstjänst Underskriftstjänst	Bank ID-teknik Teliateknik	
{EFST2010}*	{EFST2010}*	{eID 2008}**	* Gamla avtal ** Gamla avtal
Egen regi	Egen regi	eID 2016***	
PT14-IF****	PT14-IF****	eID 2016***	Avtalen kan kombineras
Egen regi	PT14-IF****		PT14-IF kan avropas för två av tre tjänster
PT14-IF****			Kan avropas för alla tjänster
Egen upphandling			Ytterligare kombinationer är möjliga

* EFST2010 = äldre ramavtal om e-förvaltningsstödjande tjänster (Kammarkollegiet)
** eID2008 = äldre ramavtal vars sista avropsavtal löper ut (Kammarkollegiet)
*** eID 2016= E-legitimationsnämndens valfrihetssystem eID 2016 Övergångstjänst. Täcker BankID och Telia. Täcker även BankID:s och Telias möjliga del i underskriftsflödet.
**** PT14-IF = aktuellt ramavtal via Kammarkollegiet; Programvaror och Tjänster Informationsförsörjning 2014

Diagram: E-legitimationsnämnden

7.20 Många leverantörer (till exempel CGI, Visma och Cybercom) tillhandahåller helhetslösningar där tillhörande avrop och kombinationer av avtal innefattar till exempel ett slags förlitandeavtal med leverantören, vilken agerar som en återförsäljare av förlitandetjänster som återförsäljaren upphandlat från till exempel en bank. De avtal som tecknas efter avrop omfattar dessutom vanligtvis ett antal andra tjänster.[76]

Komplexa avtalskonstruktioner och villkor

7.21 De regler som gäller för offentlig upphandling innebär att myndigheter måste förfara på visst sätt och inte fritt får välja leverantör av funktioner för e-legitimering, e-underskrift och anknytande hantering. I praktiken har detta fört med sig komplexa avtalskonstruktioner och villkor som gör det svårt att urskilja de beskrivna avtalstyperna och passa in dem bland de olika ramavtal från vilka myndigheter brukar avropa berörda tjänster.

Det har därmed blivit en utmaning för myndigheter som tillhandahåller e-tjänster att kontrollera om de avtal som tecknas tillgodoser de juridiska krav som myndigheten ställer i anknytning till sina e-tjänster; jfr checklistorna i kaptitel 13.

Det har också blivit en juridisk utmaning för upphandlande myndighet att utforma kompletterande dokumentation när upphandling ska ske genom förnyad

[76] Här framstår som delvis oklart vad de avtal som tecknas efter ett sådant avrop omfattar. Avtalen är i vart fall inte avgränsade till leverans av funktioner för e-legitimations- och underskriftssystem. Som beskrivits är det idag vidare delvis oklart vad som gäller för de särskilda underskriftscertifikaten och hanteringen av dem samt den kedja av parter och urkunder som är berörda av en underskrift. Liknande komplikationer uppkommer vid avrop av den särskilda övergångstjänsten. I vissa fall har de tekniska kraven enligt avtal en hög detaljeringsgrad utan att de juridiska kraven kommit till uttryck, i andra fall är även de tekniska specifikationerna starkt begränsade. Berörda upphandlingar förefaller i vissa delar vara utformade som om det var fråga om rena tekniska tjänster, trots att det huvudsakliga syftet är att etablera juridiskt anpassade och säkra funktioner för rättshandlingar där hanteringen avses vara baserad på att aktörerna åtar sig att följa avtalsvillkor som säkerställer avsedda rättsverkningar och fördelar ansvaret på ett balanserat och heltäckande sätt.

konkurrensutsättning och att bedöma om helheten tillgodoser myndighetens juridiska krav. Till detta kommer att två olika upphandlingar – och därmed två olika kravställningar – kan behöva göras om en myndighet ska införa en sådan underskriftstjänst där aktivering sker indirekt och särskilt underskriftscertifikat ska utfärdas.

Civilrättsligt ansvar vid E-legitimering

Avtalet om eget utrymme

7.22 En förlitande part som förser användare med eget utrymme bör genom avtal ansvara för att skydda utrymmet och tillhandahålla tjänsten på ett ändamålsenligt sätt, så som närmare beskrivs i eSams publikation, Eget utrymme hos myndighet – en vägledning. Även användarens ansvar bör regleras genom avtalet.

> *Att tänka på:* I avtalet om eget utrymme kan också behövas information eller villkor om hur användaren får bruka sin e-legitimation; till exempel att inte möjliggöra tillträde för annan under sken av att vara innehavare av e-legitimationen.

E-legitimationsavtalet

7.23 Utfärdare av e-legitimation bör enligt avtalet ansvara för att utfärdandet och tillhörande hantering sker på ett tillräckligt säkert sätt. Användaren bör enligt avtalet skydda sin e-legitimation och använda den endast enligt vissa regler.

> *Att tänka på:* Regler kan behövas i e-legitimationsavtalen som tydliggör rättsverkningarna av till exempel en legitimering för uppgiftslämnande eller för underskrift.

Förlitandeavtalet

7.24 Leverantör av identitetsintyg bör, enligt förlitandeavtalet, ansvara för sin e-identifierings- och intygshantering. Vid indirekt leverans av identitetsintyg bör leverantören av identitetsintyg även kontrollera att intyg från bakomliggande leverantörer är äkta och att bakomliggande leverantörer utför sina uppgifter på ett fackmannamässigt sätt. Leverantören av identitetsintyg bör, gentemot förlitande part, ansvara även för fel vid e-identifiering och utfärdande av identitetsintyg som bakomliggande utfärdare av e-legitimation eller leverantör av identitetsintyg har orsakat.[77] Förlitandeavtalet bör också innehålla sedvanliga avtalssanktioner vid brister i leverantörens uppfyllnad av felansvaret.

> *Att tänka på:* Enligt avtalet bör endast sådana e-legitimationer godtas som ger den tillitsnivå förlitande part kräver för berörd e-tjänst och endast sådana leverantörer som utför sina uppgifter på ett fackmannamässigt sätt. Avtalet bör kräva att en legitimeringsfunktion för berörda e-legitimationer har tydliga användargränssnitt och förklarande texter så att betydelsen och rättsverkningarna av en användning inte kan missförstås. Det bör i förlitandeavtalet krävas att Leverantör av identitetsintyg eller utfärdaren av den e-legitimation som använts e-stämplar sina identitetsintyg så att de får urkundskvalitet. Vissa minimikrav på e-legitimationsavtalens innehåll kan också övervägas genom villkor i förlitandeavtal.

[77] Här kan också det alternativet förekomma att förlitande part sluter ett särskilt avtal med en utfärdare av e-legitimation eller en bakomliggande leverantör av identitetsintyg där detta ansvar regleras direkt mellan parterna.

En övergripande sammanställning av vissa risker

7.25 Följande sammanställning ger från juridiska utgångspunkter en bild av några av riskerna vid e-legitimering.[78] Varje organisation behöver genomföra en analys för att bedöma i vilken utsträckning dessa, och andra, risker föreligger. Bristfällig förvaring av kort, koder och liknande samt vilseledande av användare är sådant som inträffat och dokumenterats.

Åtgärd	Risk för fel/missbruk	Möjlig ansvarig
Felaktigt utfärdad e-legitimation	Vilseledande så att e-leg utfärdas i annans namn	Utfärdare av e-legitimation
Oaktsamhet med e-leg och kod	Vilseledande genom att bruka annans e-leg	Gärningsmannen (Innehavaren)
Användaren legitimerar sig – annan släpps in	Myndigheten vilseleds att släppa in någon i strid mot OSL eller egen policy för e-tjänsten	Innehavaren/den som släpps in för brott vid användning/tillträde
Fel i legitimeringsbegäran	Tekniskt fel i e-tjänsten (helt automatiserat)	Förlitande part
Fel i legitimeringsfunktion	Fel text i användargränssnittet eller tekniskt fel	Utfärdare av e-legitimation
Direkt leverans: Fel vid e-identifiering, i intyg eller vid stämpling	Tekniskt fel (helt automatiserat) – om fel i utfärdad e-leg eller oaktsamt hanterad e-leg, anses fel inte ha begåtts i detta led (metodansvar)	Leverantör (direkt) av identitetsintyg
Indirekt leverans: Fel vid kontroll av bakomliggande intyg – fel vid konvertering eller i slutligt intyg	Tekniskt fel (helt automatiserat) – fel i något led ovan, inte fel i detta led (metodansvar)	Leverantör (indirekt) av identitetsintyg
Litar på felaktigt intyg	Var och en av felen ovan kan vara orsak	Någon av dem ovan

Civilrättsligt ansvar vid e-underskrift

Avtalet om eget utrymme, e-legitimationsavtalet och förlitandeavtalet

7.26 Ansvar bör gälla civilrättsligt enligt 7.22-7.24.

Avtalet om underskriftstjänst

7.27 Leverantör av underskriftstjänst bör, vid direkt underskrift, ansvara för att identifiera undertecknaren, motta och hantera det underlag som tekniskt ska skrivas under och producera underskriften och ett intyg om underskriftens äkthet samt sända materialet till förlitande part. Om den e-legitimation som har använts vid undertecknandet är utställd av annan än leverantör av underskriftstjänst, bör den leverantör av underskriftstjänst som förlitande part slutit förlitandeavtal med, ansvara även för fel som en bakomliggande utfärdare av e-legitimation har orsakat. Avtalet om underskriftstjänst bör också innehålla sedvanliga avtalssanktioner vid brister i leverantörens uppfyllnad av felansvaret.

Här uppkommer ett antal komplicerade frågor om en balanserad fördelning av risker, som det inte finns utrymme för att närmare redovisa i denna vägledning.

7.28 Vid indirekt underskrift bör leverantör av underskriftstjänst enligt avtalet ansvara för de åtgärder som närmare beskrivs i 5.16 (att motta identitetsintyget, kontrollera att det är äkta, ställa ut särskilt underskriftscertifikat, framställa en underskrift, kontrollera underskriften, ställa ut ett intyg om att underskriften är äkta och sända intyg och underskrift till användarens eget utrymme).

[78] Färgade fält visar funktioner där personer ser något och kan vilseledas medan vita fält rör risker vid helt automatiserade förlopp.

Leverantören bör, gentemot förlitande part, svara för fel som bakomliggande utfärdare av e-legitimation eller leverantör av identitetsintyg (för underskrift) har orsakat (jfr 7.24).

> *Att tänka på:* Avtalet bör kräva att leverantör av identitetsintyg och utfärdaren av den e-legitimation som använts stämplar sina intyg så att de får urkundskvalitet. Kontrollera att leverantören av underskriftstjänst svarar för fel vid e-identifiering, framställning av underskrift och utfärdande av intyg. Se till att en aktörs ansvar (till exempel utfärdare av e-legitimations ansvar) inte helt upphör i senare led, så att förlitande part står utan ersättning till följd av fel av den bakomliggande aktören. Denne bör kunna begära ersättning från sin avtalspart som i sin tur får vända sig mot den bakomliggande aktören.[79]

En sammanställning av risker

7.29 Följande sammanställning ger en bild av några av riskerna vid e-underskrifter.[80] Varje organisation behöver genomföra en analys för att bedöma i vilken utsträckning dessa, och andra, risker föreligger.

Åtgärd	Risk för fel/missbruk	Möjlig ansvarig
Felaktigt utfärdad e-legitimation	Vilseledande så att e-leg utfärdas i annans namn	Utfärdare av e-legitimation
Oaktsamhet med e-leg och kod	Vilseledande genom att bruka annans e-leg	Gärningsmannen (Innehavaren)
Fel text skrivs under	I e-tjänsten visas fel handling för underskrift	Förlitande part
Felaktigt underlag, se 5.7	Tekniskt fel vid skapandet (helt automatiserat)	Förlitande part
Fel i legitimeringsfunktion	Visar fel förklarande text (till exempel Jag legitimerar mig)	Utfärdare av e-legitimation
Identifierings- och intygsfunktionen gör fel i intyg för indirekt underskrift	Tekniskt fel (helt automatiserat) – om fel i utfärdad e-leg eller oaktsamt hanterad e-leg, anses fel inte ha begåtts i detta led (metodansvar)	Leverantör av identitetsintyg
I underskriftstjänst sker - fel vid e-identifieringen - felgjort underskriftscert - felgjord underskrift	Tekniskt fel (helt automatiserat) – fel i något led ovan, inte fel i detta led (metodansvar)	Leverantör av underskriftstjänst/ Förlitande part
Sammanfoga urkund fel	Tekniskt fel (helt automatiserat)	Förlitande part
Litar på falsk urkund	Var och en av felen ovan kan vara orsak	Inom eller utom kontrakt?

Metodansvar och bevisning

7.30 Det civilrättsliga ansvaret för en leverantör bör vara utformat som ett metodansvar (inte ett resultatansvar) eftersom ansvaret begränsas till att hantera vissa funktioner med omsorg och noggrannhet på sätt som närmare anges i avtal mellan parterna.

> *Att tänka på:* Den begränsade dokumentation, som i många fall visat sig finnas av procedurerna för e-legitimering och e-underskrift, kan göra det svårt att utforma en ansvarsbegränsning som bygger på ett metodansvar.

[79] Här kan också det alternativet förekomma att förlitande part sluter ett särskilt avtal med en utfärdare av e-legitimation eller en bakomliggande leverantör av identitetsintyg där detta ansvar regleras direkt mellan parterna.
[80] Färgade fält visar funktioner där personer ser något och kan vilseledas medan vita fält rör risker vid helt automatiserade förlopp.

7.31 Vid en tvist räcker det inte att klargöra vad som är gällande rätt. Parter behöver också kunna bevisa vad de påstår eftersom de regelmässigt har olika uppfattning om vad som har ägt rum. Det blir därför av betydelse att kunna presentera hållbar bevisning i de avseenden som en motpart ifrågasätter en handlings äkthet, jfr kapitel 10 om bevarande.

> *Att tänka på:* Förlitande part bör, genom villkor i förlitandeavtal och avtal om underskriftstjänst, ges rätt att begära in kompletterande information från leverantören om uppgifter finns bevarade av denne och uppgifterna krävs för att en underskrifts äkthet har ifrågasatts. Förlitande part behöver också överväga eventuella krav på bevarande av sådana uppgifter som är nödvändiga för att kontrollera en underskrifts äkthet. Sådana villkor bör utformas med tanke på att material kan bli att anse som allmän handling hos förlitande part.

8. MISSBRUK OCH STRAFFRÄTTSLIGT ANSVAR

I detta kapitel beskrivs vissa manipulationer med och missbruk av e-legitimationer som har börjat förekomma och vilka bestämmelser om straffansvar som kan bli tillämpliga.

Gällande rätt

Brotten mot urkunder

8.1 Efter en ändring år 2013 i brottsbalken (BrB) gäller en ny definition av urkund som innebär att en urkund i elektronisk miljö är en elektronisk handling som upprättats till bevis eller annars är av betydelse som bevis och som har en utställarangivelse som kan kontrolleras på ett tillförlitligt sätt (14 kap. 1 § BrB).[81]

Den nya regleringen innebär att brotten mot urkunder har sträckts ut till e-underskrivna och e-stämplade handlingar. Straffansvaret omfattar både urkundsförfalskning och de s.k. sanningsbrotten där äkta urkunder ges ett osant innehåll eller används på ett missvisande sätt. Följande bestämmelser är av särskilt intresse.

8.2 Enligt 14 kap. 1 § BrB döms den som obehörigen framställer en falsk urkund för urkundsförfalskning.

Exempel: A skriver under en elektronisk handling i anknytning till en e-tjänst med hjälp av en e-legitimation på kort och ett lösenord antecknat på en papperslapp. A har funnit kort och lösenord i en stulen plånbok. E-legitimationen är inte utställd för A, som därför obehörigen producerar en annan persons e-underskrift och därmed en falsk urkund.

8.3 Enligt 15 kap. 13 § BrB döms den som förnekar sin underskrift på en urkund eller sin utställarangivelse avseende en urkund, när angivelsen är sådan att den kan likställas med en underskrift, för förnekande av underskrift.

Exempel: B har legitimerat sig för underskrift i anknytning till en tjänst för företagsregistrering men hävdar därefter felaktigt att någon annan har startat funktionen för underskrift och att ingiven ansökan därför är förfalskad.

8.4 Av 15 kap. 10 § BrB följer att den som på annat sätt än muntligen lämnar osann uppgift eller förtiger sanningen, när uppgiften enligt lag eller annan författning lämnas på heder och samvete eller under annan liknande försäkran, döms för osann försäkran.

[81] Utgångspunkten för dessa lagändringar var enligt lagmotiven att straffskyddet för uppgifter och handlingar som förekommer i elektronisk miljö – till exempel i ett elektroniskt intyg – bör likna det som gäller för traditionella handlingar (prop. 2012/13:74 s. 1).

Exempel: C försäkrar osant, i anknytning till en e-tjänst, vissa uppgifter som enligt lag ska lämnas på heder och samvete. Även om uppgifterna inte varit undertecknade elektroniskt hade bestämmelsen om straffansvar kunnat bli tillämplig, till exempel efter e-legitimering för uppgiftslämnande.

8.5 I 15 kap. 11 § första stycket BrB föreskrivs att den döms för osant intygande som i ett intyg eller en annan urkund (även en elektronisk) lämnar osann uppgift om (1) vem han eller hon är, (2) om annat än egna angelägenheter eller (3) för skens skull upprättar en urkund rörande rättshandling. Även den som åberopar eller på annat sätt använder en sådan osann urkund kan dömas till ansvar. – De två första fallen och brukandet är av intresse inom e-förvaltningen. Straffansvaret omfattar även medverkan och anstiftan till brottet.

Exempel: D legitimerar sig för tillträde med sin kollegas e-legitimation och anstiftar därmed den som ställer ut intyg om vem som har legitimerat sig till att osant intyga att det är kollegan (utställaren av intyget saknar uppsåt). – Samtidigt brukar D osant identitetsintyget för att få tillträde i kollegans namn.

8.6 Enligt 15 kap. 12 § första stycket BrB ska den ska dömas för missbruk av urkund som sanningslöst åberopar pass, betyg, identitetshandling eller annan sådan för enskild person utställd urkund såsom gällande för sig eller annan person eller lämnar ut sådan urkund för att missbrukas på det sättet. – Begreppet urkund omfattar numera även e-underskrivna eller e-stämplade e-legitimationer och andra elektroniska intyg.

Exempel: E har legitimerat sig för tillträde hos myndighet M med användning av sin kollegas e-legitimation. E har därmed sanningslöst åberopat kollegans e-legitimation såsom gällande för sig. Även kollegan har gjort sig skyldig till brott genom att lämna sin e-legitimation och kod till denne för att missbrukas på det sättet.

8.7 Enligt 15 kap. 12 § tredje stycket BrB döms den för missbruk av handling som sanningslöst utger en handling för att vara en riktig kopia av en viss urkund.

Exempel: Myndighet M begär att få en elektronisk kopia av en viss originalhandling från F. M anger att det inte krävs att den elektroniska kopian vidimeras (eftersom F och M inte har någon teknisk lösning för hantering av en vidimering och kontroll av den). F gör en elektronisk kopia av den begärda handlingen. Kopian innehåller en fullständig avbild av originalet med dess layout återgiven. F ändrar emellertid i innehållet och skickar därefter kopian till M i sådan form att den ser ut som en riktig kopia av originalet. F gör sig därför skyldig till missbruk av handling.

Dataintrång och brott mot tystnadsplikt

8.8 Enligt 4 kap. 9 c § BrB ska den som olovligen har berett sig tillgång till uppgift som är avsedd för automatiserad behandling dömas till ansvar för dataintrång.

Exempel: G legitimerar sig med sin kollega K:s e-legitimation och släpps därmed in i en e-tjänst med eget utrymme så att G där får del av sekretessbelagd information om K. Myndighet M släpper in G i tron att det är K som begär tillträde. G får därmed tillgång till uppgifter utan lov av myndighet M. Eftersom det är M som bestämmer om G ska ges elektronisk tillgång till uppgifterna kan K:s samtycke i förening med ett vilseledande om vem som släpps in inte utgöra lovlig tillgång till information i dataintrångsbestämmelsens mening.

8.9 Lämnas uppgifter som omfattas av sekretess ut av en myndighet till någon för vilken uppgifterna inte får röjas kan ansvar inträda enligt 20 kap. 3 § BrB för brott mot tystnadsplikt. Sker utlämnandet till följd att en e-legitimation missbrukas av annan (en individ brukar annans e-legitimation för att ge sig ut för att vara denne) har myndighetens företrädare inte uppsåt till gärningen och har normalt inte heller förfarit oaktsamt. Däremot kan ansvar komma i fråga för den som missbrukat eller medverkar vid missbruk av e-legitimationen och på detta sätt uppsåtligen främjat gärningen (det otillåtna utlämnandet).

Exempel: H befinner sig i sin bostad. Telefonförsäljare P befinner sig på sin arbetsplats och förmår vid ett samtal H att legitimera sig med mobilt BankID. P har redan skrivit in H:s personnummer i en e-tjänst för att bli inloggad som om han vore H. När P loggats in under sken av att vara H får P ut sekretessbelagd information som myndigheten på föreliggande underlag inte äger rätt att lämna ut till P.

Olovlig identitetsanvändning

8.10 Enligt 4 kap. 6 b § BrB ska den som genom att olovligen använda en annan persons identitetsuppgifter utger sig för att vara honom eller henne och därigenom ger upphov till skada eller olägenhet för honom eller henne, döms för olovlig identitetsanvändning.

För ansvar behöver inte någon viss urkund eller annan handling ha använts. Missbruk av e-legitimationer synes inte ha berörts i lagstiftningsärendet. För straffbarhet krävs att den person vars identitetsuppgifter används har drabbats av skada eller olägenhet.

Straffskydd vid felaktig e-legitimering och e-underskrift

Myndigheter bör öka tilliten till systemen genom att ta tillvara det straffrättsliga skyddet

8.11 Riskerna för missbruk vid e-legitimering och e-underskrift har tekniskt minimerats genom olika skyddsåtgärder som hittills fungerat väl. Mindre nogräknade aktörer har istället inriktat sig på att antingen försöka komma över användares lösenord och e-legitimation för att missbruka dem eller förmå användare att medvetet eller omedvetet använda sin e-legitimation felaktigt så att identitetsintyg eller e-underskrivna handlingar missbrukas av en annan person.

> *Att tänka på:* Missbruk av en e-legitimation genom att vilseleda innehavaren kan normalt inte förhindras tekniskt. Därför bör förlitande parter utforma sina e-tjänster så att beskrivet straffrättsligt skydd tas tillvara fullt ut.

En endast delvis anpassad hantering av intyg och bristande information

8.12 Förlitandeavtalet för den särskilda övergångstjänsten har utformats så att leverantörerna ska lämna identitetsintyg. Av avtalet framgår emellertid inte om intygen ska vara stämplade av leverantören så att de ges urkundskvalitet.

> *Att tänka på:* Vid tecknande av förlitandeavtal bör en myndighet eftersträva att få identitetsintyg som är e-stämplade med någon av leverantörernas elektroniska stämpel. Vid direkt leverans stämplas intyget av en aktör som utfärdar e-legitimationer medan intyget, vid leverans indirekt från en annan leverantör, stämplas av den andra leverantören med dennes e-stämpel (se 4.11).
>
> – De funktioner som är mest frekvent använda har dock visat sig bygga på att den som legitimerar sig skriver under sina egna uppgifter och att utfärdare av e-legitimation (inte leverantör av identitetsintyg) e-stämplar ett intyg om att användarens e-legitimation inte har spärrats vid det aktuella tillfälle. Den som legitimerar sig har här inte kännedom om att han eller hon skapar ett intyg med uppgifter om sin egen identitet. Samtidigt är de uppgifter som förlitande part tar emot och i praktiken använder för sin kontroll av vem användaren är inte e-underskrivna eller e-stämplade. Förlitande myndigheter bör uppmärksammas på detta.

8.13 Kunskap om vad som gäller enligt 14 och 15 kap. BrB vid e-legitimering och e-underskrift är inte spridd. Därför behöver användare tydlig information om det ansvar som föreskrivs för till exempel urkundsförfalskning, förnekande av underskrift, osant intygande och missbruk av urkund genom att ge sig ut för att vara någon annan. E-tjänster och användargränssnitt behöver anpassas så att straffskyddet för urkunder tas tillvara fullt ut.

> *Att tänka på:* Dagens hantering innebär visserligen att e-underskrifter och e-stämplar skapas rent tekniskt. Den som inom övergångstjänsten legitimerar sig vet emellertid inte om att han eller hon ”skriver under” ett slags urkund om sin identitet. Användargränssnittet är utformat så att användaren klickar på knappen ”Jag legitimerar mig”. Användaren upprättar således inte medvetet något intyg om vem han eller hon är och förlitande part känner normalt inte till att användaren skriver under sådana uppgifter.
> – Det kan visa sig att handlingar som har stämplats eller skrivits under utan att utställare eller förlitande part känner till detta inte anses ha den betydelse som bevis som krävs enligt 14 kap. 1 § BrB.[82] – Den som uppsåtligen använder annans e-legitimation har emellertid sanningslöst åberopat e-legitimationen såsom gällande för sig hos leverantör av identitetsintyg. Ansvar enligt 15 kap. 12 § BrB kan därmed komma i fråga för missbruk av urkund.

Handlingar som har stämplats eller skrivits under

8.14 Identitetsintyg som en myndighet litar på efter e-legitimering för indirekt leverans är normalt försedda med en e-stämpel som leverantör av identitetsintyg ställt ut efter att ha mottagit och kontrollerat en direkt leverans. En indirekt leverantör av identitetsintyg e-stämplar denna information, medveten om syftet med detta, och förlitande part brukar intyget och kontrollerar dess äkthet.

[82] Den information som förlitande part i praktiken använder efter en legitimering för direkt leverans (se 4.11) saknar vanligtvis urkundskvalitet eftersom den varken är e-underskriven eller e-stämplad. Visserligen uttalade IT-förfalskningsutredningen i sitt betänkande Urkunden I Tiden – en straffrättslig anpassning (SOU 2007:92 s. 129) att det straffrättsliga skyddet inte skulle vara begränsat till att endast omfatta elektroniskt underskrivna handlingar och att det även kan finnas handlingar som inte har en sådan utställarangivelse inom handlingen, men som ändå finns i en sådan miljö och tillkommit under sådana omständigheter att de förtjänar tilltro. Detta uttalande återfinns emellertid inte i propositionen. Det kan dessutom ifrågasättas om den momentana kontrollen vid överföring inom det aktuella systemet kan anses tillräcklig för att översänd information ska anses ha urkundskvalitet.

Exempel: Bedragare B använder den oskyldige O:s e-legitimation för att felaktigt få tillträde till O:s eget utrymme med känslig information. B har informerats om förfarandet så att han förstår att han därmed underförstått åberopar O:s e-legitimation genom ett e-stämplat intyg som anger att O begär att få tillträde. B har därmed sanningslöst åberopat e-legitimationen och det e-stämplade identitetsintyget såsom gällande för sig (15 kap. 12 § BrB). Dessutom resulterar e-legitimeringen i att leverantören av identitetsintyget ställer ut ett osant intyg om vem som har legitimerat sig (15 kap. 11 § BrB).

Exemplet kan varieras: I praktiken kan exempelvis Mobilt BankID användas för att logga in på en valfri dator (till exempel en som tillhandahålls åt användaren på ett hotell) genom att användaren legitimerar sig med en app på sin mobila enhet. B har börjat missbruka denna teknik genom att övertala innehavare av e-legitimation att medvetet legitimera sig för att B eller B:s robot ska kunna begära tillträde under sken av att vara den som anges i e-legitimationen. Ibland lurar B också innehavare av e-legitimation att begära tillträde för B eller B:s robot genom att innehavaren av e-legitimation legitimerar sig ovetande om att B eller B:s robot skrivit in B:s personnummer på en viss webbsida.
– Användarens samtycke till eller fullmakt för den som felaktigt släpps in fritar inte från ansvar eftersom straffansvar föreskrivs för den som sanningslöst åberopar identitetshandling eller annan sådan för enskild person utställd urkund såsom gällande för sig eller lämnar ut sådan urkund för att missbrukas på det sättet.

8.15 En förutsättning är vidare att den som legitimerar sig eller skriver under verkligen besöker den webbsida (domänadress) som han eller hon tror och inte en bluffsida, där användaren vilseleds att lämna ut uppgifter eller vidta åtgärder för legitimering eller underskrift som medför att informationssäkerheten kan brytas igenom.

Det tekniska och administrativa skydd som ges för domänadresser och webbsidor genom att en bild av ett hänglås visas vid domänadressen och att texten för denna adress blir grön används inte konsekvent. De förklarande texterna och innehållet i certifikat som en användare kan ta del av bör göras begripliga även för användare som inte har särskild kompetens inom området.

8.16 Det finns alltså vissa brister från tekniska, administrativa och straffrättsliga utgångspunkter i dagens e-legitimations- och e-underskriftssystem. Myndigheter som tillhandahåller e-tjänster bör därför överväga de tekniska och administrativa lösningarna så att identitetsintyg och intyg om att en underskrift är äkta ges urkundskvalitet.

Myndigheter och leverantörer behöver lämna information till användare och förlitande parter så att de förstår att urkunder och intyg ställs ut och att förfalskningar och missbruk av sådana urkunder kan utgöra brott.

Rapporteringsskyldighet

8.17 Manipulationer och missbruk av beskrivet slag kan utgöra sådana it-incidenter som statliga myndigheter ska rapportera till MSB enligt 20 § förordning (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap.

Brottsliga förfaranden bör polisanmälas.

9. HUR SÄKRAS INFORMATIONEN?

Förtroendet för att en e-tjänst där e-legitimering och e-underskrift används är säker blir av central betydelse för att tjänsten ska nyttjas i önskad utsträckning. Detta förtroende bygger i grunden på att:

- **obehöriga inte ska få tillgång till informationen**
- **informationen inte kan ändras på ett obehörigt sätt**
- **tjänsten är tillgänglig för användaren**
- **det är spårbart vem som har gjort vad och när**

För att kunna uppfylla dessa krav behövs ett systematiskt informationssäkerhetsarbete så att det inte uppstår luckor som kan nyttjas för missbruk och manipulationer. I detta kapitel beskrivs hur ett sådant arbete kan bedrivas med stöd av ett Ledningssystem för informationssäkerhet (LIS).

Ett systematiskt informationssäkerhetsarbete

9.1 Alla ingående komponenter i en e-tjänst och tillhörande infrastruktur, såsom system och tjänster för e-legitimering och e-underskrift, måste ha en tillräckligt hög nivå av säkerhet för att kunna skydda den information som hanteras i och kring e-tjänsten.

På samma sätt som ledningen i organisationen behöver styra och tillsätta resurser för arbetet med att införa e-legitimationer och e-underskrifter behöver ledningen se till att säkerhetsfrågorna beaktas. Ett ledningssystem för informationssäkerhet (LIS) är ett sätt för organisationens ledning att på ett systematiskt sätt styra arbetet med informationssäkerhet i syfte att planera, genomföra, kontrollera, följa upp, utvärdera och förbättra säkerheten i verksamhetens informationshantering. Skyddet för e-tjänster och stödsystem och tillhörande infrastruktur är en del i detta arbete.

Statliga myndigheter är skyldiga att bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av ett ledningssystem för informationssäkerhet.[83] Samtliga organisationer som hanterar information som behöver skyddas avseende konfidentialitet, riktighet, tillgänglighet och spårbarhet har dock behov av ett LIS utformat för att passa den egna verksamheten. Ytterligare information och praktiskt metodstöd för detta arbete finns på https://www.informationssäkerhet.se.

Klassificera informationen

9.2 I syfte att säkerställa ett väl avvägt skydd för informationen och att kunna identifiera och hantera risker behöver organisationen som ett första steg klassificera den information som hanteras med utgångspunkt i konfidentialitet,

[83] Myndigheten för samhällsskydd och beredskaps Föreskrifter (MSBFS 2016:1) om statliga myndigheters informationssäkerhet.

riktighet och tillgänglighet i olika nivåer utifrån vilka konsekvenserna kan bli om skyddet brister. Klassificeringen kan även omfatta spårbarhet, eller andra aspekter, där så behövs. Därefter behöver de hot som riktas mot information, system och tjänster identifieras och analyseras för att på så sätt kunna bedöma aktuell risknivå. En sådan riskanalys för en e-tjänst behöver innefatta hela den kedja av behandlingar som är aktuella.

Vidta åtgärder

9.3 Utifrån informationsklassificeringens resultat och den genomförda riskanalysen identifieras och vidtas därefter de tekniska och organisatoriska åtgärder som krävs för att uppfylla skyddsbehovet. Exempelvis behöver tekniska metoder för tillträdesbegränsning och behörighetskontroll införas. Krypteringsmekanismer för att ge skydd mot obehörig insyn och förändring kan också behövas. Det systematiska informationssäkerhetsarbetet innebär även att vidtagna åtgärder och gjorda bedömningar följs upp och utvärderas. Detta görs för att kontinuerligt utveckla skyddet för att över tid upprätthålla behovet av informationssäkerhet.

Vidtagna åtgärder och gjorda bedömningar följs upp och utvärderas

En förenklad sammanfattning av vad ett LIS innefattar

9.4 Att arbeta systematiskt med informationssäkerhet är en förutsättning för att inte under- eller överarbeta säkerhetsåtgärder, att som organisation ha en överblick över området, att hålla ledningen uppdaterad om risker och att kunna prioritera bland de åtgärder som behöver införas. Följande åtta punkter kan ses som en lägsta nivå för systematiskt informationssäkerhetsarbete inom en organisation.

1. *Utse en funktion för informationssäkerhet.* Funktionens placering bör vara direkt underställd den högsta ledningen. För att på bästa sätt kunna arbeta med frågorna visar erfarenhet att funktionen behöver använda en majoritet av sin tid till informationssäkerhetsuppdraget. Funktionen behöver kontinuerligt kompetensutvecklas.
2. Det första funktionen bör göra är att *ta fram en analys av nuläget i organisationen.* Gör en övergripande verksamhetsanalys för att få kunskap om organisationens processer, vilken information som hanteras, samt vilket behov av skydd och vilka krav som finns. Gör därefter en övergripande analys för att få en bild av riskerna kopplade till den information som hanteras. Gör också en gap-analys genom en inventering av existerande säkerhetsåtgärder jämförda med skyddsbehovet som framkommit genom verksamhets- och riskanalysen. Här handlar det om att skapa en samlad bild om informationssäkerhetsnivån i organisationen. Det är viktigt för att kunna presentera läget för ledningen.
3. *Informera ledningen hur nuläget ser ut.* Visa exempel på reella hot och inträffade incidenter. Visa på förutsättningarna för säker digitalisering. Informationssäkerhetsområdet är ett komplext område och flera kompetenser behövs i arbetet.
4. *Skapa en handlingsplan utifrån nuläget.* Handlingsplanen bör beslutas av ledningen. Ta fram styrdokument, policy och riktlinjer samt åtgärda de viktigaste bristerna och sårbarheterna, t ex beredskap mot skadlig kod, backuprutiner etc.

5 Identifiera vilken information som hanteras i verksamheten. *Klassificera sedan informationen* efter hur allvarliga konsekvenserna skulle bli av bristande informationssäkerhet. Fokusera på den mest kritiska informationen/känsliga informationen som är i behov av höga skyddskrav. Ta här gärna hjälp av Metodstöd för LIS som är publicerat på https://www.informationssakerhet.se.

6 *Se till att höja säkerhetsmedvetandet inom organisationen* och stödja organisationens förmåga att efterleva kraven i framtagna riktlinjer. Detta kan ske till exempel genom utbildning och att ta fram vägledningar och annan information.

7 *Ta fram* informationssäkerhetsrelaterade *krav som sedan används vid upphandlingar.* Det är viktigt att få med informationssäkerhetskrav vid upphandling.

8 *Gör uppföljningar.* Se över om organisationen efterlever det som står i de framtagna riktlinjerna. Planera in återkommande uppföljning/revison av verksamheten. Resultaten av uppföljning ska ingå som en del av den återkommande rapporteringen till ledningen.

Säkerhetsåtgärder

9.5 Alla verksamheter behöver vidta vissa säkerhetsåtgärder för att ha en god informationssäkerhet. En säkerhetsåtgärd kan vara av karaktären fysisk (till exempel brandlarm och lås), administrativ (till exempel att styrande dokumentation finns och efterlevs), organisatorisk (till exempel tillräckliga personella resurser) eller teknisk (till exempel brandvägg och antivirus).

Säkerhetsåtgärder införs för att minska de risker som identifierats vid riskanalysen och gapanalysen (se 9.4 punkt 2). Genom att till exempel utgå från den katalog av säkerhetsåtgärder som anges i bilaga A av SS-ISO/IEC 27001:2014[84] kan en bruttolista upprättas över de säkerhetsåtgärder som kan behöva införas. – I denna vägledning nämns vissa sådana säkerhetsåtgärder men även andra åtgärder bör övervägas.

[84] Det finns även andra referensverk att utgå från för att identifiera tänkbara säkerhetsåtgärder, såsom NIST SP800-53 utgåva 4 (http://dx.doi.org/10.6028/NIST.SP.800-53r4).

10. VAD MÅSTE BEVARAS?

I samband med att e-tjänster införs, används, förändras och avvecklas behöver det bedömas vilken information om e-legitimationer och e-underskrifter som ska bevaras och vilken information som får tas bort från systemen. Frågan är av såväl juridisk som säkerhetsmässig betydelse där exempelvis behov av att spara valideringsdata är något som organisationen måste analysera.
Även om regleringen gäller myndigheter är de bakomliggande övervägandena av intresse också för andra organisationer. I detta kapitel redovisas översiktligt vad som gäller för bevarande och gallring vid e-legitimering och e-underskrift samt vilken inriktning som kan vara lämplig för hanteringen av dessa frågor. De säkerhetsmässiga aspekterna på bevarande behandlas i kapitel 2 och 9.

Arkivlagen

10.1 Allmänna handlingar bildar enligt arkivlagen myndighetens arkiv och ska bevaras. E-underskrivna handlingar och handlingar som produceras i anknytning till e-underskrift eller e-legitimering blir enligt 2 kap. tryckfrihetsförordningen allmänna när de kommer in till eller upprättas av en myndighet.

Sådana handlingar får gallras endast om det har stöd i lag, förordning eller föreskrifter eller beslut av en arkivmyndighet.[85] I praktiken behöver en statlig myndighet alltså ha stöd i föreskrifter eller beslut av Riksarkivet för att få gallra e-underskrivna handlingar eller andra handlingar som produceras vid e-underskrift eller e-legitimering. Finns särskilda regler om gallring i till exempel en s.k. registerförfattning gäller dock den regeln.

Den e-underskrivna handlingen ska bevaras i ursprungligt skick

10.2 Rätten till insyn enligt 2 kap. tryckfrihetsförordningen (TF) förutsätter att handlingar bevaras i ursprungligt skick, dvs. med det innehåll de hade vid den tidpunkt de inkom till eller upprättades vid myndigheten.[86] Är det fråga om en inkommen handling behöver dess ursprungliga skick vid den tidpunkt när den kom in till myndigheten fastslås.

Av arkivförfattningarna följer inget krav på att en myndighet ska införa elektroniska underskrifter eller motsvarande skydd för en handlings äkthet. Där ställs inte heller krav på att inkomna eller upprättade handlingars äkthet omedelbart ska kontrolleras eller att en myndighet ska hämta in bevis från andra aktörer för att säkerställa möjligheterna till kontroll på kort och lång sikt. Däremot måste de handlingar som faktiskt har kommit in till eller upprättats av en myndighet, till exempel inom ramen för en e-tjänst, bevaras om det inte följer av föreskrifter eller beslut att gallring får ske.[87]

---

[85] Riksarkivet är statlig arkivmyndighet (8 § arkivförordning) medan kommunstyrelsen är arkivmyndighet i en kommun och landstingsstyrelsen i ett landsting, om inte kommunfullmäktige eller landstingsfullmäktige har utsett någon annan nämnd eller styrelse till arkivmyndighet (8 § arkiv-lagen).
[86] Prop. 2001/02:70 s.35.
[87] Se Riksarkivets rapport (2006:1) Elektroniskt underskrivna handlingar, s. 31 f.

Tidpunkt för inkommande

10.3 En elektronisk handling är enligt 2 kap. 6 § TF att anse som inkommen till myndigheten när annan har gjort den tillgänglig för myndigheten på sätt som anges i 3 § andra stycket samma kapitel. I praktiken innebär detta normalt att en handling anses ha kommit in när den nått den funktion för automatiserad behandling som myndigheten har anvisat som mottagningsställe, dvs. mottagningsfunktionen i den tekniska infrastruktur som myndigheten använder.

En handling och dess delar

10.4 En inkommen underskriven handling består av själva handlingen. Till den hör valideringsdata. Vilka handlingar med valideringsdata som inkommer kan variera beroende på avtal och tjänst. De allmänna handlingar som uppkommer vid e-underskrift eller e-legitimering kan därför bestå av

- den handling som ingivaren sänt in (till exempel genom att fylla i ett formulär i sitt eget utrymme eller motsvarande, skriva under och skicka till myndigheten)
- valideringsdata (information om en underskrift eller en legitimering) bestående av till exempel
  - ett identitetsintyg
  - en e-underskrift
  - information om gällande certifikatkedjor,[88]
  - övrig metadata som till exempel ip-adresser samt uppgifter om teknisk utrustning och användare.

Handlingar med valideringsdata kommer in till en myndighet i flera till varandra relaterade filer, som kan vara sammanhållna i ett datapaket. Filerna representerar tillsammans de ursprungligen inkomna handlingarna.

Handlingens ursprungliga skick ska bevaras

Hade en handling visst format när den kom in till myndigheten utgör denna version handlingens ursprungliga skick. Det ska bevaras. Detta gäller även om myndigheten använder en konverterad kopia av handlingen i sin ärendehandläggning och bevarar både versionerna parallellt.

För beslutshandlingar som skrivits under elektroniskt inom myndigheten gäller ett likartat förfarande. Här är det dock tidpunkten för när beslutshandlingen upprättades som ska fastställas.

Uppgifter som tillkommer vid äkthetskontroll och stämpling

10.5 När en e-underskriven handling har kommit in till en myndighet kan ytterligare handlingar upprättas om till exempel utfallet av en äkthetskontroll och när den gjordes. Nya valideringsdata och handlingar upprättas dessutom om myndigheten stämplar en handling.

Riksarkivets föreskrifter om elektroniska handlingar

10.6 Riksarkivet har utfärdat föreskrifter och allmänna råd (RA-FS 2009:1) om elektroniska handlingar samt föreskrifter och allmänna råd (RA-FS 2009:2) om tekniska krav. Föreskrifterna kompletterar arkivförfattningarnas bestämmelser.

[88] Uppgifter om rotcertikatet, utfärdarens certifikat och användarens certifikat.

Bestämmelser som uttryckligen tar sikte på elektroniskt underskriva handlingar finns i 3 kap. 5 § RA-FS 2009:2 Där föreskrivs att elektroniska handlingar som är elektroniskt underskrivna, och som tillkommer inom ramen för e-tjänster, ska följa: PKCS #7: Cryptographic Message Syntax Version 1.5, eller XML-signaturs för strukturerade dokument i XML (Extensible Markup Language). I övrigt gäller samma bestämmelser som för handlingar som inte är elektroniskt underskrivna. Det innebär att alla delar ska finnas kvar som behövs för att upprepat kunna presentera, förstå och bedöma en handlings trovärdighet över den tid handlingen ska bevaras och skyddas mot förstörelse eller förvanskning.

Riksarkivets föreskrifter anger också vilken planering och vilka åtgärder i övrigt som myndigheten ska eller bör vidta. Som allmänna handlingar ska e-underskrivna handlingar redovisas enligt Riksarkivets föreskrifter och allmänna råd om arkivredovisning (RA-FS 1991:1 senast ändrad RA-FS 2008:4).

Stämpling som kompletterande åtgärd vid bevarande av e-underskrivna handlingar

10.7 När en e-underskriven handling kommer in till en myndighet sker det med stöd av en hel infrastruktur. Det är inte rimligt att en myndighet ska hämta in, bevara och upprätthålla hela den ursprungliga infrastruktur, som behövs för att kontrollera underskrifters äkthet i efterhand, som i allt högre uträckning skapas hos leverantörer som myndigheten förlitar sig på och har avtal med. Istället bör myndigheten fokusera på att beskriva och dokumentera processen för e-underskrivna handlingar och berörda avtal. Sett till de handlingar som uppkommer i processen behöver myndigheten bevara själva handlingen inklusive bilagor (ingivarens uppgifter) de valideringsdata som kom in med den underskrivna handlingen (identitetsintyget m.m.) och utfallet av de äkthetskontroller (jämförelse av checksummor för de dokument eller filer som kontrolleras) som myndigheten gjort av de inkomna handlingarna. Vill myndigheten gallra någon av dessa handlingar behöver en framställning göras till Riksarkivet.

Det kan uppkomma situationer där myndigheten i efterhand behöver bevisa både att den e-underskrivna handlingen är äkta och att dokumentation av utfallet av de äkthetskontroller som gjorts inte har förvanskats.

Som en kompletterande åtgärd vid bevarande av e-underskrivna handlingar kan myndigheten även stämpla handlingen och dess valideringsdata med myndighetens elektroniska stämpel. Syftet med en sådan stämpling är att visa att myndigheten har utfört en äkthetskontroll när handlingen inkom, vad utfallet av kontrollen blev och att informationsinnehållet inte har ändrats efter det att kontrollen gjordes.

Detta material kan över tid lagras så att det går att visa om handlingen eller kontrollmaterial har ändrats efter det att äkthetskontrollerna gjordes.[89]

Behovet av att stämpla de elektroniskt underskrivna inkomna handlingarna och dokumentationen av utfallet av de äkthetskontroller som myndigheten gjort måste bedömas av myndigheten själv, där till exempel bevarandetider och det ekonomiska eller symboliska värdet av att kunna påvisa en handlings äkthet tas med i bedömningen, se vidare Juridisk checklista för bevarande och gallring i kap. 13.

[89] Riksarkivet berör i en rapport den 29 maj 2015 från Arkiv E – Delprojekt 3: Framställning och bevarande av elektroniska signaturer (avsnitt 6), metoden med myndighetsstämpling och för även ett resonemang om att stämplingen kan behöva upprepas över tid (s.k. rekursiv stämpling).

Att utreda och formalisera gallring

10.8 Enligt 4 kap. 4 § Riksarkivets föreskrifter och allmänna råd (RA-FS 2009:1) om elektroniska handlingar ska myndigheter fortlöpande pröva förutsättningarna för gallring av elektroniska handlingar. I de föreskrifter om bevarande och gallring som Riksarkivet har utfärdat berörs inte specifikt e-underskrivna handlingar. En myndighet måste därför själv utreda förutsättningarna för om och när sådan gallring kan ske. Myndigheten behöver vid sin gallringsutredning värdera de e-underskrivna handlingarna och tillhörande valideringsdata utifrån dessa kriterier.

När gallring inte kan ske genom en tillämpning av föreskrift av Riksarkivet och inte heller inom ramen för en registerförfattning, behöver myndigheten ge in en framställning om gallring till Riksarkivet. Riksarkivet kan sedan efter att ha prövat framställningen utfärda myndighetsspecifika föreskrifter om gallring. Av framställningen bör framgå vilken funktion de e-underskrivna handlingarna har vid myndigheten, till exempel inom vilken typ av ärenden de förekommer och vad de har för betydelse där, se vidare Juridisk checklista för bevarande och gallring i kap. 13.

11. PERSONDATASKYDD

E-legitimationer och e-underskrifter bygger på behandling av personuppgifter. För organisationer är det viktigt att säkerställa att behandlingen inte bara utförs i enlighet med gällande regelverk utan även tar höjd för de regelskärpningar som föranleds av Dataskyddsförordningen som träder ikraft 2018. I detta kapitel redovisas översiktligt de frågor om persondataskydd som aktualiseras inom ramen för e-legitimationssystemet och hur dessa frågor bör hanteras.

Skyddet i grundlag

11.1 Skyddet i grundlag mot otillbörligt integritetsintrång stärktes år 2010 genom att ett andra stycke infördes i 2 kap. 6 § regeringsformen enligt vilket var och en gentemot det allmänna är skyddad mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden.

11.2 Med användningen av till exempel e-legitimation och eget utrymme för användare[90] blir det möjligt att upprätthålla de tydliga gränser mellan till exempel myndigheter och enskilda som från integritetssynpunkt uppfattas som en självklarhet i traditionell fysisk miljö.[91] Medborgares behov kan dessutom tillgodoses genom att få avskärma sig från omgivningen inom en fredad, privat zon, så som vid användning av papper och penna eller en dator utan internetuppkoppling i bostaden.[92] Skyddet för enskildas personliga integritet säkerställs härvid så att intrång genom identitetsstölder, förfalskningar och liknande förhindras eller i vart fall försvåras.

Mot detta får ställas den identifiering av individer och den övriga behandling av personuppgifter som krävs för att skyddet ska kunna upprätthållas inom de e-legitimations- och underskriftssystem som används för att hindra manipulationer och missbruk.

Skyddet i vanlig lag och enligt dataskyddsförordningen

11.3 På området för persondataskydd gäller för närvarande personuppgiftslagen (1998:204; PuL). Från och med den 25 maj 2018 tillämpas i stället Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (dataskyddsförordningen). Alla krav som följer av dataskyddsförordningen ska tillämpas genast vid ikraftträdandet. Det finns inte några övergångsbestämmelser.

---

[90] Se 5.6 ovan och eSams publikation Eget utrymme hos myndighet – en vägledning.

[91] Behovet av tydliga gränser inom dagens nätverkssamhälle har också kommit till uttryck i HFD 2015 ref. 61 som avser elektroniskt informationsutbyte där skydd ges genom till exempel e-legitimationer och servercertifikat. HFD fann att sådan teknisk tillgång till upptagningar som avses i 2 kap. 3 § andra stycket TF inte föreligger när en myndighet begär att få ut uppgifter från annan, men inte på egen hand kan söka information hos den andra aktören, eftersom ett utlämnande förutsätter att den utlämnande aktören reagerar på en begäran. Genom domstolens dom återställs de tydliga gränser mellan myndigheter, respektive mellan myndigheter och enskilda, som ses som en självklarhet i traditionell fysisk miljö.

[92] Se hur det i lagmotiven (SOU 2008:3, s. 14 f.) förklarats att det alltid måste finnas ett skydd för rätten att stänga om sig – dvs. att utgångspunkten måste vara att den enskilde ska vara fri att kunna avskärma sig från omgivningen (jfr SOU 2016:41 s. 146).

En anpassning till dataskyddsförordningen av de e-legitimations- och underskriftssystem som numera används bör därför övervägas redan nu.

11.4 Enligt personuppgiftslagen ska lämpliga tekniska och organisatoriska åtgärder vidtas för att skydda de personuppgifter som behandlas. Åtgärderna ska åstadkomma en säkerhetsnivå som är lämplig med beaktande av de tekniska möjligheter som finns, vad det skulle kosta att genomföra åtgärderna, de särskilda risker som finns med behandlingen av personuppgifterna och hur pass känsliga de behandlade personuppgifterna är.

Åstadkomma en säkerhetsnivå som är lämplig

Enligt artikel 24 i dataskyddsförordningen ska på motsvarande sätt den personuppgiftsansvarige – med beaktande av behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter – genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen utförs i enlighet med förordningen. Dessa åtgärder ska dessutom ses över och uppdateras vid behov. Om det står i proportion till behandlingen, ska åtgärderna också omfatta den personuppgiftsansvariges genomförande av lämpliga strategier för dataskydd.[93]

11.5 Vid dessa överväganden behöver artikel 25 dataskyddsförordningen om inbyggt dataskydd och dataskydd som standard också beaktas.[94]

Behovet av åtgärder

11.6 När en legitimeringsfunktion, en identifierings- och intygsfunktion, en underskriftsfunktion eller ett eget utrymme för användare ska anskaffas och införas behöver till exempel

- den tekniska utformningen i sig ge skydd för enskildas personliga integritet (inbyggt dataskydd och dataskydd som standard),
- personuppgiftsansvarets fördelning beaktas redan när de tekniska och administrativa funktionerna utformas,
- en analys av hot och sårbarheter och vilka säkerhetsåtgärder som behöver vidtas, göras som en integrerad del av utvecklingsarbetet, och omfatta hela den tänkta infrastrukturen,
- tjänsten utformas så att den eller de personuppgiftsansvariga kan uppfylla samtliga krav i personuppgiftslagen och/eller registerförfattningar (i registerförfattningar berörs till exempel ändamålsbestämmelser och bestämmelser om direktåtkomst),
- personuppgiftsbiträdesavtal upprättas med berörda biträden, och
- varje aktör vidta lämpliga tekniska och organisatoriska säkerhetsåtgärder

[93] Av samma artikel följer att godkända uppförandekoder som avses i artikel 40 eller godkända certifieringsmekanismer som avses i artikel 42 får användas för att visa att den personuppgiftsansvarige fullgör sina skyldigheter.

[94] Artikel 25 har följande innehåll: 1. Med beaktande av den senaste utvecklingen, genomförandekostnader och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige, både vid fastställandet av vilka medel behandlingen utförs med och vid själva behandlingen, genomföra lämpliga tekniska och organisatoriska åtgärder – såsom pseudonymisering – vilka är utformade för ett effektivt genomförande av dataskyddsprinciper – såsom uppgiftsminimering – och för integrering av de nödvändiga skyddsåtgärderna i behandlingen, så att kraven i denna förordning uppfylls och den registrerades rättigheter skyddas. 2. Den personuppgiftsansvarige ska genomföra lämpliga tekniska och organisatoriska åtgärder för att, i standardfallet, säkerställa att endast personuppgifter som är nödvändiga för varje specifikt ändamål med behandlingen behandlas. Den skyldigheten gäller mängden insamlade personuppgifter, behandlingens omfattning, tiden för deras lagring och deras tillgänglighet. Framför allt ska dessa åtgärder säkerställa att personuppgifter i standardfallet inte utan den enskildes medverkan görs tillgängliga för ett obegränsat antal fysiska personer. 3. En godkänd certifieringsmekanism i enlighet med artikel 42 får användas för att visa att kraven i punkterna 1 och 2 i den här artikeln följs.

för att skydda sin information och för att åstadkomma en lämplig säkerhetsnivå (jfr E-delegationens juridiska vägledning för verksamhetsutveckling inom e-förvaltningen, version 2.0, avsnitt 3.2).

11.7 Den information som enligt personuppgiftslagen och andra författningar måste lämnas till dem som registreras är omfattande och bör samlas så att den blir enkel att ta del av. När en tjänst bygger på att samtycke ges, beträffande personuppgiftsbehandling eller för att sekretessreglerade uppgifter ska få lämnas ut, måste rutinerna för samtycke utformas så att giltiga samtycken uppkommer (jfr E-delegationens nämnda juridiska vägledning, avsnitt 3.2).

11.8 Skyddet för personuppgifter i eget utrymme och frågan om i vilken mån den myndighet som tillhandahåller *eget utrymme* är personuppgiftsansvarig för de behandlingar av personuppgifter som äger rum i ett sådant utrymme har varit föremål för diskussion under flera år. För eSams del hänvisas i denna del till redogörelsen i avsnitt 5.5 i eSams publikation Eget utrymme hos myndighet – en vägledning.

11.9 Fördelningen av personuppgiftsansvaret för *legitimerings-, identifierings-, intygs- och underskriftsfunktioner* har berörts av E-legitimationsnämnden och i de utredningar som föregått bildandet av nämnden. Där har personuppgiftsansvaret beskrivits så att det flyttas över stegvis när en transaktion flödar genom infrastrukturen. Detta synsätt, som avses gälla även för den särskilda övergångstjänsten, innebär att varje aktör är personuppgiftsansvarig för sitt led i hanteringen enligt följande.

a) *Utfärdare av e-legitimation*
- tar emot ansökningar om e-legitimation, registrerar uppgifter, utfärdar och lämnar ut e-legitimationer samt tillhandahåller funktioner för spärr och spärrkontroll, och
- tillhandahåller en legitimeringsfunktion och i vissa fall en underskriftsfunktion för direkt underskrift (det gränssnitt som möter användaren).

För dessa behandlingar bär utfärdare av e-legitimation personuppgiftsansvaret.

b) *Leverantör av intygstjänst (och tjänst för direkt underskrift)*
- kontrollerar användares identitet, ställer ut intyg och sänder intyg till den förlitande parten, och
- skapar underskrifter, vid direkt underskrift, och sänder underskrifter till förlitande part tillsammans med intyg om underskriftens äkthet.

För dessa behandlingar bär leverantören av tjänsten personuppgiftsansvaret.

c) *Förlitande part*
- identifierar användare med hjälp av mottagna identitetsintyg,
- skapar och skickar underlag som tekniskt ska skrivas under (se 5.7), och
- tillhandahåller, vid indirekt underskrift, en underskriftstjänst åt användaren där denne identifieras med hjälp av ett från en leverantör av intygstjänst mottaget identitetsintyg och en underskrift skapas med ett särskilt underskriftscertifikat som utfärdas i underskriftstjänsten.

För dessa behandlingar bär förlitande part personuppgiftsansvaret (jfr E-legitimationsnämndens bedömning av personuppgiftsansvarets fördelning i Regelverk för identitetsfederationer för Svensk e-legitimation, Bilaga I, ref.nr: ELN-0508-v1.3).

12. EIDAS-FÖRORDNINGEN

Kapitlet innehåller en redogörelse för EU:s förordning om gränsöverskridande elektronisk legitimering (eIDAS-förordningen) och hur till exempel kraven på ömsesidigt erkännande av anmälda e-legitimationer fr.o.m. den 29 september 2018 påverkar myndigheterna.

Övergripande om eIDAS-förordningen

12.1 Europaparlamentet och rådet har antagit förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG (eIDAS-förordningen). Förordningen är uppdelad i två huvudsakliga delar, (1) krav på ömsesidigt erkännande av anmälda e-legitimationer och (2) krav på tillhandahållande av betrodda tjänster och en rättslig ram för sådana tjänster.

Förordningens materiella delar började tillämpas den 1 juli 2016. Från och med den 29 september 2018 krävs också att svenska offentliga myndigheter erkänner utländska e-legitimationer i svenska e-tjänster.[95]

Ömsesidigt erkännande av anmälda e-legitimationer

12.2 Medel för elektronisk identifiering, som är utfärdade inom ramen för ett system för elektronisk identifiering som har anmälts av en medlemsstat (EU/EES) och förts upp på en särskild förteckning som offentliggörs av Europeiska kommissionen, ska under vissa förutsättningar omfattas av ömsesidigt erkännande (artikel 6).

Vilka omfattas av kravet?

12.3 eIDAS-förordningen gäller för alla offentliga organ.[96] Kravet på erkännande gäller om

- den utländska e-legitimationen har anmälts av en medlemsstat och förts upp på en särskild förteckning som offentliggörs av Europeiska kommissionen,
- e-tjänsten i fråga kräver att en nationell e-legitimation på tillitsnivå ”väsentlig” eller högre används, dvs. motsvarande BankID/Telia eller högre, och
- den utländska e-legitimationen motsvarar minst den tillitsnivå som det ställs krav på nationellt för användning av e-tjänsten.[97]

---

[95] Förordningen upphäver det tidigare signaturdirektivet (1999/93/EG) som implementerats i Sverige genom lagen (2000:832) om kvalificerade elektroniska signaturer (signaturlagen). Genom lagen (2016:561) om kompletterande bestämmelser till EU:s förordning om elektronisk identifiering upphävs även den svenska signaturlagen.

[96] Förordningen använder samma definition och avgränsningar av offentligrättsligt organ som de nya upphandlingsdirektiven (2014/24/EU).

[97] De tillitsnivåer som definieras i förordningen är ”låg”, ”väsentlig” och ”hög”, vilket i princip motsvarar nivåerna 2, 3 och 4 enligt andra internationella ramverk såsom ISO 29115 samt tillitsramverket för Svensk e-legitimation. Detta innebär att en myndighet, kommun eller landsting som tillhandahåller en e-tjänst där man använder sig av BankID eller Telia för legitimering, som bedömts ligga på tillitsnivå 3 (eller ”väsentlig”), även måste kunna ta emot utländska anmälda e-legitimationer på tillitsnivå ”väsentlig” eller högre. – Det är i dagsläget oklart vad som gäller om vi nationellt väljer att definiera våra e-legitimationer som högre än tillitsnivå ”väsentlig” eller ”hög”, och huruvida det innebär att det inte finns någon skyldighet att erkänna utländska e-legitimationer på lägre nivå. En tydlig definiering av tillitsnivån på den nationella e-legitimationen görs först i samband med en anmälan av e-legitimationen. Efter anmälan på viss definierad tillitsnivå torde det dock vara svårt att hävda att den nationella e-legitimationen skulle befinna sig på en högre nivå.

Hur långt sträcker sig kravet?

12.4 Artikel 6 ställer krav på ”erkännande” av den utländska e-legitimationen ”för gränsöverskridande autentisering” för e-tjänsten i fråga. Frågan om vad ett erkännande för autentisering innebär är inte helt enkel att svara på, men i förklarandesatserna anges tydligt att erkännandet inte avser själva åtkomsten till e-tjänsterna och deras slutliga leverans till den sökande. Autentiseringen ska således frikopplas från frågor om åtkomst och behörighet.[98]

12.5 Den tekniska interoperabiliteten inom ramen för det ömsesidiga erkännandet bygger på en modell med nationella förbindelsepunkter (eIDAS-noder) som kopplar samman olika nationella tekniska arkitekturer. En e-legitimationsutfärdare eller förlitande part behöver alltså bara kunna kommunicera med den nationella noden, inte respektive lands motsvarande aktörer.

Den redan komplexa kedja av inblandade aktörer som beskrivits ovan i kap. 4 – 7 blir således, från juridisk utgångspunkt, ännu mer komplex vid gränsöverskridande elektronisk identifiering, när ytterligare mellanhänder i form av nationella eIDAS-noder berörs. Här finns inga särskilda förlitandeavtal. De ersätts av de krav som ställs i eIDAS-förordningen och Kommissionens genomförandeförordningar. Anslutning till den nationella eIDAS-noden kan dock komma att förenas med särskilda villkor. E-legitimationsnämnden ansvarar för vår nationella eIDAS-nod.

Krav på och rättslig ram för elektroniska underskrifter

12.6 eIDAS-förordningen ställer även krav på tillhandahållare av betrodda tjänster. Som betrodd tjänst definieras till exempel skapande, kontroll och validering av elektroniska underskrifter och certifikat kopplade till elektroniska underskrifter (artikel 3).[99]

12.7 Regleringen av elektroniska underskrifter i eIDAS-förordningen skiljer sig inte i någon större utsträckning från regleringen i det numera upphävda signaturdirektivet. Förordningen behåller uppdelningen i avancerade och kvalificerade elektroniska underskrifter, och kraven för respektive nivå är snarlik den som gällt enligt äldre regler. Den nya regleringen gäller emellertid direkt utan nationell implementering, vilket syftar till att råda bot på den bristande harmonisering som enligt EU-kommissionen präglat området. Dessutom omfattar eIDAS-förordningen en bredare kategori av betrodda tjänster än signaturdirektivet.

12.8 Det finns inga krav på medlemsstaterna att använda sig av kvalificerade elektroniska underskrifter. Sådana krav kan dock i högre grad komma att ställas genom olika former av gränsöverskridande tjänster eller samarbeten. De svenska direkta och indirekta underskrifterna anses generellt sett uppfylla kraven för avancerade elektroniska underskrifter.

---

[98] En rimlig tolkning bör vara att skyldigheten att erkänna således sträcker sig så långt som att kunna ta emot och bekräfta de identitetsintyg som översänds i den tekniska arkitekturen för interoperabilitet, men att det därefter står e-tjänsten fritt att neka vidare åtkomst på grund av bristande behörighet, exempelvis med hänsyn till avsaknad av svenskt person- eller samordningsnummer. Den utländska användaren placeras således efter autentisering i ett digitalt väntrum, i avvaktan på att rätt förutsättningar finns på plats för åtkomst till e-tjänsten. Frågan är dock inte okontroversiell, och flera medlemsstater argumenterar även för att ett åtkomstskrav som helt grundas på innehav av ett nationellt ID-nummer går emot själva grundprincipen om ömsesidigt erkännande av de utländska personidentitetsbeteckningar som förekommer i e-legitimationerna.

[99] För det som numera benämns elektronisk underskrift användes tidigare termen elektronisk signatur, till exempel i den svenska signaturlagen. Termen elektronisk signatur kommer från signaturdirektivet. I det allmänna språkbruket har den termen med tiden kommit att ersättas med den rättsligt mer korrekta termen elektronisk underskrift. Båda termerna har dock samma innebörd.

12.9 eIDAS-förordningen ger ett uttryckligt stöd för distansbaserade förfaranden för elektronisk underskrift, exempelvis då en e-legitimation används för att aktivera en central underskriftsfunktion (indirekt underskrift). Det finns ingen direkt koppling mellan tillitsnivå och underskrift, mer än att det kan komma att krävas en viss tillitsnivå på en e-legitimation för att kunna uppfylla kraven för avancerad eller kvalificerad underskrift för det fall att det rör sig om en indirekt underskrift.

Ingen direkt koppling mellan tillitsnivå och underskrift

12.10 Kvalificerade elektroniska underskrifter ska enligt eIDAS-förordningen ha samma rättsliga verkan som en handskriven underskrift (artikel 25). Detta hindrar inte att en nationell rättsordning kan ge även andra former av elektroniska underskrifter samma rättsliga verkan som en handskriven underskrift. Ett exempel är en avancerad elektronisk underskrift som kommit till inom ramen för en allmänt spridd lösning inom svensk offentlig sektor.

Det finns också ett undantag i eIDAS-förordningens (artikel 2) enligt vilket förordningen inte påverkar regler i nationell rätt som avser rättsliga eller förfarandemässiga skyldigheter avseende formkrav. Med hänsyn till rådande syn på krav i författning på egenhändigt undertecknande (se kapitel 2 ovan) får det anses föreligga ett nationellt formkrav på fysiskt undertecknande som alltså har företräde framför eIDAS-förordningens reglering av rättslig verkan för elektroniska underskrifter. Tillämpningsområdet för undantaget i artikel 2 är emellertid inte helt tydlig och utvecklingen i praxis kan leda till en annan bedömning i förhållande till artikel 25.

Av artikel 27 följer även en skyldighet för offentliga organ att ömsesidigt erkänna avancerade elektroniska underskrifter eller högre i e-tjänster i enlighet med de format som framgår av ett särskilt genomförandebeslut. Svenska e-tjänster kommer troligtvis i huvudsak att hantera underskrifter från utländska medborgare genom en indirekt underskrift som baseras på ett identitetsintyg via eIDAS-noderna för gränsöverskridande e-legitimering. Förekomsten av individer som hävdar sin rätt att använda en annan form av avancerad elektronisk underskrift bör därför vara marginell. Skyldigheten kvarstår dock och om inte det generella undantaget för nationella formkrav i artikel 2 blir tillämpligt behöver myndigheten i förekommande fall även kunna ta emot och hantera andra format.[100] I sammanhanget bör även noteras att det inte krävs att det är fråga om ett gränsöverskridande förhållande för att skyldigheten ska aktualiseras.

12.11 I artikel 2 finns det ett generellt undantag för betrodda tjänster som till följd av nationell rätt eller avtal mellan en avgränsad uppsättning deltagare endast används inom slutna system. Detta innebär exempelvis att ett helt myndighetsinternt system för elektroniska underskrifter av medarbetare sannolikt faller utanför förordningens krav på betrodda tjänster. Ett system som vem som helst kan ansluta sig till anses däremot knappast vara begränsat till en avgränsad uppsättning deltagare.

[100] Utformningen av genomförandebeslutet komplicerar frågan ytterligare, då i princip alla format måste kunna hanteras förutsatt att den medlemsstat där certifikatet är utfärdat erbjuder möjligheter till validering av underskrift som är lämpad för automatiserad behandling.

Var kan man få mer information?

12.12 För frågor om gränsöverskridande e-legitimering enligt eIDAS hänvisas till E-legitimationsnämnden (http://www.elegnamnden.se/eIDAS), som till exempel ansvarar för den svenska eIDAS-noden. För frågor om betrodda tjänster enligt eIDAS hänvisas till tillsynsmyndigheten Post- och telestyrelsen, som även har tagit fram en särskild vägledning för betrodda tjänster (http://www.pts.se/eIDAS).

Vissa av de frågor som berörs i detta kapitel är föremål för utredning i annan ordning; se Effektiv styrning av nationella digitala tjänster i en samverkande förvaltning (N 2016:01).

13. VAD MYNDIGHETER OCH ORGANISATIONER BÖR GÖRA

I det här kapitlet finns praktiska råd och rekommendationer för att samordna och underlätta införandet av e-legitimationer och e-underskrifter samlade. De är uppdelade i tre delar med checklistor som stöd för

- **införande av e-legitimering**
- **införande av e-underskrifter**
- **hantering av bevarande och gallring**

Råden och rekommendationerna tar höjd för såväl de juridiska som de säkerhetsmässiga perspektiven. Grunden för råden och rekommendationerna finns i vägledningens tidigare kapitel. Som tidigare nämnts kan checklistorna med fördel användas både av den som står i begrepp att införa e-legitimationer och e-underskrifter och av den som vill kontrollera att de redan införda tjänsterna har utformats på ett korrekt och säkert sätt.

Det bör noteras att de frågor som aktualiseras vid upphandling av e-legitimering och e-underskrift är så komplexa att myndigheterna aktivt bör söka stöd i redan utfört arbete, med hjälp av de myndigheter som har i uppdrag att stödja och samordna dessa frågor.

Utgångspunkter

Involvera alla relevanta yrkeskategorier

En organisation som inför e-legitimering och e-underskrifter i syfte att utföra rättshandlingar och hantera andra juridiskt betydelsefulla mellanhavanden behöver engagera inte bara sina jurister och informationssäkerhetsansvariga vid utformningen av system. En grupp där alla relevanta yrkeskategorier ingår (jurister, informationssäkerhetssamordnare, verksamhetsutvecklare, it-tekniker, arkivarie med flera) bör inrättas för att säkerställa att alla aspekter omhändertas vid till exempel utformning av användargränssnitt, avtal och tjänsternas koppling till andra verksamhetssystem och organisationens it-arkitektur.

Organisationen bör även kartlägga vilka nätverk som det kan vara lämpligt att ansluta sig till för att inhämta ytterligare information och utbyta erfarenheter.

Enhetlig terminologi

Genom att använda den terminologi, de avtalslösningar och de krav på rättsligt och säkerhetsmässigt hållbara lösningar som redovisas i denna vägledning kan dubbelarbete undvikas, införandet göras enhetligt och leverantörerna dra nytta av stordriftsfördelar.

Balanserade krav

Balanserade krav på it- och informationssäkerhet måste ställas och inte förväntas bli tillgodosedda av någon annan aktör.[101]

Rutiner för uppföljning och utvärdering

Rutiner för uppföljning och utvärdering av en myndighets e-legitimations- och e-underskriftstjänster behöver etableras för att säkerställa att de kan uppfylla såväl de rättsliga som de säkerhetsmässiga kraven över tid.[102]

Säkerställ de juridiska kraven

De juridiska kraven måste säkerställas av varje organisation (de kan inte förväntas vara tillgodosedda av någon av aktörerna), vid upphandling och vid användning, så att e-legitimering och e-underskrift resulterar i rättshandlingar, så som avsetts.

De juridiska kraven måste i många hänseenden även säkerställas i flera led och i en komplex kontext av avtal och parter. Detta gäller exempelvis vid de olika indirekta förfaranden för e-legitimering och e-underskrift som har redovisats i vägledningen. Men det kan också innebära att en förlitande part i sin kravställning behöver ställa vissa minimikrav på avtalsrelationen mellan utfärdare av e-legitimation och användare för att säkerställa att processen hänger ihop rättsligt och att användare garanteras det juridiska skydd som får anses vara rimligt i sammanhanget.

[101] All kravställning gällande informationssäkerhet ska utgå ifrån ett systematiskt arbete samt följa minst MSBFS 2016:1 föreskrifter och allmänna råd om statliga myndigheters informationssäkerhet. För statliga myndigheter behöver även MSBFS 2016:2 föreskrifter och allmänna råd om statliga myndigheters rapportering av it-incidenter beaktas.

[102] Utkontrakterar organisationen (förlitande part) hela eller delar av e-legitimations- och e-underskriftstjänsterna till en leverantör är det av vikt att säkerställa att de rutiner som reglerar att leverantören rapporterar inträffade it-incidenter till organisationen finns på plats.

1. Checklista för förlitandeavtal (e-legitimering)

När en organisation ska sluta förlitandeavtal med en leverantör bör till exempel de frågor som tas upp i följande checklista beredas och bedömas.

Sluts förlitandeavtal för direkt eller indirekt leverans av intyg?

- Ska din myndighet upphandla en identifierings- och intygsfunktion
  - direkt från en leverantör av identitetsintyg som utfärdar e-legitimationer (till exempel med en BankID-bank),
  - indirekt från en leverantör av identitetsintyg som inte utfärdar e-legitimationer utan agerar som ”återförsäljare” (till exempel CGI/Visma/Cybercom)?
    - Har myndigheten analyserat konsekvenserna av detta val?
      - Hur hanterar ni format, bevarande och äkthetskontroller på sikt vid direkt leverans?
      - Hur säkerställer ni ansvaret i tidigare led vid indirekt leverans?

Sluts förlitandeavtal via en myndighet som har en samordnande roll?

- Egen upphandling: Ska din myndighet upphandla förlitandeavtal genom en egen upphandling från en leverantör av identitetsintyg?
  - Ska intygen levereras
    - direkt (från till exempel BankID-bank/Telia), utan konvertering, i ett format som leverantör av identitetsintyg bestämt,
      - Levereras stämplade intyg med urkundskvalitet eller endast uppgifter i skyddad miljö?
      - Bär leverantören ett metod- eller resultatansvar? Är specifikationerna tydliga?
    - indirekt (från till exempel CGI/Visma/Cybercom), efter kontroll av bakomliggande leverantörs (till exempel BankID-bank) intyg och konvertering?
      - Ska även andra tjänster levereras – går det att urskilja ett förlitandeavtal bland villkoren?
      - Vem anges stämpla – är leverantören endast ett osjälvständigt biträde?
- Samordnad upphandling: Sluter din myndighet förlitandeavtal inom ramen för E-legitimationsnämndens övergångstjänst (dvs. ett valfrihetssystem) eller ett ramavtal som upphandlats av en samordnande myndighet,
  - för direkt leverans av identitetsintyg utan konvertering (till exempel CSN med E-legitimationsnämnden som samordnare), eller
  - indirekt leverans av identitetsintyg, efter kontroll av bakomliggande leverantörs intyg och konvertering av intyg (till exempel Skatteverket med Kammarkollegiet som samordnare)?

- Har din myndighet analyserat konsekvenserna av dessa val?
  - Innebär avrop från ramavtal att villkoren inte utformats särskilt för e-legitimering och e-underskrifter med hjälp av avropad tjänst?
  - Täcker ett avrop inom valfrihetssystemet myndighetens behov? Hur anskaffas tillägg?

- Fyller samordnande myndighet en reell roll för att förenkla din kravställning?[103]
  - Behöver din myndighet göra en kompletterande kravställning vid avrop?
  - Samordnas dina krav med övriga myndigheter?
    - Har din myndighet analyserat konsekvenserna av en bristande samordning?
      - Hur kan kraven i praktiken kompletteras? Räcker detaljeringsgraden för metodansvar?
      - Finns de kravbilagor som behövs redan hos en annan myndighet? Uppfinns hjulet igen?
      - Kommer en egen kravställning att ge ett annat system än hos andra myndigheter?

Hur ska identitetsintygen och övrig hantering vara utformad?

- Är de identitetsintyg, som ska levereras till din myndighet, försedda med en sådan e-stämpel att intyget har urkundskvalitet eller saknar det e-stämpel?
  - Är kravställningen för de intyg som ska levereras utformad så att e-stämpling sker av rätt part eller blir de till exempel e-underskrivna av den som legitimerat sig?
    - Har din myndighet analyserat konsekvenserna av leveransens innehåll?
      - Kan straffansvar utkrävas vid missbruk så som intyg och funktioner utformas?
  - Är e-stämpelfunktionen av intygen sådan att den uppfyller kraven på till exempel nyckelhantering, fysiskt driftutrymme, val av kryptografiska funktioner, validering av hård- och mjukvara initialt och över tid samt därtill tillhörande säkerhetsåtgärder?

- Är innehållet i de identitetsintyg och berörda användargränssnitt som din myndighet använder utformade så att det tydliggörs att e-legitimation och identitetsintyg inte får missbrukas?
  - Finns det risk för att någon legitimerar sig så att annan (en individ eller en robot) sanningslöst kan åberopa e-legitimationen eller intyget som gällande för sig och bli insläppt i din myndighets e-tjänst utan någon reell prövning av om denna individ eller robot ska få komma in?
    - Har din myndighet information på till exempel berörd webbplats om på vilket sätt e-legitimation får användas?
      - Finns det särskild risk för att robotar eller liknande används för att otillåtet samla in uppgifter i funktioner som din myndighet tillhandahåller?
      - Överväger din myndighet tekniska eller rättsliga åtgärder mot sådana angrepp?

[103] Jfr E-legitimationsnämndens direkta samordningsuppdrag för legitimering med Kammarkollegiets mera allmänna uppdrag.

- Tillhandahåller din leverantör av intygstjänst en funktion för säker kommunikation för beställning av e-legitimering och leverans av intyg?
  - Hur förvaltas kraven för ”säker kommunikation” såsom krav gällande nyckelhantering, val av kryptografiska algoritmer, sårbarhetsanalyser för aktuella gränssnitt och åtgärder vid incidenter?

- Har kraven på tillitsnivå och informationsklassificering beaktats?
  - Har informationsinnehållet i till exempel handlingar som ges åtkomst till efter identifiering och behörighetskontroll informationsklassificerats?
  - Har samtliga tekniska, organisatoriska, fysiska och administrativa säkerhetsåtgärder som är knutna till informationsklassificeringen applicerats?
    - Hur hanteras risker kopplade till sådana säkerhetsåtgärder som inte är införda? Har organisationen gjort en dokumenterad riskanalys där berörda kvarvarande risker har en ägare och en åtgärdsplan?
      - Finns det rutiner för att förvalta risklistan?
  - Håller de e-legitimationer som är knutna till e-tjänsten en tillräcklig tillitsnivå i förhållande till informationsklassificeringen av de handlingar till vilka åtkomst begärs med stöd av e-legitimation?
    - Hur säkerställer myndigheten att kraven för respektive tillitsnivå uppfylls? Är kraven harmoniserade med övrig offentlig sektor? Hur följs kraven upp över tid?

- Har det beaktats att eIDAS kräver att utländska e-legitimationer ska erkännas och att det ska finnas en koppling till den svenska landsnod som E-legitimationsnämnden har regeringens uppdrag att tillhandahålla?

Ansvar för avtalade funktioner och bakomliggande leverantörer

- Innebär ditt förlitandeavtal att leverantör av identitetsintyg ansvarar för den identifiering och anknytande hantering som skett vid
  - utfärdande av använd e-legitimation (ofta bakomliggande leverantör),
  - besvarande av spärrfråga (ofta bakomliggande leverantör),
  - e-identifiering efter att användaren legitimerat sig (en bakomliggande leverantör vid indirekt leverans av intyg – i vissa fall även vid direkt leverans)[104],
  - kontroll av intyg från en bakomliggande leverantör (till exempel från en BankID-bank till kontrakterad leverantör av identitetsintyg)?

- Om ett förlitandeavtal inte innebär att leverantör av identitetsintyg svarar för bakomliggande leverantör – har förlitande part istället slutit avtal direkt med bakomliggande leverantör om ansvar för denne?

- Är avtalat ansvar utformat som ett resultat- eller ett metodansvar – vilka friskrivningar har gjorts – har förlitande part analyserat riskerna?

- Har leverantören i förlitandeavtalet tagit på sig ett felansvar med sedvanliga sanktioner vid brister i tjänsten?

[104] Som exempel kan nämnas att ett förlitandeavtal med en BankID-bank kan innebära att en användare identifieras, av den bank som är part i förlitandeavtalet, genom en e-legitimation som är utställd av en annan BankID-bank.

- Har avtalet tagit höjd för kravet att tjänsteleverantören åtar sig att rapportera it-incidenter i berörda system till myndigheten på ett sätt som motsvarar kraven enligt MSBFS 2016:2?
- Hur är personuppgiftsansvaret fördelat enligt förlitandeavtalet? Är leverantör av identitetsintyg ansvarig eller biträde? Gäller olika bedömningar för olika delar av det som levereras?
- Kan leverantören uppnå kraven på säkerhetsåtgärder som ställs i enlighet med informationsklassificeringen och riskanalysen som är resultat av den egna organisationens arbete?
  - Hur hanteras kvarvarande risker avtalsmässigt och dess ägandeskap mellan leverantör och förlitande part?
  - Hur mäts effektiviteten i säkerhetsåtgärderna?
- Hur avtalas leverantörens ansvar att på ett systematiskt sätt arbeta med informationssäkerhet? Hur kan detta redovisas och följas upp?

Vad sänds till förlitande part?

- Vad sänds (i form av intyg) till din myndighet, från leverantör av identitetsintyg,
  - vilka intyg vid direkt respektive indirekt leverans, och
  - vad är e-stämplat eller e-underskrivet och av vem?
- Vilka kontroller gör din myndighet? Ska kontrollresultatet e-stämplas?
- Har din myndighet rätt att begära ytterligare uppgifter för kontroll från leverantören? Blir sådant material allmän handling hos er?

Rättsverkningar av e-legitimering

- Har det beaktats i din myndighets förlitandeavtal att vissa e-legitimeringar sker för att utföra en rättshandling i enlighet med vedertagna juridiska synsätt och tolkningsmetoder (till exempel vid e-legitimering för uppgiftslämnande eller för indirekt underskrift, se 4.5).
  - Finns det villkor i din myndighets avtal om att hanteringen ska gå till på visst sätt för att säkerställa att rättsverkningar inträder på motsvarande sätt som vid en manuell hantering?
    - Ställer villkoren krav på att leverantörens eller bakomliggande leverantörs användargränssnitt ska ha visst innehåll?
      - Ska det stå ”Jag legitimerar mig” vid legitimering för tillträde eller uppgiftslämnande och ”Jag skriver under” vid legitimering för underskrift?

Kan civilrättsligt bindande avtal slutas mellan aktörerna?

- Är din myndighet och leverantören en del av samma juridiska person – vanligtvis staten – så att en tvist inte kan prövas i domstol?

2. Checklista för avtal om underhålls-tjänst

När en organisation ska sluta avtal om underskriftstjänst bör till exempel de frågor som tas upp i följande checklista beredas och bedömas.

Sluts avtal om underskriftstjänst för direkt eller indirekt underskrift?

- Ska din myndighet upphandla en underskriftstjänst för
  - direkt underskrift, med en e-legitimation som redan är utfärdad åt användaren,
    - där underskriften skapas och levereras direkt i ett format som leverantör av underskriftstjänst har bestämt (till exempel av BankID-bank), eller
  - indirekt underskrift, med ett särskilt underskriftscertifikat,
    - där underskriften skapas, efter att användaren har legitimerat sig för indirekt underskrift, och levereras i ett format som förlitande part har bestämt (till exempel CGI)?
  - Har myndigheten analyserat konsekvenserna av detta val?
    - Hur hanterar ni format, bevarande och äkthetskontroller på sikt vid direkt underskrift?
    - Hur säkerställer ni ansvaret i tidigare led vid indirekt underskrift?

Sluts underskriftsavtal via en myndighet som har en samordnande roll?

- Sluter din myndighet avtal om underskriftstjänst
  - omedelbart med en leverantör av underskriftstjänst (egen upphandling),
    - Levereras stämplade intyg med urkundskvalitet eller endast uppgifter i skyddad miljö?
    - Bär leverantören ett metod- eller resultatansvar? Är specifikationerna tydliga?
  - genom avrop från ett ramavtal (med E-legitimationsnämnden/Kammar-kollegiet som samordnare)?
    - Ska även andra tjänster levereras – går det att urskilja ett avtal om underskriftstjänst bland villkoren?
    - Vem anges stämpla – är leverantören endast ett osjälvständigt biträde?

- Har din myndighet analyserat konsekvenserna av dessa val?
  - Innebär avrop från ramavtal att villkor ska gälla som inte är anpassade för tjänsten?
  - Täcker ett avrop inom valfrihetssystemet myndighetens behov? Hur anskaffas tillägg?
  - Hur hanterar ni format, bevarande och äkthetskontroller på sikt vid direkt underskrift?
  - Hur säkerställer ni ansvaret i tidigare led vid indirekt underskrift?
  - Hur säkerställer ni eIDAS-kraven om e-underskrifter?

- Fyller samordnande myndighet en reell roll för att göra det enklare för din myndighet, så att funktionerna för e-underskrift blir enhetliga, eller måste din myndighet till betydande del göra kravställningen själv?
  - Har din myndighet underlag för att utforma en egen kravställning inför avrop och kan den samordnas med andra myndigheters hantering?
    - Har din myndighet analyserat konsekvenserna av en bristande samordning?
      - Hur kan kraven i praktiken kompletteras? Räcker detaljeringsgraden för metodansvar?
      - Finns de kravbilagor som behövs redan hos en annan myndighet? Uppfinns hjulet igen?
      - Kommer en egen kravställning att ge ett annat system än hos andra myndigheter?

Hur skapas e-underskriften och hur hanteras leveransen?

- Är e-underskriftsfunktionen sådan att den uppfyller kraven på till exempel nyckelhantering, fysiskt driftutrymme, val av kryptografiska funktioner, validering av hård- och mjukvara initialt och över tid samt därtill hörande säkerhetsåtgärder?

- Sänder leverantör av underskriftstjänst underskriften till din myndighet tillsammans med ett stämplat intyg om underskriftens äkthet, eventuellt tillsammans med ett särskilt underskriftscertifikat?
  - Är de intyg som levereras inte stämplade?
  - Utgör allt relevant kontrollmaterial en del av intyget? Om inte allt material finns med, är leverantör av underskriftstjänst skyldig att bevara och lämna ut det vid behov?
  - Tillhandahåller din leverantör av underskriftstjänst en funktion för säker kommunikation för beställning av underskrift och leverans av svar?
    - Hur förvaltas kraven för ”säker kommunikation” såsom krav gällande nyckelhantering, val av kryptografiska algoritmer, sårbarhetsanalyser för aktuella gränssnitt och åtgärder vid incidenter?

- Har kraven på tillitsnivå och informationsklassificering beaktats?
  - Har informationsinnehållet i till exempel handlingar som ges åtkomst till efter identifiering och behörighetskontroll informationsklassificerats?
  - Har samtliga tekniska, organisatoriska, fysiska och administrativa säkerhetsåtgärder som är knutna till informationsklassificeringen applicerats?
    - Hur hanteras de säkerhetsåtgärder som inte är applicerade? Har organisationen gjort en dokumenterad riskanalys där berörda kvarvarande risker har en ägare och en åtgärdsplan?
      - Finns det rutiner att förvalta risklistan?
  - Håller de e-legitimationer som är knutna till e-tjänsten en tillräcklig tillitsnivå i förhållande till informationsklassificeringen av de handlingar som skrivs under?
    - Hur säkerställer myndigheten att kraven för respektive tillitsnivå uppfylls? Är kraven harmoniserade med övrig offentlig sektor? Hur följs kraven upp över tid?
- Hur för din myndighet samman levererad e-underskrift och tillhörande material med den underskrivna handlingen och vilka kontroller utförs av mottaget och sammanställt material?

Ansvar för avtalade funktioner och bakomliggande leverantörer

- Innebär din myndighets avtal om underskriftstjänst att leverantören ansvarar för
  - e-identifiering[105] av undertecknaren,
  - underskriften, och eventuellt särskilt underskriftscertifikat, samt
  - kontrollen av att underskriften blivit riktig och intyget om dess äkthet?
- Ansvarar din myndighets leverantör av underskriftstjänst, i förhållande till din myndighet, också för bakomliggande leverantörers åtgärder för att
  - utfärda den e-legitimationen som använts (direkt eller indirekt) för underskrift,
  - besvara en spärrfråga, och
  - ställa ut identitetsintyg, när e-legitimering sker för indirekt underskrift?
- Har din myndighet slutit annat avtal om ansvar med en bakomliggande leverantör för det fall att avtalet om underskriftstjänst inte innebär att leverantör av identitetsintyg ansvarar för bakomliggande leverantörer?
- Är ansvaret gentemot din myndighet utformat som ett resultat- eller ett metodansvar?

[105] Med stöd av det identitetsintyg som ställts ut efter legitimering för indirekt underskrift.

- Har avtalet tagit höjd för kravet att tjänsteleverantören åtar sig att rapportera it-incidenter i berörda system till myndigheten på ett sätt som motsvarar kraven enligt MSBFS 2016:2?
- Kan leverantören uppnå kraven på säkerhetsåtgärder som ställs i enlighet med informationsklassificeringen och riskanalysen som är resultat av den egna organisationens arbete?
  - Hur hanteras kvarvarande risker avtalsmässigt och dess ägandeskap mellan leverantör och förlitande part?
  - Hur mäts effektiviteten i säkerhetsåtgärderna?
- Hur avtalas leverantörens ansvar att på ett systematiskt vis arbeta med informationssäkerhet? Hur kan detta redovisas och följas upp?
- Är frågan om vem som ställer ut och ansvarar för ett särskilt underskrifts-certifikat genomlyst och reglerad i avtal?
- Har leverantören i avtalet tagit på sig ett felansvar med sedvanliga sanktioner vid brister i tjänsten?
- Hur är personuppgiftsansvaret fördelat enligt avtalet om underskriftstjänst?
  - Är leverantör av underskriftstjänst personuppgiftsansvarig eller person-uppgiftsbiträde?
  - Gäller olika bedömningar för delar av det som levereras?

Vad sänds till förlitande part?

- Vad sänds (i form av underskrifter eller intyg) till din myndighet, från leverantör av underskriftstjänst,
  - vilka intyg levereras vid direkt respektive indirekt underskrift, och
  - vad är e-stämplat eller underskrivet och av vem?
- Vilka kontroller gör din myndighet?
- Har din myndighet rätt att begära ytterligare uppgifter för kontroll från leverantören? Blir sådant material allmän handling hos din myndighet?
- Ska din myndighet e-stämpla de e-underskrivna handlingarna efter att de har kontrollerats och ska även intyg och kontrollresultat e-stämplas av din myndighet?

Rättsverkningar av underskrift

- Har det beaktats i din myndighets avtal om underskriftstjänst att e-underskrifter vanligtvis används för rättshandlingar och att de juridiska verkningarna av en underskrift bestäms av innehållet i den information som skrivs under och det sammanhang där undertecknaren skriver under, allt i enlighet med vedertagna juridiska synsätt och tolknings-metoder?
  - Finns det villkor i din myndighets avtal om att hanteringen ska gå till på visst sätt för att säkerställa att rättsverkningar inträder på motsvarande sätt som vid en manuell hantering?
    - Ställer villkoren krav på att leverantörens eller bakomliggande leverantörs användargränssnitt ska ha visst innehåll?
    - Ska det stå ”Jag skriver under” vid underskrift?
    - Finns det risk för att den som skriver under i användargränssnittet för underskrift möts av texten ”Jag legitimerar mig”?
  - Har avtalsvillkoren utformats för att underskrifterna, tillsammans med intygens och berörda användargränssnitt, ska få avsedda rättsverkningar?
  - Har myndigheten behov av kvalificerade elektroniska underskrifter enligt eIDAS-förordningen och har åtgärder i så fall vidtagits i kravställning för att säkerställa att sådana kan produceras?

Kan civilrättsligt bindande avtal slutas mellan aktörerna?

- Är din myndighet och leverantör av underskriftstjänst en del av samma juridiska person – vanligtvis staten – så att en tvist inte kan prövas i domstol?

3. Juridisk checklista för bevarande och gallring

När en organisation ska införa e-legitimering och e-underskrift bör till exempel de frågor som tas upp i följande checklista beredas och bedömas rörande bevarande och gallring.

Vilket regelverk gäller

- När arkivlagens bestämmelser om bevarande och gallring gäller för handlingar hos din myndighet får de endast gallras med stöd av föreskrifter från Riksarkivet. Begreppet handling är här så vidsträckt att varje begäran om legitimering eller underskrift som din myndighet expedierar och alla svar som kommer in eller kontrollresultat som upprättas omfattas av reglerna.
- Du kan få gallra dels genom att din myndighet direkt tillämpar Riksarkivets föreskrifter och allmänna råd om gallring (RA-FS), dels efter att din myndighet begärt att Riksarkivet ska besluta om en myndighetsspecifik föreskrift (RA-MS) och en sådan föreskrift beslutats.[106]
- Gäller en registerförfattnings bestämmelser om gallring ska bevarande och gallring ske inom ramen för de bestämmelserna.

Hur ser processen för de elektroniska handlingarna ut

- För att du genom en gallringsutredning ska kunna förstå och värdera de elektroniskt underskrivna handlingarna och de valideringsdata som är knuta till handlingarna måste den process inom vilken de uppkommit vara beskriven och finnas dokumenterad så länge handlingarna ska vara kvar. Din dokumentation av processen är också till för att visa på en säker hantering och för att förstå och värdera handlingarna och valideringsuppgifterna så länge de bevaras. Du bör uppmärksamma följande:
  - Är processen beskriven i klassificeringsstrukturen (RA-FS 2008:4)?
  - Finns ytterligare beskrivningar som behöver bevaras?
  - Är beskrivningarna målgruppsanpassade för de målgrupper som bedöms kunna bli aktuella, till exempel tekniker, kund, myndighetsjurist, handläggare eller domstol?
  - Vilka möjligheter finns att beställa fram den ursprungliga handlingen, valideringsdata och myndighetsstämplade dokumentet (om stämpling sker) vid behov för aktuella målgrupper?

[106] Som framgår nedan, under rubriken Famställan till Riksarkivet, finns det inte någon RA-FS som specifikt tar upp gallring av elektroniskt underskrivna handlingar.

Vad består de elektronisk underskrivna och inkomna handlingarna av

- Din gallringsutredning behöver beskriva vad aktuella typer av handlingar har för beståndsdelar när de kommer in till myndigheten, dvs. handlingarnas ursprungliga skick. Du bör därför utreda följande:
  - När inkommer handlingarna till av myndigheten anvisat mottagningsställe?
  - Vad utgör de av kunden eller den externa organisationen ingivna uppgifterna i handlingarna?
  - Vilka valideringsdata medföljer handlingarna till myndigheten – får myndigheten
    - identitetsintyg/OCSP-svar/e-legitimation,
    - en elektronisk underskrift/intyg om underskriften, och
    - andra liknande uppgifter?

Vilka ytterligare handlingar upprättas

- I samband med den äkthetskontroll som din myndighet gör av de elektroniskt underskrivna handlingar som inkommer, avseende till exempel informationsinnehåll och avsändare, kan ytterligare uppgifter och handlingar upprättas. Du behöver identifiera även dem i en gallringsutredning, till exempel
  - uppgifter om utfallet av en äkthetskontroll,
  - nya handlingar i nya format (till exempel Pdf eller Tiff) som framställs ur en ursprunglig handling och används vid din myndighets ärendehandläggning, och
  - nya handlingar (och handlingarnas delar) som produceras vid myndighetsstämpling (se nedan)

Framställan till Riksarkivet

- När gallring inte kan ske genom en tillämpning av RA-FS, och inte heller inom ramen för en registerlag, behöver din myndighet ge in en framställan till Riksarkivet om en myndighetsspecifik föreskrift (RA-MS) för att få gallra. Eftersom det inte finns någon RA-FS som specifikt tar upp gallring av elektroniskt underskrivna handlingar är det lämpligt att din myndighet framställer till Riksarkivet om sådan gallring. En sådan framställan bör utgå från en beskrivning av:
  - processen för elektroniskt underskrivna handlingar,
  - vilka handlingar som skapas i den processen,
  - om och i sådana fall vilken betydelse handlingarna och dess valideringsdata kan ha för allmänhetens rätt till insyn i myndighetens verksamhet eller för forskningen,

- vilken funktion och vilket bevisvärde handlingarna och dess valideringsdata har för din myndighets verksamhet och ur ett rättsligt perspektiv, och
- när din myndighet bedömer att handlingarna inte längre har något värde ur dessa aspekter utan kan gallras.

- En framställan kan till exempel omfatta förslag till gallring av:
  - de expedierade handlingar där legitimering eller underskrift begärs,
  - de ursprungliga handlingarnas valideringsdata efter att din myndighet gjort en äkthetskontroll och dokumenterat den, eller
  - de ursprungliga handlingarna (ingivarnas uppgifter i dess originalformat) efter att de konverterats till annat format som utgör bevarandeformat (RA-FS 2009:2) och används till exempel i myndighetens handläggning.

- Kan gallring ske inom ramen för en registerlag bör samma delar som ovan beaktas om myndigheten vill utreda tidigare gallring än de gallringsfrister som anges i den aktuella lagen. Om registerlagen inbegriper att en framställan om bevarande bör eller ska göras till Riksarkivet bör upplägget för en sådan framställan vara likartat som en framställan om gallring men med tyngdpunkten på de handlingarnas och valideringsuppgifternas eventuella värde för historiska, statistiska eller vetenskapliga ändamål.
- Se vidare Riksarkivets vägledning om Framställningar om myndighetsspecifika föreskrifter (RA-MS) om vad myndigheterna bör beakta när sådana skrivs.

När bör myndighetsstämpling övervägas?

- Din myndighets elektroniska stämpel kan användas som komplement till den dokumentation som ska visa att hanteringen av elektroniskt underskrivna handlingar följt en säker process. En myndighetsstämpel ska visa att en äkthetskontroll utförts när den elektroniska handlingen kom in till myndigheten och hur denna kontroll utföll samt visa att informationsinnehållet inte ändrats sedan äkthetskontrollen gjordes. Myndighetsstämpling bör primärt övervägas
  - vid längre bevarandetider, där äktheten kan komma att ifrågasättas lång tid efter att handlingen kom in (svårigheter att uppbåda och förklara att processen varit säker över tid),
  - om det ekonomiska eller symboliska värdet av att en handlings äkthet kan bevisas på ett säkert sätt är högt (till exempel om rättsprocesser kan förespås i utlandet), och
  - i form av omstämpling av de stämplade handlingarna, när bevarandetiden är lång (de tidigare stämplingarna kan bli osäkra till följd av den tekniska utvecklingen).

eSam är ett medlemsdrivet program för samverkan mellan myndigheter och Sveriges Kommuner och Landsting (SKL) om digitaliseringen inom det offentliga. Det bildades 2015 som en frivillig fortsättning på E-delegationen och bygger vidare på kunskaper och erfarenheter som byggts upp inom ramen för E-delegationen. En viktig uppgift för programmet är att ge ut vägledningar som skapar förutsättningar för att öka den digitala samverkan inom offentlig förvaltning.

Vägledningarna finns tillgängliga på esamverka.se

I eSam ingår Arbetsförmedlingen, Bolagsverket, Centrala Studiestödsnämnden, eHälsomyndigheten, Ekonomistyrningsverket, Försäkringskassan, Jordbruksverket, Kronofogdemyndigheten, Lantmäteriet, Migrationsverket, Naturvårdsverket, Pensionsmyndigheten, Polisen, Riksarkivet, Skatteverket, Skolverket, Sveriges kommuner och landsting, Statens servicecenter, Tillväxtverket, Transportstyrelsen och Tullverket.