Vem kan man lita på?

Enkel och ändamålsenlig användning av betrodda tjänster i den offentliga förvaltningen

DELBETÄNKANDE AV
UTREDNINGEN OM
BETRODDA TJÄNSTER

STATENS OFFENTLIGA UTREDNINGAR

SOU 2021:9

Vem kan man lita på?

Enkel och ändamålsenlig användning av betrodda tjänster i den offentliga förvaltningen

Delbetänkande av Utredningen om betrodda tjänster

Stockholm 2021

STATENS OFFENTLIGA UTREDNINGAR

SOU 2021:9

SOU och Ds finns på regeringen.se under Rättsliga dokument.

Svara på remiss – hur och varför
Statsrådsberedningen, SB PM 2003:2 (reviderad 2009-05-02).
Information för dem som ska svara på remiss finns tillgänglig på regeringen.se/remisser.

Layout: Kommittéservice, Regeringskansliet
Omslag: Elanders Sverige AB
Tryck och remisshantering: Elanders Sverige AB, Stockholm 2021

ISBN 978-91-525-0029-3
ISSN 0375-250X

Till statsrådet Anders Ygeman

Regeringen beslutade den 12 mars 2020 att tillkalla en särskild utredare med uppdrag att utreda och lämna förslag för ökad och standardiserad användning av betrodda tjänster i syfte att höja säkerheten och stärka tilliten när de används i den offentliga förvaltningen.

Som särskild utredare förordnades från och med den 23 mars 2020 målkanslichefen Henrik Ardhede.

Den 17 december 2020 beslutades om tilläggsdirektiv till utredningen.

Som sekreterare i utredningen anställdes från och med den 23 mars uppdragsledaren Eva Sartorius och från och med den 30 mars 2020 juristen Philip Levin. Eva Sartorius avslutade sitt arbete i utredningen den 31 augusti 2020 och från och med samma dag förordnades seniora handläggaren Björn Scharin som utredningssekreterare.

Som experter att biträda utredningen förordnades den 27 april 2020 näringspolitiska experten och förbundsjuristen My Bergdahl (IT & Telekomföretagen), seniora digitala strategen Anna Fors (Försäkringskassan), ramavtalsförvaltaren Pedra Herdegen (Kammarkollegiet), tjänsteområdesansvarig Lotta Hämäläinen (Myndigheten för digital förvaltning), sektionschefen Lotta Nordström (Sveriges Kommuner och Regioner), seniora handläggaren Björn Scharin (Post- och telestyrelsen), it-arkitekten David Skullered (E-hälsomyndigheten), chefen Dag Ströman (Sveriges Certifieringsorgan för IT-säkerhet vid Försvarets materielverk), seniora handläggaren Gustav Söderlind (Myndigheten för samhällsskydd och beredskap), departementssekreteraren Sophie Ankarcrona Thelin (Infrastrukturdepartementet) och utredaren Benjamin Yousefi (Riksarkivet).

Björn Scharin entledigades från sitt uppdrag som expert den 31 augusti 2020 och den 1 september 2020 förordnades uppdragsledaren Eva Sartorius (Myndigheten för digital förvaltning) att vara expert i utredningen.

Utredningen redogör för uppdraget med användande av vi-form även om det inte funnits fullständig samsyn i alla delar. Utredningen, som har tagit sig namnet Utredningen om betrodda tjänster, överlämnar härmed delbetänkandet *Vem kan man lita på? – Enkel och ändamålsenlig användning av betrodda tjänster i den offentliga förvaltningen* (SOU 2021:9). Återstående frågor som omfattas av utredningens uppdrag kommer att behandlas i slutbetänkandet i juni 2021.

Göteborg i februari 2021

Henrik Ardhede

/Philip Levin
Björn Scharin

Innehåll

Vissa förkortningar

EU-rättsakter

Dataskyddsförordningen	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
eIDAS-förordningen	Europaparlamentets och rådets 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
Tjänstedirektivet	Europaparlamentets och rådets direktiv 2006/123/EG av den 12 december 2006 om tjänster på den inre marknaden
Signaturdirektivet	Europaparlamentets och rådets direktiv 1999/93/EG av den 13 december 1999 om ett gemenskapsramverk för elektroniska signaturer

Övriga förkortningar

a.a.	anfört arbete
CEF	Fonden för ett sammanlänkat Europa
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CSEC	Sveriges Certifieringsorgan för IT-säkerhet vid Försvarets materielverk
DID	Decentralised Identifiers
Dir.	Kommittédirektiv
Ds	Departementsserien
DSS	Digital Signature Service
EU	Europeiska unionen
f./ff.	följande sida/sidor
FMV	Försvarets materielverk
DIGG	Myndigheten för digital förvaltning
ENISA	Europeiska unionens cybersäkerhetsbyrå
eSam	eSamverkansprogrammet
ETSI	European Telecommunications Standards Institute
FESA	Forum of European Supervisory Authorities for trust service providers
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
ITS	Sveriges Informations- och Telekommunikationsstandardisering
ITU	International Telecommunication Union
MSB	Myndigheten för samhällsskydd och beredskap

NJA	Nytt Juridiskt Arkiv
NOBID	Nordic-Baltic co-operation on digital identities
OSL	Offentlighets- och sekretesslagen (2009:400)
PKI	Public Key Infrastructure
prop.	Regeringens proposition
PTS	Post- och telestyrelsen
RH	Rättsfall från hovrätterna
RIF	Rättsväsendets informationsförsörjning
RSA	Rivest–Shamir–Adleman (krypteringsalgoritm)
RÅ	Regeringsrättens årsbok
SAMFI	Samverkansgruppen för informationssäkerhet
SDK	Säker digital kommunikation
SEK	Svensk Elstandard
SGSI	Swedish Government Secure Intranet
SHA	Secure Hash Algortihm
SIS	Svenska institutet för standarder
SKA	Samrådsgruppen för kommunala arkivfrågor
SKR	Sveriges Kommuner och Regioner
SOU	Sveriges Offentliga Utredningar
SSI	Self Sovereign Identity
Swedac	Styrelsen för ackreditering och teknisk kontroll
TF	Tryckfrihetsförordningen
UD	Utrikesdepartementet
XML	Extensible Markup Language

Sammanfattning

Inledning

Den starkaste drivkraften bakom användningen av betrodda tjänster inom den offentliga förvaltningen är givetvis den digitalisering som alltjämt pågår i samhället. Även om vissa betrodda tjänster funnits under lång tid pekar vårt kartläggningsarbete mot att behoven rörande dessa tjänster fortsatt kommer att öka. Detta beror delvis på att allt fler processer och arbetsmoment i den offentliga förvaltningen digitaliseras, delvis på att allmänhetens förväntningar om att genomföra sina ärenden digitalt ökar. Det förekommer även författningsbestämmelser som ställer krav på användning av vissa betrodda tjänster. Den i skrivande stund pågående pandemin har därtill accelererat den offentliga förvaltningens digitaliseringstakt och därigenom dess behov av betrodda tjänster.

Utredningen har i uppdrag att kartlägga och analysera den offentliga förvaltningens behov av åtgärder för ökad och standardiserad användning av betrodda tjänster samt lämna förslag på sådana åtgärder. En slutsats som kan dras av kartläggningsarbetet är att det inte finns något isolerat värde i en ökad användning av betrodda tjänster i den offentliga förvaltningen. Värdet av en ökad användning kommer i stället när betrodda tjänster utifrån verksamhetens behov används på ett ändamålsenligt sätt. Utredningens förslag i detta delbetänkande fokuserar därmed i stort på sådana åtgärder som leder till en enkel och ändamålsenlig användning av betrodda tjänster i den offentliga förvaltningen.

Kartläggning av den offentliga förvaltningens behov

Vår kartläggning visar att den offentliga förvaltningen i dagsläget upplever störst behov av att på olika sätt kunna använda och hantera elektroniska underskrifter. Många aktörer upplever osäkerhet kring vissa eller alla steg i hanteringen av elektroniska underskrifter. Det kan gälla allt från bedömningen av om underskrifter krävs till bevarandet av elektroniskt undertecknade handlingar. Vi bedömer att det finns ett stort behov av ett mer samlat och utvecklat stöd för förvaltningen att tillgå för dessa frågor. Vidare visar kartläggningen att det finns ett behov av stöd som gör det enklare att kunna validera elektroniska underskrifter, framför allt sådana som lämnas in till förvaltningen. Det finns bl.a. en osäkerhet kring om en betrodd tjänst som har skapat en underskrift, eller tillhandahållaren av tjänsten, lever upp till de krav som ställs i eIDAS-förordningen.

Elektroniska stämplar, som en form av utställarverifikation, används endast i begränsad omfattning i förvaltningen. Eftersom flera aktörer har framfört att de ser ett behov av att i framtiden kunna använda elektroniska stämplar samt gett uttryck för utmaningar där elektroniska stämplar hade varit en lämplig lösning finns det ett behov av stöd rörande användningen även av dessa tjänster.

När det gäller elektroniska tidsstämplingar, certifikat för autentisering av webbplatser och elektroniska tjänster för rekommenderade leveranser har kartläggningen inte visat att förvaltningen i dagsläget upplever något behov av dessa specifika tjänster som föranleder förslag från vår sida.

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

Utredningen ska enligt direktiven tydliggöra när avancerade respektive kvalificerade elektroniska underskrifter bör användas i den offentliga förvaltningen. I Sverige finns det en utbredd användning av avancerade elektroniska underskrifter medan kvalificerade elektroniska underskrifter endast används i begränsad omfattning. I dagsläget finns det vidare ett relativt stort antal tillhandahållare av betrodda tjänster i Sverige. Det finns emellertid endast två tillhandahållare som är kvalificerade.

Vi ser inget självändamål med en ökad användning av kvalificerade elektroniska underskrifter. Enligt vår uppfattning är det inte heller lämpligt att på en generell nivå slå fast när avancerade respektive kvalificerade elektroniska underskrifter bör användas. Detta kräver en kartläggning av vilka behov en specifik verksamhet har och vilka krav som externa regelverk uppställer. Utifrån en sådan kartläggning går det sedan att bedöma om elektroniska underskrifter bör användas samt eventuell nivå för sådana underskrifter. Utan att ha full inblick i behoven går det inte att göra en fullgod bedömning om det är mest lämpligt att använda avancerade eller kvalificerade elektroniska underskrifter. Det är således behoven i de enskilda processerna där underskrifterna ska användas som måste avgöra. Detta gäller både när aktörer i den offentliga förvaltningen fattar besluten på egen hand och vid utformning av författningsbestämmelser som reglerar användning av elektroniska underskrifter. Även om vi inte anser det lämpligt att fastställa när respektive nivå ska användas kan vi utifrån vår kartläggning dra vissa slutsatser om faktorer som bör påverka bedömningen. Exempelvis talar den interoperabilitet som en kvalificerad elektronisk underskrift har för att använda denna typ av underskrift i gränsöverskridande sammanhang.

En utökad tillitsförteckning

Vår kartläggning visar att många aktörer inom förvaltningen upplever det som svårt att bedöma om vissa betrodda tjänster lever upp till kraven i eIDAS-förordningen. Detta påverkar även möjligheterna att anskaffa tjänster för skapande av avancerade elektroniska underskrifter och förutsättningarna för att validera dessa underskrifter.

Varje medlemsstat i EU ska enligt eIDAS-förordningen upprätta, underhålla och offentliggöra en förteckning över kvalificerade tillhandahållare av betrodda tjänster och de kvalificerade betrodda tjänster som dessa aktörer tillhandahåller. Det främsta användningsområdet för förteckningarna är att de möjliggör kontroll och validering av kvalificerade betrodda tjänster. Det finns emellertid inga hinder mot att även föra upp icke kvalificerade tillhandahållare och icke kvalificerade betrodda tjänster på förteckningen. En europeisk infrastruktur finns alltså redan på plats som möjliggör de kontroller som förvaltningen efterfrågar. Vi anser därför att en utökning av den för-

teckning som redan existerar i Sverige är det bästa sättet att tillgodose behoven och även det lämpligaste alternativet sett till de EU-rättsliga aspekterna då området i stor utsträckning är harmoniserat och att nationella lösningar kan uppställa hinder mot den fria rörligheten. En utökning av förteckningen hade även höjt säkerheten och stärkt tilliten vid användning av betrodda tjänster.

Vi föreslår att förteckningen ska benämnas tillitsförteckning och att tjänster som skapar och validerar avancerade elektroniska underskrifter eller stämplar ska få föras upp på förteckningen. Tillhandahållare eller tjänster förs upp på förteckningen efter en ansökningsprocess som innefattar en kontroll av om de uppfyller vissa kriterier och tekniska krav.

En nationell valideringstjänst

Vårt kartläggningsarbete har visat att många aktörer inom förvaltningen upplever svårigheter med valideringen av elektroniska underskrifter. Många har även framfört behov av en förvaltningsgemensam valideringstjänst som stödjer validering av både utländska och svenska elektroniska underskrifter. Vi bedömer att en nationell valideringstjänst för validering av elektroniska underskrifter och stämplar som både inkommer till och skapas av offentliga aktörer hade starkt bidragit till att lösa denna problematik. Det finns även stora samordningsvinster för förvaltningen med en sådan lösning.

Vi föreslår att Myndigheten för digital förvaltning (DIGG) ska tillhandahålla en sådan valideringstjänst och att den ska benämnas nationell valideringstjänst. Det ska finnas både en central version och en möjlighet att ha lokalt installerade versioner av tjänsten. Tjänsten ska vara tillgänglig för statliga myndigheter, kommuner, regioner, offentligt styrda organ och privata aktörer som yrkesmässigt bedriver verksamhet som till någon del är offentligt finansierad inom vissa utpekade områden. Även enskilda mottagare av elektroniskt undertecknade och stämplade handlingar som skapats av ovan nämnda aktörer ska kunna använda tjänsten för att validera sådana handlingar.

Stöd för att underlätta bevarande av elektroniskt undertecknade och stämplade handlingar

Bevarande av elektroniskt undertecknade och stämplade handlingar är ett område där vår kartläggning visat att det finns stora behov av tekniska lösningar och andra stöd avseende de bedömningar som behöver göras. Den grundläggande problematiken med bevarande av elektroniskt undertecknade och stämplade handlingar är att dessa har en tidsbegränsad giltighet som grundar sig både i tillgång till nödvändiga kontrollkällor samt krypteringsnyckelns livslängd. En kompletterande åtgärd som en myndighet kan företa är att stämpla handlingen och dess valideringsdata med myndighetens elektroniska stämpel. Eftersom dessa stämplar bygger på samma teknologi som den undertecknade eller stämplade handling som stämplas kommer man med denna lösning dock inte helt runt den grundläggande problematiken med tidsbegränsad giltighet.

En lösning som tagits fram för att hantera denna problematik är s.k. valideringsintyg. Valideringsintyg är en metod som underlättar möjligheten att skapa en härledningsbar kedja av bevis som kan påvisa den ursprungliga giltigheten av en underskrift eller stämpel vars kontrollfunktion inte längre kan valideras som giltig. Metoden bevarar alltså inte eller förlänger livslängden av den ursprungliga kontrollfunktionen, men bestyrker den och alla andra bestyrkanden.

Vi bedömer att användandet av valideringsintyg potentiellt kan medföra sådana fördelar för den offentliga förvaltningen i stort att frågan bör utredas vidare. Vi föreslår därför att Riksarkivet och DIGG får i uppdrag att utreda förutsättningarna för att använda valideringsintyg som metod för att bevara undertecknade och stämplade handlingars giltighet. Myndigheterna ska även utreda förutsättningarna för att valideringsintygen skapas inom ramen för den nationella valideringstjänsten.

Utöver den tekniska lösning som valideringsintyg kan innebära har kartläggningen även visat att det finns ett stort behov av ökat stöd rörande bedömningar kring bevarande och gallring av elektroniskt undertecknade eller stämplade handlingar. Vi föreslår därför att Riksarkivet ska få i uppdrag att utreda förutsättningarna för att införa generella bestämmelser och/eller annat stöd avseende bevarande av elektroniskt undertecknade eller stämplade handlingar.

Ett utökat och reformerat stöd till den offentliga förvaltningen

I dagsläget finns det inget samlat stöd eller en för förvaltningen gemensam vägledning rörande införande och hantering av betrodda tjänster. Det finns ett stort behov av sådana stöd och det stöd som finns i dag behöver utökas. I dagsläget är ansvaret för att ge stöd även delat mellan Post- och telestyrelsen (PTS) och DIGG. Vi föreslår att PTS inte längre ska ha i uppgift att ge stöd och information till myndigheter avseende betrodda tjänster. PTS ska dock fortsatt ge sådant stöd till enskilda. DIGG ska i stället enligt vårt förslag få som uppgift att främja användningen av betrodda tjänster. Myndigheten ska även få i uppdrag att ta fram en vägledning för den offentliga förvaltningens användning av betrodda tjänster.

En ökad användning av elektroniska stämplar bör främjas

Den elektroniska stämpelns juridiska funktioner är desamma som den elektroniska underskriftens. Den avgörande skillnaden mellan underskriften och stämpeln är endast att det är en utställarverifikation från en enskild individ respektive en juridisk person. Vi ser att kunskapsnivån rörande vilka användningsområden som elektroniska stämplar kan ha inom den offentliga förvaltningen behöver ökas och vi bedömer att en ökad användning av elektroniska stämplar särskilt bör främjas av DIGG.

Ökad medverkan i standardiseringsarbete

Standarder spelar en stor roll inom området betrodda tjänster. Det standardiseringsarbete i Europa som avser eller påverkar tillhandahållare av betrodda tjänster genomförs i dag av ett antal aktörer och då främst europeiska tillhandahållare av betrodda tjänster, deras underleverantörer, fristående experter och experter från olika medlemsstaters myndigheter. Från Sverige deltar bl.a. ett fåtal tillhandahållare av betrodda tjänster och experter. Svenska myndigheter bidrar och deltar i dag endast i begränsad omfattning i arbetet. Vi anser att Sveriges påverkan på standardiseringsarbetet kan förbättras.

Vår uppfattning är vidare att det är angeläget att Sverige tar en mer aktiv roll i det relevanta standardiseringsarbetet.

Både DIGG och PTS har i sina instruktioner uppdrag som avser standardisering. Vår bedömning är att det standardiseringsarbete som bedrivs avseende betrodda tjänster kan samordnas i större utsträckning än vad som sker i dag. Vi bedömer också att det finns behov av ett mer strategiskt arbete och att resurser tillsätts i sådan utsträckning att Sverige kan påverka utifrån sina prioriteringar på området. Mot den bakgrunden föreslår vi att regeringen ger DIGG och PTS i uppdrag att, i samråd med relevanta aktörer på området, ta fram en handlingsplan för hur Sverige ska kunna påverka standardiseringsarbetet i större utsträckning än i dag.

Utformning av författningsbestämmelser rörande underskrifter

Författningsbestämmelser rörande användning av elektroniska underskrifter är inte enhetligt utformade. I syfte att uppnå en mer enhetlig och långsiktigt utformad lagstiftning anser vi att bestämmelser som tillåter användning av elektroniska underskrifter som huvudregel bör vara teknikneutralt utformade. Angivande av vilken nivå av elektronisk underskrift som krävs bör endast anges i lag om det bedöms nödvändigt för att säkerställa en tillräckligt hög nivå av informationssäkerhet för det sammanhang där underskriften ska förekomma.

Teknikneutraliteten bör inte heller nödvändigtvis avgränsas till underskrifter. Teknikneutrala bestämmelser bör även enligt vår mening utformas så att de möjliggör användning av elektroniska stämplar när det är lämpligt.

1 Författningsförslag

1.1 Förslag till lag om ändring i lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering

Härigenom föreskrivs i fråga om lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering

dels att det ska införas fem nya paragrafer, 7–11 §§, och närmast före 7 § respektive 9 § två nya rubriker av följande lydelse,

dels att nuvarande 7 och 8 §§ ska betecknas 12 och 13 §§,

dels att rubrikerna närmast före nuvarande 7 och 8 §§ ska sättas närmast före 12 respektive 13 §§.

Nuvarande lydelse	*Föreslagen lydelse*
	Tillitsförteckning
	7 §
	Tillsynsmyndigheten ska i enlighet med artikel 22 i EU:s förordning om elektronisk identifiering upprätta, underhålla och offentliggöra en förteckning över kvalificerade tillhandahållare av betrodda tjänster och de kvalificerade betrodda tjänster som dessa aktörer tillhandahåller (tillitsförteckning).

På tillitsförteckningen får även föras upp

1. icke kvalificerade betrodda tjänster som tillhandahålls av kvalificerade tillhandahållare av betrodda tjänster, och

2. icke kvalificerade tillhandahållare av betrodda tjänster och betrodda tjänster som de tillhandahåller.

8 §

Beslut om att föra upp sådana tillhandahållare eller tjänster som avses i 7 § andra stycket på tillitsförteckningen fattas av tillsynsmyndigheten.

Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om

1. kriterier och tekniska krav som icke kvalificerade tillhandahållare av betrodda tjänster ska uppfylla för att föras upp på tillitsförteckningen,

2. vilka icke kvalificerade betrodda tjänster som får föras upp på tillitsförteckningen samt kriterier och tekniska krav för dessa, och

3. ansökningsförfarandet.

Om en icke kvalificerad tillhandahållare av betrodda tjänster eller en icke kvalificerad betrodd tjänst som förts upp på tillitsförteckningen inte längre uppfyller de kriterier och tekniska krav som meddelats med stöd av andra stycket får tillsynsmyndigheten be-

sluta om att avföra tillhandahållaren eller tjänsten från tillitsförteckningen.

Om en icke kvalificerad tillhandahållare av betrodda tjänster begär det ska denne eller en betrodd tjänst denne tillhandahåller avföras från tillitsförteckningen. Detsamma gäller för en kvalificerad tillhandahållare av betrodda tjänster som vill att en icke kvalificerad betrodd tjänst som denne tillhandahåller ska avföras från tillitsförteckningen.

Tillsynsmyndigheten får bestämma att beslut enligt tredje stycket ska gälla omedelbart.

Nationell valideringstjänst

9 §

Den myndighet som regeringen bestämmer ska tillhandahålla en tjänst som validerar elektroniska underskrifter och stämplar (nationell valideringstjänst).

Den nationella valideringstjänsten får användas av

1. offentliga aktörer, och

2. enskilda som validerar elektroniska underskrifter och elektroniska stämplar som skapats av offentliga aktörer.

Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om den nationella valideringstjänstens funktionalitet, tekniska specifikationer

samt villkor och avgifter för användning av tjänsten.

10 §

Med en offentlig aktör avses

1. en statlig eller kommunal myndighet,

2. en beslutande församling i en kommun eller region,

3. ett sådant offentligt styrt organ som avses i andra stycket,

4. en sammanslutning som inrättats särskilt för att tillgodose behov i det allmännas intresse, under förutsättning att behovet inte är av industriell eller kommersiell karaktär, och som består av

a) en eller flera myndigheter eller församlingar som anges i 1 och 2, eller

b) ett eller flera organ enligt andra stycket,

5. en privat aktör som yrkesmässigt bedriver verksamhet som till någon del är offentligt finansierad och som

a) aktören bedriver i egenskap av enskild huvudman inom skolväsendet eller huvudman för en sådan internationell skola som avses i 24 kap. skollagen (2010:800),

b) utgör hälso- och sjukvård enligt hälso- och sjukvårdslagen (2017:30) eller tandvård enligt tandvårdslagen (1985:125),

c) bedrivs enligt socialtjänstlagen (2001:453), lagen (1988:870) om vård av missbrukare i vissa fall, lagen (1990:52) med sär-

skilda bestämmelser om vård av unga eller lagen (1993:387) om stöd och service till vissa funktionshindrade, eller

d) utgör personlig assistans som utförs med assistansersättning enligt 51 kap. socialförsäkringsbalken, och

6. en enskild utbildningsanordnare med tillstånd att utfärda examina enligt lagen (1993:792) om tillstånd att utfärda vissa examina, och som till största delen har statsbidrag som finansiering av högskoleutbildning på grundnivå eller avancerad nivå eller av utbildning på forskarnivå.

Med ett offentligt styrt organ avses en sådan juridisk person som tillgodoser behov i det allmännas intresse, under förutsättning att behovet inte är av industriell eller kommersiell karaktär, och

1. som till största delen är finansierad av staten, en kommun, en region eller någon av de offentliga aktörer som avses i första stycket 1–4,

2. vars verksamhet står under kontroll av staten, en kommun, en region eller någon av de offentliga aktörer som avses i första stycket 1–4, eller

3. i vars styrelse eller motsvarande ledningsorgan mer än halva antalet ledamöter är utsedda av staten, en kommun, en region eller någon av de offentliga aktörer som avses i första stycket 1–4.

11 §

Personuppgifter får behandlas i den nationella valideringstjänsten av den myndighet som regeringen enligt 9 § första stycket bestämmer ska tillhandahålla tjänsten om det är nödvändigt för att

1. validera en elektronisk underskrift eller elektronisk stämpel, eller

2. säkerställa efterlevnaden av villkor för användning av tjänsten, om föreskrifter om sådana villkor har meddelats med stöd av denna lag.

Denna lag träder i kraft den 1 januari 2022.

1.2 Förordning om ändring i förordningen (2016:576) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering

Härigenom föreskrivs i fråga om förordningen (2016:576) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering

dels att det ska införas två nya paragrafer, 6 och 7 §§, och närmast före 6 § en rubrik av följande lydelse,

dels att det närmast före 5 § ska införas en ny rubrik av följande lydelse,

dels att 5 § ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	Tillitsförteckning
	5 §
Post- och telestyrelsen ska i enlighet med artikel 22 i förordning (EU) nr 910/2014 upprätta, underhålla och offentliggöra en förteckning över kvalificerade tillhandahållare av betrodda tjänster och de kvalificerade betrodda tjänster som dessa aktörer tillhandahåller.	*Den tillitsförteckning som avses i 7 § lagen med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering får utöver kvalificerade betrodda tjänster även innehålla icke kvalificerade betrodda tjänster som skapar eller validerar avancerade elektroniska underskrifter eller avancerade elektroniska stämplar.* *Post- och telestyrelsen får meddela föreskrifter om* *1. kriterier och tekniska krav som icke kvalificerade tillhandahållare av betrodda tjänster ska uppfylla för att föras upp på tillitsförteckningen,* *2. kriterier och tekniska krav för tjänster som avses i första stycket, och* *3. ansökningsförfarandet.*

Nationell valideringstjänst

6 §

Myndigheten för digital förvaltning ska tillhandahålla den nationella valideringstjänst som avses i 9 § första stycket lagen med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering.

7 §

Den nationella valideringstjänsten ska validera elektroniska underskrifter och elektroniska stämplar som är skapade av betrodda tjänster som finns på den tillitsförteckning som avses i 7 § lagen med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering samt på förteckningar i andra länder som upprättats i enlighet med artikel 22 i EU:s förordning om elektronisk identifiering.

Myndigheten för digital förvaltning får meddela föreskrifter om den nationella valideringstjänstens funktionalitet, tekniska specifikationer och villkor för användning av tjänsten.

Denna förordning träder i kraft den 1 januari 2022.

1.3 Förslag till förordning om ändring i förordningen (2007:951) med instruktion för Post- och telestyrelsen

Härigenom föreskrivs att 4 § i förordningen (2007:951) med instruktion för Post- och telestyrelsen ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*

4 §[1]

Post- och telestyrelsen har till uppgift att

1. främja tillgången till säkra och effektiva elektroniska kommunikationer, inbegripet att se till att samhällsomfattande tjänster finns tillgängliga, och att främja tillgången till ett brett urval av elektroniska kommunikationstjänster,

2. främja utbyggnaden av och följa tillgången till bredband och mobiltäckning i alla delar av landet, inbegripet att skapa förutsättningar för samverkan mellan myndigheter som kan bidra till utbyggnaden av bredband,

3. svara för att möjligheterna till radiokommunikation och andra användningar av radiovågor utnyttjas effektivt,

4. svara för att nummer ur nationella nummerplaner utnyttjas på ett effektivt sätt,

5. främja en effektiv konkurrens,

6. övervaka pris- och tjänsteutvecklingen,

7. bedriva informationsverksamhet riktad till konsumenter,

8. följa utvecklingen när det gäller säkerhet vid elektronisk kommunikation och uppkomsten av eventuella miljö- och hälsorisker,

9. pröva frågor om tillstånd och skyldigheter, fastställa och analysera marknader samt utöva tillsyn och pröva tvister enligt lagen (2003:389) om elektronisk kommunikation,

10. meddela föreskrifter enligt förordningen (2003:396) om elektronisk kommunikation,

11. upprätta och offentliggöra planer för frekvensfördelning till ledning för radioanvändningen samt offentliggöra information av allmänt intresse om rättigheter, villkor, förfaranden och avgifter som rör radiospektrumanvändningen,

[1] Senaste lydelse 2019:1061.

12. tillhandahålla information om frekvensanvändning till Europeiska radiokommunikationskontorets frekvensinformationssystem (EFIS),

13. vara marknadskontrollmyndighet enligt radioutrustningslagen (2016:392),

14. vara tillsynsmyndighet enligt lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering och ge stöd och information till *myndigheter och* enskilda när det gäller betrodda tjänster,

14. vara tillsynsmyndighet enligt lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering och ge stöd och information till enskilda när det gäller betrodda tjänster,

15. följa utvecklingen när det gäller toppdomäner med geografiska namn som har anknytning till Sverige,

16. vara tillsynsmyndighet enligt lagen (2006:24) om nationella toppdomäner för Sverige på internet samt meddela föreskrifter enligt förordningen (2006:25) om nationella toppdomäner för Sverige på internet,

17. verka för robusta elektroniska kommunikationer och minska risken för störningar, inbegripet att upphandla förstärkningsåtgärder, och verka för ökad krishanteringsförmåga,

18. verka för ökad nät- och informationssäkerhet i fråga om elektronisk kommunikation, genom samverkan med myndigheter som har särskilda uppgifter inom informationssäkerhets-, säkerhetsskydds- och integritetsskyddsområdet samt med andra berörda aktörer,

19. lämna råd och stöd till myndigheter, kommuner och regioner och till företag, organisationer och andra enskilda i frågor om nätsäkerhet,

20. vara tvistlösnings- och tillsynsmyndighet enligt lagen (2016:534) om åtgärder för utbyggnad av bredbandsnät och ansvara för informationstjänsten för utbyggnad av bredbandsnät enligt samma lag, och

21. vara tillsynsmyndighet enligt lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.

Denna förordning träder i kraft den 1 januari 2022.

1.4 Förslag till förordning om ändring i förordningen (2018:1486) med instruktion för Myndigheten för digital förvaltning

Härigenom föreskrivs att 3 och 18 §§ i förordningen (2018:1486) med instruktion för Myndigheten för digital förvaltning ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
3 §	
Myndigheten ska	
1. ansvara för den offentliga förvaltningens tillgång till infrastruktur och tjänster för elektronisk identifiering och underskrift,	
2. främja användningen av elektronisk identifiering *och underskrift*,	2. främja användningen av elektronisk identifiering *samt sådana betrodda tjänster som avses i Europaparlamentets och rådets 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)*,
3. tillhandahålla och administrera valfrihetssystem enligt lagen (2013:311) om valfrihetssystem i fråga om tjänster för elektronisk identifiering, samt	
4. ansvara för de svenska förbindelsepunkterna (noderna) för gränsöverskridande elektronisk identifiering i enlighet med *Europaparlamentets och rådets 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 1993/93/EG*	4. ansvara för de svenska förbindelsepunkterna (noderna) för gränsöverskridande elektronisk identifiering i enlighet med eIDAS-förordningen samt rättsakter som har meddelats med stöd av förordningen.

(eIDAS-förordningen) samt rättsakter som har meddelats med stöd av förordningen.	
18 §	
Myndigheten får ta ut avgifter av de myndigheter som har anslutit sig till valfrihetssystem för säker elektronisk identifiering enligt 3 § 3 och för utbildningsverksamhet.	Myndigheten får ta ut avgifter *1.* av de myndigheter som har anslutit sig till valfrihetssystem för säker elektronisk identifiering enligt 3 § 3, *2. av de som nyttjar den nationella valideringstjänst som avses i 9 § första stycket lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering,* *3.* och för utbildningsverksamhet.

Denna förordning träder i kraft den 1 januari 2022.

2 Utredningens uppdrag och arbete

2.1 Utredningens uppdrag

Regeringen beslutade den 12 mars 2020 kommittédirektiv om att ge en särskild utredare i uppdrag att utreda förutsättningarna för ökad och standardiserad användning av betrodda tjänster i den offentliga förvaltningen i syfte att höja säkerheten och stärka tilliten när betrodda tjänster används. Av utredningsdirektiven framgår bl.a. att utredaren ska kartlägga och analysera den offentliga förvaltningens behov av åtgärder för ökad och standardiserad användning av betrodda tjänster samt lämna förslag på sådana åtgärder. Utredaren ska även lämna nödvändiga författningsförslag.

Regeringen beslutade den 17 december 2020 om tilläggsdirektiv. Av tilläggsdirektiven följer att den del av uppdraget som avser åtgärder för ökad och standardiserad användning av betrodda tjänster enligt punktuppställningen nedan ska redovisas senast den 15 februari 2021.

I delredovisningen ska följande ingå

- kartläggning och analys av den offentliga förvaltningens behov av åtgärder för ökad och standardiserad användning av betrodda tjänster,
- förslag på sådana åtgärder och nödvändiga författningsförslag, särskilt när det gäller att
  - tydliggöra när avancerade respektive kvalificerade elektroniska underskrifter bör användas i den offentliga förvaltningen, och
  - validera och bevara elektroniska underskrifter.

Resterande delar av uppdraget som framgår av utredningens ursprungliga direktiv ska slutredovisas den 30 juni 2021.

Utredningens direktiv finns bifogade till delbetänkandet i bilaga 1 och 2.

2.2 Utredningens arbete

Utredningsarbetet påbörjades i slutet av mars 2020. Under utredningstiden har vi hittills haft fem sammanträden med expertgruppen. Till följd av den rådande pandemin har alla utredningens möten genomförts digitalt.

Utredningens uppdrag har delvis varit att genomföra en kartläggning av den offentliga förvaltningens behov av åtgärder för ökad och standardiserad användning av betrodda tjänster. En del av kartläggningsarbetet har bestått av att ta del av befintligt skriftligt underlag som berör den aktuella frågeställningen. En central källa i detta arbete har varit den s.k. E-legitimationsenkäten som Myndigheten för digital förvaltning (DIGG), Sveriges Kommuner och Regioner (SKR) samt Regeringskansliet genomförde 2019. DIGG och SKR har släppt varsin rapport baserat på resultatet av enkäten.[1] Relevanta behov och utmaningar har också lyfts fram i tidigare utredningars arbete, bl.a. av Utredningen om effektiv styrning av nationella digitala tjänster och Digitaliseringsrättsutredningen.[2] Vi har därtill mottagit skriftliga underlag från både myndigheter och tillhandahållare av betrodda tjänster.

För att komplettera det skriftliga underlaget har vi vidare genomfört ett 40-tal möten och samtal med aktörer i offentlig förvaltning samt med tillhandahållare av betrodda tjänster.

I syfte att inhämta synpunkter från en bredare grupp av myndigheter samt tillhandahållare av betrodda tjänster har vi även genomfört sammanlagt fem digitala möten med öppen anmälan. De första mötena hölls i maj 2020 och hade ingen deltagarbegränsning. Vid mötet för representanter för offentlig förvaltning medverkade ca 220 deltagare och vid mötet med tillhandahållare av betrodda tjänster medverkade ca 40 deltagare. I oktober 2020 arrangerades tre möten där deltagarantalet begränsades för att skapa bättre förutsättningar för fördjupade diskussioner. Två möten arrangerades med deltagare från offentlig för-

[1] DIGG, *E-legitimering inom den offentliga förvaltningen – Enkätundersökning 2019* (dnr 2019-389) och SKR, *Rapport enkät e-legitimationer – 2019 Kommuner och Regioner*, mars 2020.
[2] Se *reboot – omstart för den digitala förvaltningen (*SOU 2017:114) och *Juridik som stöd för förvaltningens digitalisering* (SOU 2018:25).

valtning med ca 20 deltagare per möte och ett möte med deltagare från tillhandahållare av betrodda tjänster, även det med ca 20 deltagare.

Vi har enligt våra direktiv haft att beakta relevant arbete som bedrivs inom Regeringskansliet och utredningsväsendet samt särskilt beakta det arbete som bedrivs hos DIGG. Vi har under utredningstiden haft flera möten och kontakter med DIGG. Vi har även haft kontakt med flera statliga utredningar, däribland Cybersäkerhetsutredningen (Fö 2019:01), Ställföreträdarutredningen (Ju 2019:03), It-driftsutredningen (I 2019:03) och Utredningen om elektroniska underskrifter på regeringsbeslut (Ju 2020:13).

Vi har vidare enligt våra direktiv haft att undersöka och översiktligt redovisa hur de frågor som uppdraget omfattar hanteras i andra länder som är jämförbara med Sverige. I detta syfte har vi utöver en granskning av tillgängligt material på internet haft kontakter med myndighetsrepresentanter i Danmark, Norge, Nederländerna, Italien och Österrike. Vi har även tagit del av den undersökning avseende betrodda tjänster i de nordiska och baltiska länderna som under 2020 genomförts av Nordic-Baltic co-operation on digital identities (NOBID).[3]

Vi har också presenterat vårt uppdrag för olika nätverk och arbetsgrupper samt haft kontakt med företrädare för Europeiska kommissionen.

Visst underlag till konsekvensutredningen har tagits fram av Analysys Mason AB på vårt uppdrag.

2.3 Utredningens prioriteringar

I relation till den begränsade tid vi haft till förfogande har vi valt att prioritera frågor som enligt vår bedömning kan åstadkomma störst nytta för den offentliga förvaltningen som helhet. Vi har därtill valt att särskilt lyfta fram informationssäkerhetsfrågor då det av utredningens direktiv framgår att syftet med utredningen är att höja säkerheten och stärka tilliten när betrodda tjänster används.

[3] Hinsberg, Hille m.fl., *Study on Nordic-Baltic Trust Services*, 2020.

2.4 Delbetänkandets disposition

I kapitel 3 definieras några för delbetänkandet centrala begrepp och termer.

I kapitel 4 redogörs för på vilka sätt betrodda tjänster eller deras motsvarigheter inom pappersbaserade processer används, eller kan användas, i den offentliga förvaltningen

I kapitel 5 redogörs översiktligt för teknik, bestämmelser och standarder avseende betrodda tjänster.

Kapitel 6 innehåller en redovisning av de behov och utmaningar kopplade till användning av dessa tjänster som vår kartläggning har visat.

I kapitel 7 redogör vi för det nationella utrymmet att reglera betrodda tjänster.

I kapitel 8 presenteras utredningens förslag.

Kapitel 9 behandlar de potentiella risker för den offentliga förvaltningen och samhället i stort som måste beaktas i samband med användning av betrodda tjänster.

I kapitel 10 redogör vi för konsekvenserna av våra förslag.

I kapitel 11 behandlas ikraftträdande och i kapitel 12 finns författningskommentarerna.

3 Definitioner av vissa centrala begrepp och termer

3.1 Betrodda tjänster

Det centrala regelverket inom området betrodda tjänster utgörs av EU-förordningen (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden, härefter kallad eIDAS-förordningen (förordningen i dess helhet återfinns i bilaga 3 till detta delbetänkande). Termen betrodda tjänster definieras i artikel 3.16 i eIDAS-förordningen som en elektronisk tjänst som vanligen tillhandahålls mot ekonomisk ersättning och som består av

- skapande, kontroll och validering av elektroniska underskrifter, elektroniska stämplar eller elektroniska tidsstämplingar, elektroniska tjänster för rekommenderade leveranser och certifikat med anknytning till dessa tjänster, eller
- skapande, kontroll och validering av certifikat för autentisering av webbplatser, eller
- bevarande av elektroniska underskrifter, stämplar eller certifikat med anknytning till dessa tjänster.

Betrodda tjänster är således enkelt uttryckt elektroniska tjänster som erbjuder vissa utpekade funktioner kopplade till elektroniska underskrifter, elektroniska stämplar, elektroniska tidsstämplingar eller certifikat för autentisering av webbplatser. Dessutom är elektroniska tjänster för rekommenderade leveranser betrodda tjänster i sig.

3.2 Certifikat

I eIDAS-förordningen definieras i artikel 3.14 och 3.29 certifikat som ett intyg som kopplar valideringsuppgifter för en elektronisk underskrift eller en elektronisk stämpel till en fysisk person respektive juridisk person och bekräftar åtminstone namnet eller pseudonymen på den personen. Annorlunda uttryckt kan ett certifikat beskrivas som ett elektroniskt intyg som bl.a. innehåller uppgifter som möjliggör validering av t.ex. en elektronisk underskrift eller elektronisk stämpel. Certifikat är även, vad avser autentisering av webbplatser, ett intyg som gör det möjligt att autentisera en webbplats och koppla webbplatsen till den fysiska eller juridiska person som certifikatet utfärdats för.

3.3 Validering

Validering är ett begrepp som används inom flera discipliner och som innebär någon form av granskning och godkännande av dokument, kunskaper eller kravhantering.[1] I relation till betrodda tjänster betyder validering enligt artikel 3.41 i eIDAS-förordningen kontroll och bekräftelse av elektroniska underskrifters giltighet. Validering sker emellertid även av elektroniska stämplar. Med validering avses alltså i detta sammanhang en tjänst som kompletterar användningen av elektroniska underskrifter och stämplar och som kontrollerar att t.ex. en elektronisk underskrift eller stämpel är äkta.

3.4 Tillhandahållare

Leverantörer av betrodda tjänster benämns i eIDAS-förordningen som tillhandahållare. I artikel 3.19 i förordningen definieras tillhandahållare som en fysisk eller juridisk person som tillhandahåller en eller flera betrodda tjänster, antingen i egenskap av kvalificerade eller icke kvalificerade tillhandahållare av betrodda tjänster. För att följa förordningens systematik kommer därför termen tillhandahållare att användas i delbetänkandet i stället för det i vardagligt språkbruk mer frekvent förekommande begreppet leverantör.

[1] Se t.ex. 20 kap. 42 § skollagen (2010:800).

3.5 Förlitande part

En förlitande part är enligt artikel 3.6 i eIDAS-förordningen en fysisk eller juridisk person som förlitar sig på en elektronisk identifiering eller betrodda tjänster. Med andra ord är den förlitande parten den som exempelvis tar emot en elektroniskt undertecknad handling och som ska kunna förlita sig på att den är undertecknad av den person som handlingen anger.

3.6 Underskrift och andra närliggande begrepp

Det finns ett antal begrepp som förekommer i relation till begreppet underskrift som i vissa fall är synonyma och i andra fall inte. Det sätt på vilket begreppen används i olika sammanhang kan ge upphov till både viss förvirring och missförstånd. De begrepp som är vanligast förekommande i dessa sammanhang är – utöver underskrift – signatur, namnteckning, namnunderskrift, egenhändig underskrift/egenhändigt undertecknande samt urkund. För att tydliggöra vilken innebörd vi anser att de har i dagens kontext samt i delbetänkandet behövs en närmare genomgång av respektive begrepp och i vilka sammanhang de förekommer.

Det finns ingen legaldefinition av begreppet underskrift. I eIDAS-förordningen definieras i artikel 3.10 emellertid en elektronisk underskrift som uppgifter i elektronisk form som är fogade till eller logiskt knutna till andra uppgifter i elektronisk form och som används av undertecknaren för att skriva under.

Underskrift är enligt vår mening ett teknikneutralt begrepp och kan likaväl åsyfta en underskrift med penna som en elektronisk underskrift skapad med en underskriftstjänst. Begreppet har dock i lagtext tidigare ansetts utgöra ett s.k. formkrav som medför att det krävs en underskrift på papper (se mer om detta i avsnitt 8.9.3).

I Svenska Akademiens ordlista definieras ordet underskrift som en namnteckning i anslutning till dokument. Namnteckning definieras i sin tur som ett personligt sätt att skriva det egna namnet. I Svensk ordbok definieras namnteckning som en persons egenhändigt skrivna namn på det för denne typiska sättet och att namnteckning används för identifiering, särskilt i juridiska sammanhang. Vi anser att begreppet namnteckning är tydligt sammanlänkat med den fysiska handlingen att för hand skriva sitt namn med penna på papper. En namn-

teckning kan dock även ske i elektronisk form när den görs med penna på en elektronisk anordning, ett exempel inom offentlig förvaltning när detta är möjligt är i samband med underskrift av ett föreläggande av ordningsbot i närvaro av polisman.[2]

Egenhändig underskrift eller egenhändigt undertecknade har även en tydlig koppling till den fysiska handlingen att skriva sitt namn.[3] I såväl allmänt språkbruk som i tre nu gällande lagar förekommer begreppet namnunderskrift.[4] Detta begrepp får likt namnteckning anses kopplat till den fysiska handlingen att teckna sitt namn.

Sammantaget anser vi att begreppen namnteckning, namnunderskrift och egenhändig underskrift/egenhändigt undertecknade endast bör användas när det är fråga om den fysiska handlingen att teckna sitt namn, vare sig det sker med penna på papper eller med penna på en elektronisk anordning. Det är även med denna innebörd som dessa begrepp används i detta delbetänkande.[5]

Det tveklöst mest tvetydiga och snåriga begreppet i dessa sammanhang är begreppet signatur. Signatur definieras i Svenska Akademiens ordlista antingen som en förkortad namnteckning eller kortare namn som ersätter en journalists egentliga namn alternativt, enligt en något äldre definition, som en påskrift med bruksanvisning på läkemedelsförpackning. I Svensk ordbok framgår att en signatur är en egenhändigt skriven namnteckning eller förkortad namnteckning som särskilt används för att intyga tillförlitlighet eller äkthet hos dokument, konstverk eller dylikt. Även i rättsfall har det med begreppet signatur åsyftats en förkortad namnteckning i form av signering med initialer.[6]

Begreppen signatur och underskrift används dock ofta som synonymer. Detta gäller i synnerhet avseende elektroniska underskrifter. Detta har bl.a. sin förklaring i att begreppet förekom i föregångaren till eIDAS-förordningen, EU-direktivet om ett gemenskapsramverk för elektroniska signaturer (1999/93/EG), härefter kallat signaturdirektivet. Direktivet låg till grund för den numera upphävda lagen

[2] Prop. 2017/18:126 s. 27 ff.
[3] Se t.ex. RÅ 2002 not 206.
[4] Lag (1995:1570) om medlemsbanker, bostadsrättslag (1991:614) och Kungl. Maj:ts Cirkulär (1973:874) om Sveriges tillträde till europeiska konventionen den 7 juni 1968 om avskaffande av legalisering av handlingar som utfärdas av diplomatiska eller konsulära tjänstemän.
[5] Vad gäller egenhändigt undertecknade kan det noteras att en ändring som införts i rättegångsbalken den 1 januari 2021 i 33 kap. 1 a § föreskriver att en ansökan som enligt en bestämmelse i rättegångsbalken ska vara egenhändigt undertecknad får skrivas under med en sådan avancerad elektronisk underskrift som avses i artikel 3 i eIDAS-förordningen.
[6] Kammarrätten i Stockholms dom den 18 oktober 2002 i mål nr 3099-2002.

(2000:832) om kvalificerade elektroniska signaturer och i lagen benämndes det som nu kallas för elektroniska underskrifter som elektroniska signaturer. Begreppet elektronisk signatur förekom innan eIDAS-förordningen trädde i kraft även i ett 20-tal svenska lagar. Vidare är det i den engelska språkversionen av eIDAS-förordningen begreppet ”electronic signature” som används för att benämna en elektronisk underskrift.

I förarbetena till lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering framfördes att elektronisk signatur i det allmänna språkbruket med tiden kommit att ersättas med elektronisk underskrift men att båda begreppen har samma innebörd.[7] Något som skiljer begreppen åt är däremot att digital signatur även används som en teknisk term för en metod att säkerställa utställare och integritet i samband med en elektronisk underskrift.[8]

Vi anser sammanfattningsvis att även om begreppen underskrift och signatur i allmänt språkbruk har samma innebörd bör den synonyma användningen av begreppen som i dagsläget förekommer inom den offentliga förvaltningen undvikas och att begreppet elektronisk signatur endast ska användas om det är den tekniska termen som avses eller när hänvisning görs till tidigare gällande bestämmelser där begreppet förekommer.

Slutligen bör urkund nämnas. En urkund är enligt legaldefinitionen i 14 kap. 1 § andra stycket brottsbalken:

1. en handling som upprättats till bevis eller annars är av betydelse som bevis och som har en utställarangivelse och originalkaraktär,
2. 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, och
3. ett märke som ställts ut till bevis om en persons identitet eller om en viss rättighet eller prestation och som har originalkaraktär (bevismärke).

Enligt ovan nämnda paragrafs första stycke framgår att den som obehörigen, genom att skriva eller på liknande sätt ange en annan per-

[7] Prop. 2015/16:72 s. 34.
[8] Se bl.a. Riksarkivet, *Framställning och bevarande av elektroniska signaturer (avsnitt 6)* (dnr RA 20-2013-1154), 29 maj 2015, s. 5.

sons namn eller på annat sätt, framställer en falsk urkund eller ändrar eller fyller ut en äkta urkund döms, om åtgärden innebär fara i bevishänseende, för urkundsförfalskning. eSamverkansprogrammet (eSam) har i sin vägledning för införande av e-legitimering och e-underskrifter valt att kalla en sådan urkund som framgår av andra punkten ovan för en e-urkund.[9] Vad avser att en elektronisk handling ska ha en utställarangivelse som kan kontrolleras på ett tillförlitligt sätt kräver detta enligt förarbetena inte någon särskild teknisk eller administrativ lösning. Avgörande är i stället om utställarangivelsen når upp till en viss nivå av tillförlitlighet. Utställarangivelsen ska vidare vara sådan att den typiskt sett förtjänar tilltro och dessutom vara av sådant slag att den typiskt sett faktiskt kan härledas till en viss utställare. Den ska alltså ha en inte obetydlig grad av säkerhet. Det är utställarangivelsen avseende handlingen i dess lagrade form som ska kunna kontrolleras. Som exempel lyftes i förarbetena avancerade och kvalificerade elektroniska signaturer som uppfyllde de krav som uppställdes i den upphävda lagen om kvalificerade elektroniska signaturer.[10]

3.7 Stämpel och sigill

Stämpel definieras i Svenska Akademiens ordlista som en anordning för märkning av dokument m.m. eller ett avtryck efter stämpel. I ett digitalt sammanhang är det dock inte den tekniska lösning som används för att förse en handling med en stämpel som aktualiseras. En elektronisk stämpel behöver inte heller nödvändigtvis lämna någon form av synligt avtryck på den handling som stämplats. I artikel 3.25 i eIDAS-förordningen definieras en elektronisk stämpel som 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. I artikel 3.31 definieras anordning för skapande av elektroniska stämplar som en konfigurerad programvara eller maskinvara som används för att skapa en elektronisk stämpel.

Det finns inte många närbesläktade begrepp till stämpel. Ett av dessa är dock sigill. Sigill definieras i Svenska Akademiens ordlista som ett stämpelavtryck (i stelnat material) som anbringas på dokument eller annat föremål för att symbolisera viss person eller orga-

[9] eSam, *Juridisk vägledning för införande av e-legitimering och e-underskrifter 1.1*, juni 2018, s. 22.
[10] Prop. 2012/13:74 s. 70.

nisation vilket vanligen och ursprungligen avses intyga att personen etc. står bakom dokumentet eller att försändelsen är orörd.

Det kan noteras att begreppet elektronisk stämpel i den engelska språkversionen av eIDAS-förordningen benämns som ”electronic seal”, vilket översatt betyder elektroniskt sigill. Sett till den elektroniska stämpelns funktion (se mer om detta i avsnitt 4.3) är det med hänsyn till definitionerna ovan egentligen närmare den språkliga innebörden av ett sigills funktion. Begreppet elektroniskt sigill användes även när kommissionen lämnade sitt ursprungliga förslag till eIDAS-förordningen.[11]

I den engelska språkversionen av eIDAS-förordningen finns det även en tydligare skiljelinje mellan elektroniska stämplar och elektroniska tidsstämplingstjänster (se mer om elektroniska tidsstämplingstjänster i avsnitt 4.8) då dessa benämns som ”electronic seal” respektive ”electronic time stamp”. Att de svenska begreppen är så pass snarlika har under utredningens kartläggningsarbete av vissa lyfts fram som ett problem då det leder till, eller riskerar att leda till, en sammanblandning av dessa olika typer av betrodda tjänster.

[11] COM(2012) 238 final av den 4 juni 2012, s. 21.

4 Användningsområden för betrodda tjänster

4.1 Inledning

I detta kapitel presenteras på vilka sätt betrodda tjänster eller deras motsvarigheter inom pappersbaserade processer används i den offentliga förvaltningen. Det beskrivs även på vilket sätt vissa betrodda tjänster hade kunnat användas. Gällande underskrifter och stämplar redogörs vidare för de juridiska funktioner som de fyller.

4.2 Underskrifter

4.2.1 Användning av underskrifter inom den offentliga förvaltningen

Att sätta sin namnteckning på olika typer av handlingar är för de allra flesta en rutinmässig åtgärd i dagens samhälle. Inom den offentliga förvaltningen är användningen av underskrifter mycket utbredd. Underskrifter förekommer bl.a. i rent interna processer, vid upprättande av handlingar (t.ex. beslut) som sedan kommuniceras till externa mottagare samt på inkommande handlingar i form av t.ex. ansökningar. Av e-legitimationsenkäten 2019 framgår att 63 procent av besvarande kommuner och 46 procent av besvarande statliga myndigheter angav att de erbjuder möjlighet att skriva under med elektroniska underskrifter.[1]

Användningen av en underskrift, både vanlig och elektronisk, kan vara en följd av formkrav i en författning. Vanligtvis finns det dock andra anledningar till att underskrifter förekommer.

[1] SKR, *Rapport enkät e-legitimationer – 2019 kommuner och regioner*, mars 2020, s. 14.

Digitaliseringsrättsutredningen fann att närmast rutinmässiga krav på undertecknande vid pappersförfaranden i vissa fall synes ha upp-ställts av myndigheter utan att det funnits krav i lag eller förordning som anger att det behövs.[2] Ett exempel på detta är underskrifter i samband med beslutsfattande där krav på undertecknande inte är vanligen förekommande trots att beslut ofta skrivs under.[3] När det gäller inkommande handlingar kan en myndighet enligt 21 § förvaltningslagen (2017:900) begära att en handling bekräftas av avsändaren. Det är dock inget krav och formerna för hur bekräftelsen ska göras regleras inte i lagen.[4]

4.2.2 Vilka juridiska funktioner fyller en underskrift?

Underskrifter används i många olika sammanhang. Det är ofta redan av sammanhanget eller av tradition uppenbart i vilka situationer en underskrift förväntas och vilka följdverkningar detta får. Det är inte heller ovanligt att det uttryckligen anges när en underskrift förväntas och vilka effekter som följer av undertecknandet. Utöver det som av sammanhanget är uppenbart i form av att underskriften exempelvis utgör en bekräftelse eller förbindelse reflekterar de flesta nog inte över vilket eller vilka syften en underskrift fyller. Även om de olika funktionerna ibland kallas för olika saker eller sammanfogas brukar en underskrift generellt anses fylla de fem olika juridiska funktioner som presenteras nedan.[5]

Viljeyttring

En underskrift får anses ge uttryck för en vilja att exempelvis bekräfta något, åta sig en förpliktelse eller lämna en försäkran om att uppgifterna i en handling är med sanningen överensstämmande. Viljefunktionen har också en tillitssida. En mottagare kan, utifrån den undertecknade handlingen, anta att denne kan agera på ett visst sätt.[6]

---

[2] *Juridik som stöd för förvaltningens digitalisering* (SOU 2018:25) s. 461.
[3] eSam, *Juridisk vägledning för införande av e-legitimering och e-underskrifter 1.1*, juni 2018, s. 28
[4] Prop. 2016/17:180, s. 306 f.
[5] Se bl.a. Aversten, Daniel, *Digitala signaturer och ansvarsproblem*, IRI-rapport 1998:2, s. 15, *Digitala signaturer – en teknisk och juridisk översikt* (Ds 1998:14), s. 134 ff. och eSam, *Juridisk vägledning för införande av e-legitimering och e-underskrifter 1.1*, juni 2018, s. 29 f.
[6] *Digitala signaturer – en teknisk och juridisk översikt* (Ds 1998:14), s. 135.

eSam benämner detta som ”avslutningsfunktionen” som innefattar att innehållet är fullständigt och förenligt med undertecknarens vilja.[7]

Varning

Nära kopplad till viljeyttringen är underskriftens varningsfunktion. Även om underskrifter ofta är en rutinmässig handling kan ett betydelsefullt syfte vara att handlingen att skriva under något ska ge upphov till eftertanke. Den som skriver under får anledning att överväga innebörden och vikten av det som undertecknas.[8] Detta är särskilt påtagligt i fall där en underskrift ska bevittnas även om bevittnandet som sådant framför allt uppfyller en bevisfunktion.[9]

Identifikation

En underskrift kan användas för att identifiera den som undertecknat en handling. Detta benämns ibland även som en utställarverifikation eller utställarangivelse eftersom det kopplar handlingen till en utställare. Om det är fråga om en namnteckning är det inte självklart att det enbart med ledning av denna går att identifiera vem som skrivit under. Normalt består en namnteckning av att undertecknaren skriver sitt namn på ett för denne karaktäristiskt sätt. Detta innebär emellertid inte att krav på underskrift inte skulle kunna fullgöras med någon annan typ av tecken, t.ex. ett kryss eller bomärke. Det finns inte heller något krav på att en namnteckning ska vara läslig.[10] Kammarrätten i Stockholm har i ett avgörande även funnit att det inte finns något krav på att en persons fullständiga namn behöver skrivas ut om det inte föreligger någon osäkerhet om att en undertecknad handling härrör från en viss person.[11]

[7] eSam, *Juridisk vägledning för införande av e-legitimering och e-underskrifter 1.1*, juni 2018, s. 29.
[8] Prop. 2017/18:126 s. 22.
[9] Se t.ex. bestämmelserna om upprättande av testamente i 10 kap. ärvdabalken.
[10] *Formel – Formkrav och elektronisk kommunikation* (Ds 2003:29), s. 89.
[11] Kammarrätten i Stockholms dom den 18 oktober 2002 i mål nr 3099-2002.

Äkthet

En underskrift på en handling som innehåller text knyter den person som skrivit under till handlingens innehåll. Detta innebär också ett visst skydd mot manipulation.[12] I fråga om namnteckningar är kopplingen mellan en person och en namnteckning dock inte uppenbar. Även om namnet är läsligt krävs det i princip föregående kunskap om namnteckningens utformning för att ha en möjlighet att upptäcka en förfalskad namnteckning.[13] Dock anses namnteckningar endast med svårighet kunna förfalskas på ett sådant sätt att en förfalskning inte kan upptäckas i efterhand vid närmare analys.[14] När det gäller elektroniska underskrifter innebär underskriften, om den är av mer avancerad art, ett starkare skydd mot manipulation än vad en namnteckning ger. IT-förfalskningsutredningen beskrev skillnaden mellan namnteckningar och elektroniska underskrifter på följande sätt.[15]

Traditionella underskrifter

1. Skrivs på ett självklart sätt

2. Förmågan att underteckna är medfödd och dessa egenskaper – ”skrivdonet” – kan inte komma på avvägar

3. En traditionell underskrift undersöks vanligtvis inte närmare förrän någon bestrider dess äkthet. Material för att analysera signaturen samlas in i efterhand av experter

4. Av erfarenhet vet vi att det är möjligt att lära sig att skriva en annan persons underskrift så att andra lätt vilseleds

5. Procedurerna bygger på en allmän tillit till egenhändiga underskrifter. I vissa fall finns emellertid särskilda rutiner för att kontrollera att en underskrift är äkta; t.ex. vidimering

Elektroniska underskrifter

1. Bygger på kryptografi och innehavet av en hemlighet – en ”nyckel”

2. Användaren brukar en ”nyckel”. Var och en som har tillgång till nyckeln kan underteckna elektroniskt. Nyckeln behöver därför skyddas

[12] *Digitala signaturer – en teknisk och juridisk översik*t (Ds 1998:14), s. 135.
[13] Se t.ex. *Fakturabedrägerier* (SOU 2015:77), s. 281 f.
[14] *Digitala signaturer – en teknisk och juridisk översikt* (Ds 1998:14), s. 136.
[15] *Urkunden I Tiden – en straffrättslig anpassning* (SOU 2007:92), s. 106 f.

3. Var och en som tar emot en elektroniskt underskriven handling behöver kunna kontrollera dess äkthet. Kontrollmaterialet samlas in på förhand, bevaras och hålls tillgängligt. Detta för med sig nya infrastrukturer

4. Det är i princip omöjligt att skapa en annan persons elektroniska underskrift utan att ha tillgång till den privata nyckeln

5. De elektroniska underskrifternas äkthet kontrolleras alltid. Det är viktigt att användaren kan lita på uppgiften om vem nyckeln tillhör. Detta behov tillgodoses genom e-legitimationer och anknytande tjänster

Utöver IT-förfalskningsutredningens uppställning är det även så att den elektroniska underskriften har en unik koppling till den handling som undertecknas eftersom underskriften bl.a. består av ett hashvärde som skapas utifrån den undertecknade handlingens innehåll (se mer om detta i avsnitt 5.2.2). En elektronisk underskrift innebär även att det är möjligt att skilja handlingar som kan kontrolleras på ett tillförlitligt sätt från oskyddade handlingar.[16]

Även om man bör kunna förlita sig på att en enskild individs elektroniska underskrift även skapats av denne individ går det dock inte att fastställa enbart genom en validering av underskriften. Högsta domstolen har i ett mål gällande en låneförbindelse som undertecknats med en avancerad elektronisk underskrift uttalat följande rörande äkthet i relation till elektroniska underskrifter.[17]

> En elektronisk underskrift kan vara äkta i den meningen att den faktiskt har använts och att användningen har skett med tillämpning av relevanta säkerhetslösningar, t.ex. med angivande av innehavarens personliga kod. Av detta går det dock inte att dra någon slutsats beträffande frågan om det är innehavaren eller någon annan som har använt underskriften. På det sättet skiljer sig den elektroniska underskriften från den traditionella på papper.

Bevisverkan

En viktig funktion för underskrifter är som bevis. En underskrift är ett sätt att säkra ett eventuellt framtida behov av att kunna bevisa såväl identiteten på den som undertecknat en handling som kopplingen mellan personen och den undertecknade handlingens inne-

[16] eSam, *Juridisk vägledning för införande av e-legitimering och e-underskrifter 1.1*, juni 2018 s. 23.
[17] NJA 2017 s. 1105.

håll, dvs. identifikations- och äkthetsfunktionerna som beskrivs ovan. Ofta kopplas denna bevisverkan till civilrättsliga avtal. Den är emellertid lika relevant i både förvaltningsrättsliga och straffrättsliga sammanhang. Eftersom det i svenska domstolar råder fri bevisprövning görs ingen åtskillnad mellan namnteckningar och elektroniska underskrifter vad avser deras bevisverkan.[18] När det gäller bevisbördan avseende avancerade elektroniska underskrifter uttalade Högsta domstolen följande i det tidigare nämnda målet.[19]

> Det måste ankomma på långivaren, som är den part som tillhandahåller det bakomliggande tekniska systemet, att säkerställa att tekniken motsvarar högt ställda kvalitetskrav. En avancerad elektronisk underskrift uppfyller sådana krav. Kan en långivare visa att den tekniska lösning som använts för att ingå ett låneavtal motsvarar skapandet av en avancerad elektronisk underskrift, och finns det inget som tyder på att det vid aktuellt tillfälle funnits tekniska problem med det använda systemet, bör kravet på långivaren i allmänhet anses uppfyllt. I ett sådant läge bör utgångspunkten vara att den elektroniska underskriften inte är manipulerad, utan att den har skapats genom identifiering med gäldenärens personliga kod.
>
> …
>
> Om innehavaren hävdar att någon har obehörigen använt hans eller hennes elektroniska underskrift talar flera skäl för att innehavaren måste prestera någon bevisning avseende detta. Det gäller oavsett övriga omständigheter kring avtalsslutet, såsom att innehavaren är en konsument. Det är innehavaren av den elektroniska underskriften som har möjlighet att kontrollera och skydda den säkerhetslösning som ska tillämpas på hans eller hennes sida, exempelvis en personlig kod. Det är vidare innehavaren som vet om han eller hon tidigare har gett någon annan tillgång till koden. Det är även innehavaren som kan känna till händelser som ger anledning till misstanke om t.ex. teknisk manipulation av hans eller hennes dator. Till detta kommer att utgångspunkten att den elektroniska underskriften endast kan skapas av den som har tillgång till den personliga och hemliga koden är ägnad att skapa en tillit hos mottagaren - den förlitande parten - med innebörden att han eller hon ska kunna utgå från att en elektronisk handling kommer från den vars elektroniska underskrift har använts vid undertecknandet.

[18] Principen om fri bevisprövning kommer till uttryck i 35 kap. 1 § rättegångsbalken och innebär att parterna i ett mål får åberopa all bevisning de vill (s.k. fri bevisföring) och att domstolen fritt prövar värdet av den åberopade bevisningen (s.k. fri bevisvärdering).
[19] A.a.

> Med hänsyn till det anförda bör det krävas att innehavaren av den avancerade elektroniska underskriften gör åtminstone antagligt att användandet av underskriften skett obehörigen.

Det aktuella målet gällde en civilrättslig tvist men samma bevisbörda har även använts i förvaltningsrättsliga mål.[20] I straffrättsliga mål är det åklagarens uppgift att utom rimligt tvivel styrka att något har skett. När det gäller avancerade elektroniska underskrifter har det i underrättsavgöranden dock, om vissa omständigheter visats rörande skapandet av underskriften, bedömts att en förklaringsbörda åligger den åtalade.[21]

När det gäller andra typer av elektroniska underskrifter finns det ingen tydlig praxis. Vad gäller namnteckning med elektronisk anordning har Svea hovrätt däremot i ett avgörande tagit fasta på att käranden i det aktuella målet inte presenterat någon bevisning som mera direkt tar sikte på de omstridda namnteckningarnas äkthet, t.ex. andra handlingar som ostridigt har undertecknats av motparten i kombination med sakkunnigutlåtanden.[22] Detta följer av naturliga skäl den placering av bevisbördan som gäller för vanliga namnteckningar på papper.[23]

4.3 Stämplar

4.3.1 Användning av stämplar inom den offentliga förvaltningen

Stämplar används relativt ofta inom den offentliga förvaltningen. Ett vanligt förekommande användningsområde är för att märka inkomna pappershandlingar med datum då handlingen kom in och diarienummer eller annan beteckning handlingen fått vid registreringen. De kan också användas som varning för att exempelvis markera att en handling omfattas av sekretess. Dessa typer av stämplar kan även tillfogas elektroniskt på inskannade eller elektroniskt inkomna eller upprättade handlingar. Vi kan inte se någon anledning för att generellt inom den offentliga förvaltningen använda avancerade eller kvalificerade elektroniska stämplar för denna typ av stämplar som är ämnade att till-

[20] Se t.ex. Kammarrätten i Göteborgs dom den 21 mars 2019 i mål nr 4765-18.
[21] Se t.ex. Stockholms tingsrätts dom den 26 juni 2019 i mål nr B 5092-19 och Uppsala tingsrätts dom den 21 januari 2020 i mål nr B 6683-17 m.fl.
[22] Svea hovrätts dom den 11 november 2020 i mål nr FT 7229-19.
[23] Se bl.a. NJA 1976 s. 667 och RH 2014:27.

föra information till en handling. De typer av stämplar där det får anses befogat är i stället de vars syfte bl.a. är att identifiera en handlings ursprung och äkthet.

Ordet stämpel förekommer i ett 20-tal svenska författningar, av relevans för denna utredning är dock endast att det av bilaga 1 till förmynderskapsförordningen (1995:379) framgår att registerutdrag om ställföreträdarskap ska ha plats för stämpel. I övrigt har vi inte identifierat att det förekommer andra bestämmelser på lag- eller förordningsnivå som inom offentlig förvaltning ställer krav på användning av en stämpel. Bestämmelsen är ett exempel på det som enligt vår bedömning är den vanligaste anledningen till att myndigheter stämplar handlingar där stämpeln har bevisverkan, dvs. att för tredje part bevisa en handlings ursprung och äkthet. Det kan exempelvis röra sig om att Migrationsverket behöver stämpla en kopia av en utländsk ID-handling för att en asylsökande med en sådan bestyrkt kopia ska kunna öppna ett svenskt bankkonto.[24] Ofta behöver en handling även stämplas för att den ska användas utomlands, exempelvis för att lämnas in till en utländsk myndighet. I sådana fall förekommer det även att stämpeln kombineras med att den som stämplar handlingen även skriver under den.[25]

I vissa fall kan stämplar av en mer avancerad art krävas. Det finns två sådana separata stämpelförfaranden, legalisering och apostille.

Med legalisering avses det formella förfarandet för att intyga riktigheten av en namnunderskrift från en person som innehar ett offentligt ämbete, den egenskap vari den som undertecknat handlingen har uppträtt samt, i förekommande fall, äktheten hos det sigill eller den stämpel som åsatts handlingen.[26] Legaliseringar utförs i Sverige av Utrikesdepartementet (UD). Efter det att UD har legaliserat handlingen ska den vanligen också bestyrkas av den utländska ambassad i Stockholm som företräder det land där handlingen ska användas.

[24] www.regeringen.se/artiklar/2016/06/asylsokande-ska-fa-tillgang-till-bankkonto/ (hämtad 2021-01-11)
[25] Se t.ex. https://bolagsverket.se/be/sok/bevisengelska/bevis-och-intyg-pa-engelska-1.4486 (hämtad 2021-01-11) och https://skatteverket.se/privat/folkbokforing/bestallpersonbevis/vanligaonskemalfranutlandskamyndigheter.4.3810a01c150939e893f22054.html (hämtad 2021-01-11).
[26] Artikel 3.3 i Europaparlamentets och rådets förordning (EU) 2016/1191 av den 6 juli 2016 om främjande av medborgares fria rörlighet genom förenkling av kraven på framläggande av vissa officiella handlingar i Europeiska unionen och om ändring av förordning (EU) nr 1024/2012.

Apostille regleras i Konventionen om slopande av kravet på legalisering av utländska allmänna handlingar (SÖ 1999:1). En apostille fyller samma funktion som en legalisering och kan utfärdas på handlingar som ska uppvisas i ett annat land som tillträtt konventionen. I Sverige är det endast notarius publicus som har rätten att utfärda apostille. Notarius publicus är en jurist, ofta advokat, som förordnas av länsstyrelsen och har som uppgift att bl.a. bestyrka namnunderskrifter, avskrifter och andra uppgifter om innehållet i handlingar.[27]

Värt att notera i sammanhanget är att enligt Europaparlamentets och rådets förordning (EU) 2016/1191 om främjande av medborgares fria rörlighet genom förenkling av kraven på framläggande av vissa officiella handlingar i Europeiska unionen är de officiella handlingar som omfattas av förordningen och bestyrkta kopior av dessa undantagna från legalisering och apostille.

Inom den offentliga förvaltningen förekommer således att myndigheter stämplar sina egna handlingar eller att detta, genom åtgärd från enskild, utförs av UD eller notarius publicus. Även om elektroniska stämplar hade kunnat användas i dessa sammanhang bygger en sådan hantering på att den som ska ta emot den elektroniskt stämplade handlingen även kan validera stämpeln. Ett införande av elektroniska stämplar för detta ändamål kan således inte göras ensidigt av svenska myndigheter om inte den förlitande parten i form av exempelvis en utländsk myndighet accepterar elektroniska stämplar och kan validera den aktuella stämpeln. Det kan dock noteras att krav på utställarverifikation genom en betrodd tjänst vid utlämnande av elektroniska kopior och utdrag från aktiebolagsregistret införts i ett EU-direktiv som ska vara genomfört senast den 1 augusti 2021.[28] Det är således möjligt att sådana krav kan komma att införas på EU-nivå även för andra utdrag från offentliga register.

Elektroniska stämplar omnämns endast i två svenska författningar (se mer om detta i avsnitt 8.7) och vår kartläggning visar att elektroniska stämplar som används för att identifiera en handlings ursprung och äkthet endast används i begränsad omfattning i den offentliga för-

[27] 6 a § förordningen (1982:327) om notarius publicus.

[28] Genom Europaparlamentets och rådets direktiv (EU) 2019/1151 av den 20 juni 2019 om ändring av direktiv (EU) 2017/1132 vad gäller användningen av digitala verktyg och förfaranden inom bolagsrätt har det införts ett nytt krav i artikel 16a.4. Av artikeln följer att elektroniska kopior och utdrag ur handlingar och information från aktiebolagsregistret ska ha autentiserats genom betrodda tjänster enligt eIDAS-förordningen i syfte att garantera att de elektroniska utdragen kommer från registret och att deras innehåll är en bestyrkt kopia av den handling som finns i registret eller att det överensstämmer med den information som förvaras i registret.

valtningen. Elektroniska stämplar används i dagsläget framför allt som en del av maskinella processer. Exempelvis i samband med elektroniskt informationsutbyte, maskin till maskin, där certifikat för autentisering av webbplatser används för att skydda transporten och stämplar för att skydda innehållet som skickas. Stämpeln används för att säkerställa att innehållet inte har förvanskats. Stämplar används även i e-legitimationssystemet där identitetsintygen stämplas av utfärdaren för att säkerställa att det kommer från rätt källa och är oförvanskat. De flesta av dessa stämplar baserar sig på av organisationen självutfärdade certifikat och används i en begränsad krets. En del stämpelcertifikat utfärdas dock av allmänt tillgängliga certifikatutfärdare. Användning av elektroniska stämplar förekommer även i samband med bevarande av elektroniska underskrifter (se mer om detta i avsnitt 8.5.3).

I skäl 65 i eIDAS-förordningens ingress exemplifieras vidare att elektroniska stämplar kan, utöver att användas för att autentisera ett dokument som utfärdats av en juridisk person, även användas för att autentisera en juridisk persons digitala tillgångar, t.ex. programvarukoder eller servrar.

4.3.2 Vilka juridiska funktioner fyller en stämpel?

I avsnitt 4.2.2 redogörs för de fem juridiska funktioner som en underskrift i allmänhet anses fylla. Någon tidigare sammanställning rörande en stämpels eller ett sigills juridiska funktioner har vi inte hittat. Vi anser dock att en stämpel fyller samma funktioner som en underskrift gör.

För det första kan en stämpel på samma sätt som en underskrift anses ge uttryck för en vilja att exempelvis bekräfta något, åta sig en förpliktelse eller lämna en försäkran om att uppgifterna i en handling är med sanningen överensstämmande. En mottagare kan också, utifrån den stämplade handlingen, anta att denne kan agera på ett visst sätt.

Även varningsfunktionen har viss relevans vid användning av en stämpel då handlingen medför att den som stämplar kan få anledning att överväga om innehållet i den handling som stämplas är korrekt.

En stämpel kan därtill användas för att identifiera den juridiska person som står bakom en stämplad handling. Således blir stämpeln även en utställarverifikation.

En fjärde funktion är äkthet då en stämpel knyter den juridiska person som står bakom stämpeln till handlingens innehåll. Detta innebär också ett visst skydd mot manipulation.

Eftersom en enskild som begär att en handling förses med stämpel ofta använder den stämplade handlingen för att styrka något är till sist stämpelns bevisverkan avseende kopplingen mellan den juridiska personen och den stämplade handlingens innehåll, dvs. identifikations- och äkthetsfunktionerna central. Det kan här noteras att det i artikel 35.2 i eIDAS-förordningen framgår att en kvalificerad elektronisk stämpel ska omfattas av en presumtion om integritet hos de uppgifter som den kvalificerade elektroniska stämpeln är kopplad till och om att de har korrekt ursprung.

4.4 Validering

4.4.1 Användning av validering inom den offentliga förvaltningen

Som framgår av avsnitt 3.3 innebär validering inom området betrodda tjänster kontroll och bekräftelse av elektroniska underskrifters och stämplars giltighet. Denna äkthetskontroll innebär dock inte att det går att fastställa att exempelvis den person som anges som undertecknare även undertecknat en handling (se mer om detta i avsnitt 4.2.2). Trots att det inte är möjligt att genom valideringen med säkerhet bekräfta att rätt person undertecknat en handling är det ett mycket säkrare sätt att koppla en underskrift till en viss individ än vad en pappersbaserad process medger. För att granska en namnteckning på en pappershandling krävs en äkta namnteckning att jämföra med. En sådan hantering är, om det ska göras på ett korrekt sätt, mycket resurskrävande.[29] Det har inte heller av utredningens kartläggning framkommit att allmänna äkthetskontroller av namnteckningar är vanligt förekommande inom den offentliga förvaltningen. Förekomsten av validering i den offentliga förvaltningen drivs således framför allt av den ökade användningen av elektroniska underskrifter och stämplar. Många myndigheter har e-tjänster där underskrifter skapas inom ramen för den egna tjänsten. Valideringen är då en integrerad del av processen.

[29] *Fakturabedrägerier* (SOU 2015:77), s. 281 f.

Mottagande av elektroniskt undertecknade eller stämplade handlingar förutsätter emellertid inte att validering sker. Likt vad som i dagsläget gäller för namnteckningar kan mottagaren välja att utgå från att underskriften är äkta och att undertecknandet utförts av rätt person. När det gäller utbyte av handlingar mellan myndigheter brukar detta benämnas som organisationstillit. Det var E-delegationen som etablerade denna princip i syfte att effektivisera arbetet med informationsutbyte mellan offentliga aktörer. Principen bygger på att det vid informationsutbyte inom ramen för myndigheternas samverkans- och serviceskyldighet räcker att kontrollera att den andra parten är den myndighet som den uppger sig vara, eftersom en myndighet vanligtvis kan lita på att en handläggare som agerar för en annan myndighets räkning är behörig att företräda myndigheten.[30] Mottagande myndighet litar således på att rätt person skrivit under en aktuell handling utan att kontrollera att detta stämmer.[31]

4.5 Elektroniska tjänster för rekommenderade leveranser samt den offentliga förvaltningens informationsutbyten

4.5.1 Vad är elektroniska tjänster för rekommenderade leveranser?

Av skäl 66 i ingressen till eIDAS-förordningen framgår att det är av avgörande betydelse att det föreskrivs en rättslig ram för att främja gränsöverskridande erkännande mellan befintliga nationella rättssystem för elektroniska tjänster för rekommenderade leveranser. Den ramen skulle också kunna öppna nya marknadsmöjligheter för unionens tillhandahållare av betrodda tjänster att erbjuda nya paneuropeiska tjänster för elektroniska tjänster för rekommenderade leveranser. Det är mot denna bakgrund som den betrodda tjänsten elektronisk tjänst

[30] eSam, *En effektiv informationsförsörjning*, juni 2017, s. 63.

[31] Utredningen om effektiv styrning av nationella digitala tjänster (SOU 2017:114, s. 264) lyfte fram den tidigare lydelsen av 45 kap. 4 § rättegångsbalken som ett exempel på hur lagstiftningen kan sägas ha följt principen om organisationstillit. Av bestämmelsen följer att en stämningsansökan som huvudregel ska vara egenhändigt undertecknad. En stämningsansökan som ges in elektroniskt ska emellertid vara undertecknad med en sådan elektronisk underskrift som avses i artikel 3 i eIDAS-förordningen eller överföras på ett sätt som uppfyller motsvarande grad av säkerhet. Det sista ledet i bestämmelsen utgjorde enligt utredningen en författningsreglerad organisationstillit. Det bör noteras att bestämmelsen ändrades den 1 januari 2021 på så sätt att kravet på undertecknande eller överförande på ett sätt som uppfyller motsvarande grad av säkerhet togs bort helt.

för rekommenderad leverans ska förstås. Tjänsten definieras i artikel 3.36 i eIDAS-förordningen som en tjänst som gör det möjligt att överföra uppgifter mellan tredje män på elektronisk väg och tillhandahåller bevis avseende de överförda uppgifternas hantering, inklusive bevis för uppgifternas sändning och mottagande, och som skyddar överförda uppgifter mot risken för förlust, stöld, skada eller otillåtna ändringar.

4.5.2 Den offentliga förvaltningens informationsutbyten

Elektroniska tjänster för rekommenderade leveranser möjliggör informationsutbyten. Elektronisk kommunikation och informationsutbyte mellan samt till och från aktörer inom offentlig förvaltning är omfattande, exempelvis via digital post. Fler än fyra miljoner privatpersoner och företag i Sverige har en digital brevlåda genom brevlådeoperatörerna Digimail, eBoks, Kivra och Min myndighetspost. Genom dessa tjänster, som nyttjar den gemensamma infrastrukturen benämnd Mina meddelanden, kan dessa personer och företag ta emot, läsa och bevara digital myndighetspost.[32]

Mellan vissa anslutna statliga myndigheter sker bl.a. e-postutbyten via kommunikationstjänsten SGSI (Swedish Government Secure Intranet) som tillhandahålls av Myndigheten för samhällsskydd och beredskap (MSB). All datatrafik mellan SGSI-anslutna myndigheter är krypterad.[33]

Det finns även exempel på strukturerade informationsutbyten inom den offentliga förvaltningen. Ett av dem är Rättsväsendets informationsförsörjning (RIF). RIF är ett samarbete mellan rättsväsendets myndigheter, med målet att digitalisera och utveckla informationsutbytet mellan myndigheterna i rättskedjan. Inom RIF utbyts information strukturerat system till system. En viktig komponent i utbytet är att principen om organisationstillit tillämpas (se mer om denna princip i avsnitt 4.4.1). Det i sin tur medför att mottagande aktör inte behöver kontrollera om den avsändande handläggaren är behörig eller inte.[34] RIF bygger på kommunikations- och överföringsprotokollet SHS (Spridnings- och HämtningsSystem) som förvaltas av Försäkringskassan. Detta protokoll utgör även grunden för bl.a. SSBTEK

[32] www.digg.se/digital-post (hämtad 2021-01-13).
[33] www.msb.se/sv/verktyg--tjanster/sgsi/ (hämtad 2021-01-13).
[34] *reboot – omstart för den digitala förvaltningen* (SOU 2017:114), s. 264.

(Sammansatt bastjänst för ekonomiskt bistånd) och LEFI Online som ger tillgång till person- och förmånsinformation från Pensionsmyndigheten och Försäkringskassan.

Andra lösningar för informationsutbyten inom förvaltningen är t.ex. den nationella tjänsteplattformen vars syfte är att förenkla, säkra och effektivisera informationsutbytet mellan olika it-system inom vård- och omsorgssektorn. Den nationella tjänsteplattformen tillhandahålls av Inera. Inera driver även projektet Säker digital kommunikation (SDK) vars mål är att skapa en standardiserad förmåga till säker digital kommunikation mellan kommuner, regioner och statliga myndigheter. En sådan lösning ska även omfatta privata utförare av offentligt uppdrag. Kanaler som exempelvis fax och brev ska ersättas med digital och säker meddelandeöverföring. Projektet har drivits sedan 2017 och breddinförandet beräknades tidigare ske 2021. Detta är nu senarelagt. Den tekniska lösningen bygger på eDelivery (se mer om eDelivery i avsnitt 5.12.2) och vissa centrala tjänster kommer att tillhandahållas av DIGG.[35]

År 2018 gav regeringen Bolagsverket, Domstolsverket, E-hälsomyndigheten, Försäkringskassan, Lantmäteriet, Skatteverket och DIGG i uppdrag att tillsammans analysera och lämna förslag som syftar till att skapa ökad säkerhet och effektivitet i samband med elektroniska informationsutbyten inom och med den offentliga sektorn.[36] Uppdraget resulterade i rapporten *Säkert och effektivt elektroniskt informationsutbyte inom den offentliga sektorn*. I rapporten föreslogs fyra kategorier av förvaltningsgemensamma byggblock i ett ekosystem med förvaltningsgemensam digital infrastruktur för informationsutbyte: digitala tjänster, informationsutbyte, informationshantering samt tillit och säkerhet.[37] Regeringen lämnade i december 2019 ett nytt uppdrag till tidigare nämnda myndigheter samt MSB och Riksarkivet att tillsammans etablera en förvaltningsgemensam digital infrastruktur för informationsutbyte. Den 17 december 2020 beslutade regeringen om förlängd tid för uppdraget. Uppdraget ska

[35] www.inera.se/utveckling/pagaende-projekt-och-utredningar/saker-digital-kommunikation/ (hämtad 2021-01-13).
[36] Uppdrag om ett säkert och effektivt elektroniskt informationsutbyte inom den offentliga sektorn (Fi2018/02150/DF, FI2018/03037/DF och I2019/01061/DF).
[37] DIGG m.fl., *Säkert och effektivt elektroniskt informationsutbyte inom den offentliga sektorn* (DIGG dnr 2019-100), s. 17 ff.

slutrapporteras i december 2021.[38] En delredovisning skedde dock i slutet av januari 2021. I delredovisningen lämnades förslag på en lämplig struktur för arbetet med den förvaltningsgemensamma infrastrukturen för informationsutbyte, förslag på författning som reglerar myndigheternas uppgifter och ansvar, en långsiktig plan för arbetet samt redovisning av arbetet med enskilda.[39]

4.5.3 Finns det svenska tillhandahållare av elektroniska tjänster för rekommenderade leveranser?

Utredningen om effektiv styrning av nationella digitala tjänster framförde att leverantörerna av digitala brevlådetjänster som använder sig av infrastrukturen Mina meddelanden kan ses som att de tillhandahåller elektroniska tjänster för rekommenderade leveranser.[40] Post- och telestyrelsen (PTS) genomförde därefter en utredning av om den statliga brevlådeoperatören Min Myndighetspost tillhandhöll en betrodd tjänst. PTS slutsats var att Min Myndighetspost var en betrodd tjänst på så sätt att den utför validering av avancerade elektroniska stämplar. Utifrån att Min Myndighetspost som brevlådeoperatör enbart tar emot försändelser och validerar dessa omfattades den dock inte enligt PTS bedömning av eIDAS-förordningens definition av en elektronisk tjänst för rekommenderad leverans.[41]

I dagsläget finns det inte i Sverige några tillhandahållare av kvalificerade elektroniska tjänster för rekommenderade leveranser. Det är möjligt att något eller några av de system för informationsutbyten som används av den offentliga förvaltningen skulle kunna anses utgöra icke kvalificerade elektroniska tjänster för rekommenderade leveranser. För att göra en sådan bedömning krävs emellertid en genomgång av respektive systems tekniska uppbyggnad. Att göra sådana bedömningar får anses ligga utanför utredningens uppdrag.

[38] Uppdrag att etablera en förvaltningsgemensam digital infrastruktur för informationsutbyte (I2019/03306/DF, I2019/01036/DF [delvis], I2019/01361/DF [delvis] och I2019/02220/DF)
[39] DIGG m.fl. *Delredovisning – Uppdrag att etablera en förvaltningsgemensam digital infrastruktur för informationsutbyte* (AD 2019:582), 29 januari 2021.
[40] *reboot – omstart för den digitala förvaltningen* (SOU 2017:114), s. 381.
[41] Post- och telestyrelsen, *Brevlådeoperatörer och betrodda tjänster*, Presentation, 20 november 2019.

4.6 Certifikat för autentisering av webbplatser

4.6.1 Vad är certifikat för autentisering av webbplatser?

Certifikat för autentisering av webbplatser definieras i artikel 3.38 i eIDAS-förordningen som ett intyg som gör det möjligt att autentisera en webbplats och koppla webbplatsen till den fysiska eller juridiska person som certifikatet utfärdats för. Enligt skäl 67 i förordningens ingress innebär tjänster för autentisering av webbplatser en möjlighet för en besökare på en webbplats att försäkra sig om att en verklig och legitim enhet står bakom webbplatsen. Certifikatet utfärdas vanligen till ett eller flera domännamn.[42] Ett annat sätt att beskriva det är att certifikat för autentisering av webbplatser används för att skydda trafiken till och från en webbplats, t.ex. en e-tjänst eller en mobilapplikation. Dessa certifikat kan även användas för att skydda trafiken från maskin till maskin inom och mellan organisationer. Av skäl 67 i eIDAS-förordningens ingress framgår vidare att användning av denna betrodda tjänst är frivillig och att även andra sätt eller metoder för att autentisera en webbplats, än de som omfattas av förordningen, får användas.

Utvecklingen inom området drivs i stor utsträckning av CA/Browser Forum. CA/Browser Forum är ett frivilligt konsortium av certifikatutfärdare (certification authorities [CA]) samt utvecklare av webbläsare, operativsystem och andra applikationer. Konsortiet tar fram riktlinjer gällande utfärdandet och hanteringen av certifikat som finns med som standard i dessa applikationer.[43] Certifikaten används för att stämpla programkod och för användning i TLS-protokollet för att skydda trafiken till en webbplats eller mellan två maskiner.[44]

Forumet tog 2011 fram riktlinjer som är bindande för dess medlemmar och som innebär att certifikat klassificeras som domänvaliderade, organisationsvaliderade, individuellt validerade eller utökat validerade.[45] Med validerade avses i detta fall hur omfattande kontrollen av identiteten på den som köpt certifikatet är. Att följa dessa riktlinjer är en förutsättning för att finnas med i webbläsares och opera-

[42] Exempelvis är www.regeringen.se ett domännamn.
[43] https://cabforum.org/wp-content/uploads/CA-Browser-Forum-Bylaws-v2.3.pdf%20 (hämtad 2021-01-28).
[44] Transport Layer Security (TLS) är ett kryptografiskt kommunikationsprotokoll som är en öppen standard för säkert utbyte av krypterad information mellan datorsystem.
[45] https://cabforum.org/wp-content/uploads/CA-Browser-Forum-BR-1.7.3.pdf (hämtad 2021-01-28).

tivsystems listor över betrodda utfärdare, dvs. sådana som inte ger en varning till den som besöker en webbplats att certifikatet är okänt.

4.7 Användning av certifikat för autentisering av webbplatser inom den offentliga förvaltningen

Certifikat för autentisering av webbplatser används i stor utsträckning för att skydda webbplatser samt trafik mellan maskiner och mellan organisationer. Användningen av sådana kvalificerade certifikat som regleras i eIDAS-förordningen förefaller dock vara mycket begränsad. EU-kommissionen arbetar emellertid för att stimulera och öka användningen i syfte att skapa en europeisk marknad för sådana certifikat. Det har skett bl.a. genom att Europeiska unionens cybersäkerhetsbyrå (ENISA) studerat hur användningen kan ökas.[46] ENISA har även undersökt hur det i en webbläsare kan framgå att webbplatsen använder ett kvalificerat certifikat för autentisering av webbplatser.[47]

Det finns även krav på användningen av kvalificerade certifikat för elektroniska stämplar eller autentisering av webbplatser via normativa specifikationer som används i vissa sammanhang. Det finns t.ex. en delegerad förordning[48] till andra betaltjänstedirektivet[49] som ställer krav på att betaltjänsteleverantörer ska använda sig av kvalificerade certifikat för stämplar eller kvalificerade certifikat för autentisering av webbplatser. Användningen ska ske i samband med att leverantörer av kontoinformationstjänster, leverantörer av betalningsinitieringstjänster och betaltjänstleverantörer som ger ut kortbaserade betalningsinstrument identifierar sig för den kontoförvaltande betaltjänstleverantören.

Vad avser användning i Sverige används kvalificerade certifikat för autentisering av webbplatser för trafiken mellan noderna i systemet för informationsutbyte mellan socialförsökringsmyndigheterna, dvs.

[46] ENISA, *Qualified Website Authentication Certificates – Promoting consumer trust in the website authentication market*, december 2015.
[47] ENISA, *QWACs Plugin Proof of concept browser plugin to support the two-step verification of qualified certificates for web-site authentication*, januari 2018.
[48] Kommissionens delegerade förordning (EU) 2018/389 av den 27 november 2017 om komplettering av Europaparlamentets och rådets direktiv (EU) 2015/2366 vad gäller tekniska tillsynsstandarder för sträng kundautentisering och gemensamma och säkra öppna kommunikationsstandarder.
[49] Europaparlamentets och rådets direktiv (EU) 2015/2366 (PSD 2) om betaltjänster på den inre marknaden, om ändring av direktiven 2002/65/EG, 2009/110/EG och 2013/36/EU samt förordning (EU) nr 1093/2010 och om upphävande av direktiv 2007/64/EG (PSD).

Försäkringskassan och dess systermyndigheter i andra EU-länder, EESSI (Electronic Exchange of Social Security Information). Eftersom det inte finns någon svensk utfärdare av kvalificerade certifikat för autentisering av webbplatser har dessa enligt uppgift från Försäkringskassan anskaffats från kvalificerad tillhandahållare i annat land.

4.8 Elektronisk tidsstämplingstjänst

4.8.1 Vad är en elektronisk tidsstämplingstjänst?

Elektronisk tidsstämpling definieras i artikel 3.33 i eIDAS-förordningen som uppgifter i elektronisk form som binder andra uppgifter i elektronisk form till en viss tidpunkt och därmed utgör bevis för att de senare uppgifterna existerade vid den tidpunkten. Sådana tjänster kan användas som enskilda betrodda tjänster eller i kombination med andra betrodda tjänster. Av artikel 44.1 f i eIDAS-förordningen framgår exempelvis, avseende kvalificerade elektroniska tjänster för rekommenderade leveranser, att datumet och tidpunkten för avsändande, mottagande och eventuella ändringar av uppgifter måste anges genom en kvalificerad elektronisk tidsstämpling.

Alla avancerade eller kvalificerade elektroniska underskrifter och stämplar innehåller en tidsuppgift om när de skapats. Den tidsuppgiften hämtas normalt från det system där underskriften skapas, dvs. i en användares dator eller tiden i en e-tjänst. Det går även att använda en betrodd tjänst från tredje part som anger tidsuppgiften när underskriften eller stämpeln skapas och då skyddas tidsuppgiften av den betrodda tjänstens egen underskrift eller stämpel.

4.8.2 Användning av tidsstämplingstjänster inom den offentliga förvaltningen

Det förekommer formkrav i vissa medlemsstater i EU om att kvalificerade tidsstämplingstjänster ska användas. I Sverige framstår behovet av tidsstämpling som enskild tjänst utifrån vår kartläggning dock inte som särskilt stort. Detta beror troligtvis på den utbredda förekomsten av e-tjänster där underskrifter skapas i samband med användningen av e-tjänsten. Vid skapandet av underskriften används då tidsuppgifter från den som tillhandahåller e-tjänsten.

5 Betrodda tjänster – teknik, juridik och standarder

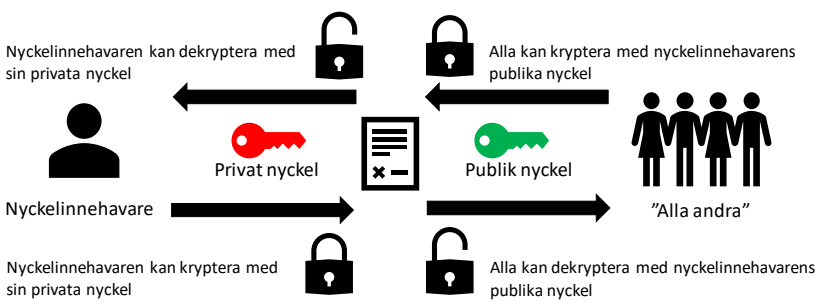
5.1 Inledning

Syftet med detta kapitel är att översiktligt beskriva den teknik som ligger till grund för betrodda tjänster, de bestämmelser som finns inom området samt framtagandet av standarder och tekniska specifikationer.

5.2 Betrodda tjänster – hur fungerar tekniken?

En förenklad beskrivning av tekniken bakom betrodda tjänster är att den vanligen bygger på kryptering med privata och publika nycklar, s.k. asymmetrisk kryptering. Nycklarna hänger samman i ett par som matematiskt är kopplade till varandra på sådant sätt att allt som krypteras med den privata nyckeln kan dekrypteras med den publika nyckeln, medan det som krypteras med den publika nyckeln enbart kan dekrypteras med den privata nyckeln (se figur 5.1). Den publika nyckeln kan publiceras eller delas öppet medan den privata nyckeln måste skyddas väl av innehavaren.

Figur 5.1 Asymmetrisk kryptering med PKI



När tekniken används i en infrastruktur kallas den Public Key Infrastructure (PKI). PKI är ett samlingsnamn för den infrastruktur, byggd på komponenter, gränssnitt, ansvar och förtroende, som med hjälp av privata och publika nycklar används för bl.a. identifiering, underskrifter och skydd mot obehörig insyn. För PKI spelar certifikat en viktig roll och inom ramen för eIDAS-förordningen är det tillhandahållarna av betrodda tjänster som utfärdar certifikaten. Dessa certifikatutfärdare knyter med hjälp av certifikatet en fysisk eller juridisk person till ett unikt nyckelpar. Detta sker genom att certifikatutfärdaren intygar att en fysisk eller juridisk person är innehavare av ett nyckelpar och kopplingen säkras genom att utfärdaren stämplar certifikatet med sin privata nyckel. I certifikatet finns information om nyckelinnehavaren på ungefär samma sätt som den information som framgår av ett id-kort. Detta nyckelpar gör det möjligt att identifiera användaren elektroniskt och för användaren att skapa elektroniska underskrifter eller stämplar.

En utfärdare identifierar en innehavare när certifikatet ges ut. Därefter tillhandahåller utfärdaren funktioner för spärrkontroll, t.ex. spärrlistor eller en kontrollfunktion online så att den förlitande parten kan kontrollera att individen inte har spärrat sitt certifikat med tillhörande nyckelpar. Olika typer av användning av dessa nyckelpar är således grunden för PKI-baserade betrodda tjänster, som i dagsläget är de absolut vanligast förekommande. Det finns dock även betrodda tjänster som använder blockkedjeteknik för elektroniska underskrifter och elektroniska tidsstämplingar i stället för PKI (se mer om detta i avsnitt 5.2.3).

5.2.1 Autentisering

Autentisering definieras i artikel 3.5 i eIDAS-förordningen som en elektronisk process som gör det möjligt att bekräfta den elektroniska identifieringen för en fysisk eller juridisk person, eller ursprunget för och integriteten hos uppgifter i elektronisk form. När PKI används för identifiering innebär det att den som vill identifiera någon krypterar med den publika nyckeln och individen, organisationen eller tjänsten dekrypterar med den privata nyckeln. Certifikatet som beskrivits tidigare kopplar ihop nyckelparet med en juridisk eller fysisk person. Förmågan att dekryptera med den privata nyckeln visar att

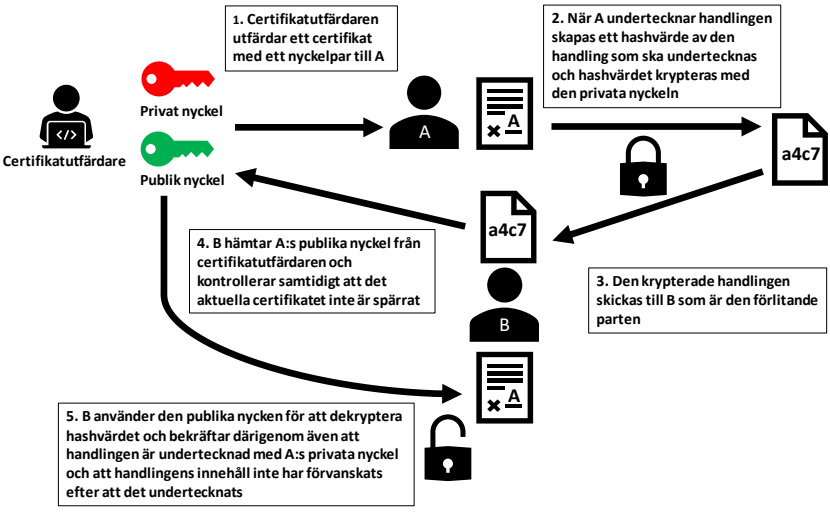
den identifierade är den som intygas vara innehavare av en publik nyckel i certifikatet. Denna teknik används bl.a. i betrodda tjänster för autentisering av webbplatser där en användare ska kunna autentisera t.ex. en e-tjänst och att myndigheten står bakom tjänsten. I fallet ovan skickar e-tjänsten ett krypterat slumptal till användaren som krypterats med e-tjänstens privata nyckel som användaren kan dekryptera med e-tjänstens publika nyckel som återfinns i certifikatet för autentisering av webbplatsen. Detta sker automatiserat i användarens webbläsare eller applikation.

5.2.2 Elektroniska underskrifter och stämplar

När en elektronisk underskrift ska framställas innebär det att den privata nyckeln används för att kryptera och att den publika nyckeln används för att dekryptera (se figur 5.2). Det som krypteras och dekrypteras i en elektroniskt underskrift eller stämpel är ett s.k. hashvärde av den undertecknade informationen. Detta för att alla ska ha möjlighet att validera en underskrift. Algoritmen som används för att skapa hashvärdet måste vara så pass avancerad att inte två olika informationsmängder ger samma hashvärde. Hashvärdet krypteras med den privata nyckeln och framställer på sådant sätt ett dataobjekt, dvs. underskriften som är unikt knuten till både den datamängd som representerar den undertecknade handlingen och användaren. Användningen av den asymmetriska krypteringsmetoden och PKI innebär att alla som litar på certifikatutfärdaren kan dekryptera med den publika nyckeln. Vilken krypteringsalgoritm och hashalgoritm som används framgår av certifikatet och med denna information kan den som vill validera underskriften göra det. Detta är grunden för avancerade och kvalificerade elektroniska underskrifter och andra kryptografiskt säkrade underskrifter. Underskrifterna kan ha olika format och egenskaper kopplade till t.ex. dokumentformat som PDF och XML.[1]

[1] Förkortningen XML står för Extensible Markup Language. XML är en teknisk standard för strukturmärkning av textbaserade elektroniska dokument.

Figur 5.2 Elektroniskt undertecknande av handling med PKI



Tekniken för en elektronisk stämpel är densamma som för en underskrift. Den enda skillnaden är att i underskriften identifieras en fysisk person som innehavare av en publik nyckel medan det för en elektronisk stämpel är en juridisk person som identifieras som innehavare av den publika nyckeln.

Samma teknik används av tidsstämplingstjänster. Tjänsten får ett hashvärde av en informationsmängd skickat till sig, varefter den sätter dit ett klockslag och säkrar klockslaget med sin egen elektroniska underskrift eller stämpel.

Fristående underskriftstjänst

DIGG rekommenderar myndigheter som har behov av att användare skriver under elektroniskt att införa en s.k. fristående underskriftstjänst.[2] En fristående underskriftstjänst möjliggör att användaren kan identifiera sig med valfri e-legitimation inom ramen för de avtal om elektronisk identifiering som myndigheten har.

[2] Avsnittet bygger i stor utsträckning på uppgifter från www.digg.se/digital-identitet/e-underskrift/offentlig-aktor (hämtad 2021-01-19) och Kammarkollegiet, *Vägledning för avrop av tjänster för elektronisk identifiering och elektronisk underskrift från ramavtalsområden inom Programvaror och Tjänster 2019 (Version 2.0)*, 8 april 2020.

När en underskrift krävs för att fullfölja ett ärende väljer myndigheten att begära användarens underskrift av en handling. Handlingen visas för användaren som bekräftar att underskrift ska göras genom att välja ”jag vill skriva under ...”, eller motsvarande.

Den handling som ska skrivas under paketeras och det skapas även ett hashvärde av den elektroniska handlingen. En begäran om underskrift skapas och sänds till underskriftstjänsten. Även ett meddelande sänds, som användaren ser när denne identifierar sig för underskrift. Det är endast hashvärdet av den elektroniska handlingen som sänds till underskriftstjänsten, inte handlingen som sådan.

Underskriftstjänsten tar emot en begäran om underskrift och sänder användaren vidare till identitets- och intygsfunktionen. Användaren ser meddelandet och identifierar sig för underskrift genom att ange sin säkerhetskod eller motsvarande. Identitets- och intygsfunktionen kontrollerar identifieringen och ställer ut ett identitetsintyg som sänds tillbaka till underskriftstjänsten. Underskriftstjänsten tar emot och kontrollerar identitetsintyget samt skapar användarens elektroniska underskrift med tillhörande underskriftscertifikat. Underskriftstjänsten skapar ett underskriftssvar som sänds tillbaka till funktionen på myndigheten som tar emot underskriftssvaret.

Underskriftssvaret tas emot och kontrolleras och myndighetens funktion fogar därefter samman underskriften med originalhandlingen till en undertecknad elektronisk handling. En kvittens visas för användaren.

Den fristående underskriftstjänsten använder samma kryptografiska metoder som beskrivs i avsnittet ovan. Däremot har inte användaren vänt sig till en certifikatutfärdare och fått ett certifikat med tillhörande nycklar utfärdat i förväg. I stället ställs ett engångscertifikat ut genom den fristående underskriftstjänsten i samband med att en underskrift skapas.

5.2.3 Blockkedjeteknik

En blockkedja är en distribuerad lista över digitala objekt som är ordnade i en struktur som kan göra information beständig mot förändring.[3] Förenklat beskrivet fungerar en blockkedja så att det utifrån ett

[3] Innehållet i detta avsnitt bygger i stor utsträckning på Yaga, Dylan, m.fl., *Blockchain Technology Overview (*National Institute of Standards and Technology, NISTIR 8202), oktober 2018.

digitalt informationsinnehåll, t.ex. ett elektroniskt dokument, skapas ett hashvärde med hjälp av en kryptografisk algoritm. Det ursprungliga dokumentet kan bevaras i ett exemplar hos innehavaren samtidigt som hashvärdet som representerar dokumentets information sparas och förmedlas vidare tillsammans med andra hashvärden i en grupp. En sådan grupp hashvärden kan i sin tur betraktas som ett nytt elektroniskt dokument som det beräknas ett samlat hashvärde för. Varje sådan grupp innehåller dessutom hashvärdet från föregående grupp, vilket bildar en kedja av grupper eller block som bygger på varandra. Alltså en blockkedja vars struktur garanterar att de ingående hashvärdena inte kan ändras utan att påverka efterföljande block i kedjan.

Den elektroniska handlingen vars hashvärde ingår i en blockkedja behöver inte vara ett dokument, utan kan exempelvis vara publika nycklar med information rörande vem de är utfärdade till. På detta sätt får man en oföränderlig historik över utfärdade identiteter.

Blockkedjan är distribuerad så att en kopia av den finns hos alla de noder i ett nätverk som samtidigt försöker att skapa nya block i kedjan. För att skapa ett nytt block krävs någon form av begränsad resurs som gör det svårt eller dyrt att förfalska blockkedjan. Ofta är denna resurs beräkningskraft, men det kan också vara hur stor andel av det som blockkedjan skyddar som kontrolleras av den som skapar block.

Eftersom en blockkedja inte består av innehållet i ett dokument, utan endast dess hashvärde går det inte att återskapa innehållet i själva dokumentet från information i blockkedjan. Det är bara innehavaren av det ursprungliga dokumentet som kan läsa eller sprida innehållet i dokumentet. Blockkedjan kan dock med en mycket hög grad av tillförlitlighet visa att dokumentet existerade vid en viss tidpunkt eller knyta det till en viss elektronisk identitet. Befintliga lösningar med användning av blockkedjeteknik innefattar elektronisk underskrift där användaren identifierats med e-legitimation eller motsvarande för att verifiera kopplingen till den fysiska person som är utställaren av dokumentet. Tekniken används även för tidsstämplingstjänster och det finns i skrivande stund åtminstone en kvalificerad tillhandahållare av kvalificerad tidsstämplingstjänst i Europa som använder blockkedjeteknik.

5.2.4 Nya metoder för att identifiera användare

Identifiering av användare är en förutsättning för att kunna knyta användare till en elektronisk underskrift och således skapa avancerade eller kvalificerade elektroniska underskrifter. Det pågår en översyn av eIDAS-förordningen (se mer om detta i avsnitt 5.4.6) och det som hittills har offentliggjorts av EU-kommissionen i samband med presentationer vid möten har till stor del varit inriktat mot elektronisk identifiering och en europeisk elektronisk identitet som baserar sig på s.k. Self Sovereign Identity (SSI).[4]

SSI bygger på tanken att individen själv skapar och har kontroll över sina attribut som används för att identifiera individen och delar med sig av de attribut som behövs för att använda en viss tjänst.[5] De attribut som delas kan i en tjänst vara för att visa att personen är myndig, i en annan tjänst kan det vara att personen har rätt att köra bil och i en tredje tjänst en mer komplex logik som kräver flera olika attribut. En grundtanke med SSI är att personen själv har medlen för att skapa, kontrollera och lagra sina unika identifierare.

Tekniken som används är baserad på blockkedjeteknik och bygger på en sorts identifierare som kallas DID[6] (Decentralised Identifiers). DID är en URL (Uniform Resource Locator). En URL definierar var och hur en resurs, t.ex. ett dokument, kan hämtas.[7] En DID pekar på en individ och ett dokument som utformas på ett specifikt sätt, kallat DID-dokument. Dokumentet beskriver hur den decentraliserade identiteten ska användas och hur dokumentet stödjer autentiseringen av individen som är kopplad till dokumentet. DID är baserat på en decentraliserad infrastruktur som inte kräver något centralt system för registrering av användare. Det kan baseras på en decentraliserad PKI med decentraliserat nyckelhanteringssystem. Kopplat till detta finns datamoduleringar och syntax för utbyte av verifierbara identifierare.

Inom EU bedrivs för närvarande ett projekt, European Self-Sovereign Identity Framework (ESSIF), som använder SSI och blockkedjeteknik via European Blockchain Services Infrastructure (EBSI). I detta arbete förutses och förutsätts att det finns centrala betrodda

[4] ENISA trust services forum – CA-day 2020, 22-23 september 2020 och PTS forum för betrodda tjänster, 19 november 2020.
[5] https://ieeexplore.ieee.org/document/8776589 (hämtad 2021-01-22).
[6] www.w3.org/TR/did-core/ (hämtad 2021-01-22).
[7] Svenska datatermgruppen, www.termado.com/DatatermSearch/?ss=url (hämtad 2021-01-13).

tillhandahållare av attribut för en viss individ, sedan tidigare verifierade attribut om individen som t.ex. körkortsbehörighet, examensbevis och liknande.

5.3 Tidigare reglering av betrodda tjänster

Signaturdirektivet

Föregångaren till eIDAS-förordningen var signaturdirektivet. Direktivet upphävdes i och med att förordningen började tillämpas. Förordningen bygger i vissa delar på direktivets bestämmelser och i syfte att ge en så heltäckande förståelse för förordningen som möjligt presenteras nedan direktivets huvuddrag. En mer omfattande genomgång av direktivet finns bl.a. i förarbetena till det svenska genomförandet.[8]

Direktivet innehöll bestämmelser om elektroniska signaturer och vissa certifikattjänster. Termen betrodda tjänster infördes först i samband med eIDAS-förordningen. Syftet med direktivet var att underlätta användningen av elektroniska signaturer, bidra till deras rättsliga erkännande samt säkerställa en väl fungerande inre marknad. När kommissionen presenterade sitt förslag till direktiv konstaterades bl.a. att öppna nätverk, såsom internet, erbjuder nya affärsmöjligheter och möjliggör interaktion mellan det offentliga och företag eller privatpersoner.[9] För att kunna ta tillvara dessa möjligheter på bästa sätt krävs säkra miljöer för elektronisk autentisering. Elektroniska signaturer konstaterades möjliggöra det. Vidare anförde kommissionen att flera medlemsstater hade vidtagit egna lagstiftningsinitiativ som riskerade att leda till fragmentisering på området och att det därför förelåg ett behov av harmonisering på EU-nivå.[10]

Direktivet hade i jämförelse med eIDAS-förordningen ett relativt begränsat antal materiella bestämmelser om elektroniska signaturer och certifikattjänster.

En central bestämmelse i direktivet som fördes vidare till eIDAS-förordningen gällde elektroniska signaturers rättsliga verkan (se mer om de nuvarande bestämmelserna i avsnitt 5.9). Enligt artikel 5.1 var medlemsstaterna skyldiga att säkerställa tre saker avseende avancerade elektroniska signaturer som var baserade på ett kvalificerat cer-

[8] Se prop. 1999/2000:117 s. 25 ff.
[9] KOM(1998) 297 slutlig av den 13 maj 1998.
[10] A.a.

tifikat och som skapats av en säker anordning för skapande av signaturer. För det första att sådana signaturer uppfyllde de rättsliga kraven på en signatur i förhållande till uppgifter i elektronisk form, på samma sätt som en handskriven signatur uppfyller samma krav i förhållande till uppgifter på papper. För det andra att de godtogs som bevis vid rättsliga förfaranden. Slutligen skulle medlemsstaterna även säkerställa att en elektronisk signatur inte förvägrades rättslig verkan eller giltighet som bevis vid rättsliga förfaranden enbart på grund av att signaturen var i elektronisk form, inte var baserad på ett kvalificerat certifikat, inte var baserad på ett kvalificerat certifikat utfärdat av en ackrediterad tillhandahållare av certifikattjänster, eller inte var skapad av en säker anordning för skapande av signaturer.

I Sverige genomfördes direktivet genom lagen (2000:832) om kvalificerade elektroniska signaturer. Lagen följde i huvudsak direktivets bestämmelser men det kan noteras att termen ”kvalificerade elektroniska signaturer” infördes i lagen, en term som saknas i direktivet. I lagens förarbeten motiverades det med att direktivet ville ge de elektroniska signaturer som inte bara var avancerade utan också baserade på ett kvalificerat certifikat och skapade av en säker anordning för signaturframställning en särskild ställning.[11] Vid genomförandet konstaterades emellertid att det fanns anledning att vara försiktig med att reglera ett bredare område än vad direktivet krävde eftersom den marknad direktivet reglerade ännu inte vuxit fram i nämnvärd omfattning.[12] PTS utsågs till tillsynsmyndighet och fick även föreskriftsrätt avseende innehåll i kvalificerade certifikat samt krav på certifikatutfärdare.[13]

År 2012 konstaterade kommissionen att området behövde reformeras. Kommissionen anförde att signaturdirektivet inte hade lett till den harmonisering som avsågs, bl.a. mot bakgrund av att medlemsstaterna hade gjort olika tolkningar av direktivet vid genomförandet och att gamla standarder användes. Tillsynen i medlemsstaterna skiljde sig också åt vilket gjorde det svårt att bedöma tillsynen över en viss tillhandahållare. I gränsöverskridande situationer upplevdes interoperabilitetsproblem. För att komma tillrätta med de identifierade problemen föreslog kommissionen det som kom att bli eIDAS-för-

[11] Prop. 1999/2000:117 s. 41.
[12] A.a. s. 33.
[13] 2 och 3 första stycket §§ förordningen (2000:833) om kvalificerade elektroniska signaturer.

ordningen. En förordning som i jämförelse med direktivet, utöver att dess bestämmelser var direkt tillämpliga, hade ett bredare tillämpningsområde och omfattade fler tjänster.[14] Lagen om kvalificerade elektroniska signaturer upphävdes den 1 juli 2016. I samband med detta gjordes även ändringar i ett flertal författningar som tidigare innehållit hänvisningar till elektroniska signaturer i den upphävda lagen, till att i stället hänvisa till elektroniska underskrifter enligt eIDAS-förordningen.

Tjänstedirektivet

Europaparlamentets och rådets direktiv 2006/123/EG av den 12 december 2006 om tjänster på den inre marknaden (tjänstedirektivet) syftar bl.a. till att underlätta utövandet av etableringsfriheten för tjänsteleverantörer och den fria rörligheten för tjänster. För att uppnå det ställs i direktivet ett flertal krav på medlemsstaterna. Direktivet är ett exempel på hur det på EU-nivå ställs krav på medlemsstaterna att vidta åtgärder för att underlätta den fria rörligheten och där det ställs uttryckliga krav på att förfaranden ska kunna genomföras elektroniskt. Användning av elektroniska underskrifter kan då bli aktuellt. Signaturdirektivet får visserligen ses som föregångaren till eIDAS-förordningen, men förordningen innehåller också aspekter som introducerades i tjänstedirektivet och tillhörande kommissionsbeslut.

Medlemsstaterna ska enligt artikel 6 i tjänstedirektivet inrätta s.k. kontaktpunkter, genom vilka en tjänsteleverantör ska kunna fullgöra förfaranden och formaliteter. I Sverige fyller webbplatsen Verksamt.se den funktionen som kontaktpunkt för tjänsteföretag.[15] Vidare ställer direktivet krav på att förfaranden och formaliteter för att få tillträde till och utöva en tjänsteverksamhet ska kunna fullgöras enkelt, på distans och på elektronisk väg via den berörda kontaktpunkten samt med de behöriga myndigheterna i den aktuella medlemsstaten. I enlighet med syftet att underlätta utövande av fri rörlighet är utgångspunkten att krav som ställs inte får vara diskriminerande gentemot tjänsteföretag i andra medlemsstater.

[14] COM(2012) 238 final av den 4 juni 2012.
[15] www.verksamt.se/om-oss/om-verksamt/kontaktpunkt-for-tjansteforetag (hämtad 2021-01-13).

År 2009 antog kommissionen ett beslut för att komplettera tjänstedirektivet.[16] Syftet var enligt skäl 3 i beslutets ingress att underlätta användningen av elektroniska förfaranden. I beslutet konstateras att förfaranden på elektronisk väg bör bygga på enkla lösningar, även när det gäller användningen av elektroniska signaturer, eftersom det underlättar gränsöverskridande användning. Efter en ändamålsenlig riskbedömning kan tjänsteleverantörerna enligt artikel 1.1 emellertid för vissa förfaranden och formaliteter åläggas att införa avancerade elektroniska signaturer baserade på ett kvalificerat certifikat, med eller utan en säker anordning för skapande av signaturer. I syfte att underlätta gränsöverskridande användning och validering av sådana signaturer framgick även av artikel 2.1 i beslutet att varje medlemsstat ska upprätta en förteckning med uppgifter om de tillhandahållare av certifieringstjänster som utfärdar kvalificerade certifikat till allmänheten och som medlemsstaten övervakar eller ackrediterar. Den förteckning som avses är en förlaga till den förteckning som numera regleras genom eIDAS-förordningen (se mer om förteckningen i avsnitt 5.8)

5.4 Allmänt om eIDAS-förordningen

5.4.1 Förordningens struktur och tolkningen av dess bestämmelser

eIDAS-förordningens materiella innehåll återfinns i förordningens artiklar samt i dess bilagor, som flera av artiklarna hänvisar till (förordningen i dess helhet återfinns i bilaga 3 till detta delbetänkande). Bestämmelserna gäller som direkt tillämplig lagstiftning i Sverige och övriga medlemsstater. Utöver dessa bestämmelser består förordningen huvudsakligen av en ingress. Ingressen är uppdelad i beaktandeled och skäl. Beaktandeledet är de led i ingressen som kommer före skälen och innehåller bl.a. hänvisningar till rättsaktens rättsliga grund. Beaktandeledet avslutas med frasen ”och av följande skäl”. Därefter följer skälen vari de viktigaste bestämmelserna i artikeldelen motiveras. Eftersom EU-förordningar i motsats till svenska lagar

[16] Kommissionens beslut nr 2009/767/EG av den 16 oktober 2009 om åtgärder som underlättar användningen av förfaranden på elektronisk väg genom gemensamma kontaktpunkter i enlighet med Europaparlamentets och rådets direktiv 2006/123/EG om tjänster på den inre marknaden.

saknar förarbeten i egentlig mening går viss ledning för hur förordningens bestämmelser ska tolkas att finna i skälen. Ytterst är det dock EU-domstolen som tolkar EU-rätten.[17]

EU-parlamentet och rådet kan ge kommissionen befogenhet att anta genomförandeakter och delegerade akter för att komplettera en förordnings bestämmelser. Sådan delegation har skett i eIDAS-förordningen. Syftet är enligt skäl 70 och 71 i ingressen att på ett flexibelt och snabbt sätt kunna komplettera vissa detaljerade aspekter av förordningen samt att säkerställa enhetliga villkor för dess genomförande.

5.4.2 Förordningens syfte och tillämpningsområde

I skäl 3 i eIDAS-förordningens ingress konstateras att signaturdirektivet inte skapade ett heltäckande, gräns- och sektorsöverskridande regelverk för säkra, pålitliga och lättanvända elektroniska transaktioner. Syftet med förordningen är enligt artikel 1 att säkerställa en väl fungerande inre marknad och att uppnå en lämplig säkerhetsnivå för medel för elektronisk identifiering och betrodda tjänster. Vidare syftar förordningen enligt skäl 2 i ingressen till att öka förtroendet för elektroniska transaktioner på den inre marknaden genom att tillhandahålla en gemensam grund för ett säkert elektroniskt samspel mellan medborgare, företag och offentliga myndigheter, och därigenom öka effektiviteten hos offentliga och privata nättjänster, elektronisk affärsverksamhet och e-handel i unionen.

De områden som omfattas av förordningen är elektronisk identifiering och betrodda tjänster. Förordningens bestämmelser om elektronisk identifiering kommer inte att beröras i detta delbetänkande. Förordningen innehåller även bestämmelser som berör sådant som kan vara relevant vid användning av betrodda tjänster, exempelvis rättslig verkan av elektroniska dokument.

eIDAS-förordningen omfattar EU:s medlemsstater och har relevans också för EES-länderna. I detta delbetänkande använder vi oss emellertid enbart av begreppet medlemsstater när vi refererar till de länder som omfattas av förordningens territoriella tillämpningsområde.

[17] I skrivande stund finns det endast ett avgörande från EU-domstolen med koppling till eIDAS-förordningen (Asociación de fabricantes de morcilla de Burgos, C-309/19 P, EU:C:2020:401). Avgörandet får ses som något udda och det ger ingen direkt vägledning rörande hur förordningens ska tolkas.

5.4.3 Undantag från tillämpningsområdet

I artikel 2 görs undantag från förordningens tillämpningsområde. Enligt artikel 2.2 är förordningen inte tillämplig på tillhandahållande av betrodda tjänster som till följd av nationell rätt, eller avtal mellan en avgränsad uppsättning deltagare, används inom slutna system. Det kan enligt skäl 21 i ingressen t.ex. vara system som inrättats i företag eller offentlig förvaltning för hantering av interna förfaranden. Vidare framgår av samma skäl att endast betrodda tjänster som tillhandahålls för allmänheten och som påverkar tredje man bör uppfylla förordningens krav. Av artikel 2.3 framgår att förordningen inte heller påverkar nationell rätt eller unionsrätt som avser ingående av avtal och deras giltighet eller andra rättsliga förfarandemässiga skyldigheter avseende formkrav. Förordningen bör enligt skäl 21 heller inte inverka på nationella formkrav avseende offentliga register.

5.4.4 Inremarknadsprincip

Syftet med eIDAS-förordningen är som tidigare nämnts att säkerställa en väl fungerade inre marknad. Enligt artikel 26.2 i fördraget om Europeiska unionens funktionssätt ska den inre marknaden omfatta ett område utan inre gränser, där fri rörlighet för varor, personer, tjänster och kapital säkerställs i enlighet med bestämmelserna i fördragen. I artikel 4 i eIDAS-förordningen uttrycks inremarknadsprincipen och vad den innebär för förordningens tillämpningsområde.

Enligt artikel 4.1 får tillhandahållande av betrodda tjänster i en medlemsstat, som utförs av en tillhandahållare av betrodda tjänster som är etablerad i en annan medlemsstat, inte begränsas av skäl som omfattas av de områden som regleras i förordningen. I artikel 4.2 föreskrivs att produkter och betrodda tjänster som överensstämmer med förordningen ska omfattas av fri rörlighet på den inre marknaden.

5.4.5 Svenska kompletterande bestämmelser

Som framgår av avsnitt 5.4.1 gäller eIDAS-förordningen likt andra EU-förordningar som direkt tillämplig lagstiftning i Sverige och övriga medlemsstater. Däremot behövs det ofta nationella bestämmelser som på olika sätt kompletterar en EU-förordning. I Sverige kom-

pletteras eIDAS-förordningen av lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering och av förordningen (2016:576) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering. Dessa författningar delegerar i huvudsak olika uppdrag som anges i eIDAS-förordningen kopplade till ackreditering, certifiering och tillsyn. Med stöd av lagen och förordningen får dessutom PTS och MSB meddela föreskrifter inom vissa områden.

5.4.6 Översyn av eIDAS-förordningen

Kommissionen genomför för närvarande en översyn av eIDAS-förordningen. Av artikel 49 i förordningen framgår att en översyn över tillämpningen av förordningen ska göras och att resultaten ska rapporteras till Europaparlamentet och rådet senast den 1 juli 2020. Arbetet är dock försenat. Kommissionen höll ett s.k. öppet samråd mellan juli och oktober 2020, där intressenter bl.a. fick möjlighet att lämna synpunkter på förordningen samt lämna förslag till hur den kan utvecklas. Kommissionen har i skrivande stund aviserat att den avser att presentera förslag under första kvartalet 2021.[18]

5.4.7 Kort om förordningens systematik avseende betrodda tjänster

I avsnitt 5.5–5.9 redogörs för eIDAS-förordningens bestämmelser om betrodda tjänster. Den övergripande systematiken kan emellertid sammanfattas på följande sätt. Förordningen reglerar dels tillhandahållarna av de betrodda tjänsterna, dels de betrodda tjänsterna som sådana. Förordningen innehåller också bestämmelser som berör den rättsliga statusen för det som skapas med betrodda tjänster, exempelvis elektroniska underskrifters rättsverkan. Förordningen bör förstås så att tillhandahållarnas roll är att genom betrodda tjänster agera tredje part som skapar tillit i en transaktion mellan två eller fler parter.

Tillhandahållare av betrodda tjänster och de betrodda tjänsterna kan vara icke kvalificerade eller kvalificerade. Förordningen innehåller ett antal krav och skyldigheter som är gemensamma för båda dessa kategorier. Det är enbart kvalificerade tillhandahållare som får

[18] COM(2020) 690 final av den 19 oktober 2020, bilaga 1.

tillhandahålla kvalificerade betrodda tjänster. Kvalificerade tillhandahållare och tjänster omfattas av kompletterande och mer detaljerade krav och skyldigheter än icke kvalificerade. Många av kraven kan på olika sätt härledas till säkerhet i vid bemärkelse. Syftet med dessa krav är enligt skäl 28 i förordningens ingress att på så sätt säkerställa en hög nivå av säkerhet oavsett vilken typ av kvalificerad betrodd tjänst eller produkt som används eller tillhandahålls, vilket i sin tur bl.a. är avsett att öka förtroendet för den inre marknaden.[19] För att bli kvalificerad tillhandahållare krävs att ett tillsynsorgan i en medlemsstat beviljar tillhandahållaren status som kvalificerad. Tillsynsorganen gör, innan de beviljar sådan status, en bedömning om tillhandahållaren och de betrodda tjänster den tillhandahåller lever upp till kraven i förordningen.

Enligt skäl 27 bör förordningen vara teknikneutral och den rättsliga verkan den medför bör vara möjlig att uppnå med alla typer av tekniska medel, förutsätt att kraven i förordningen är uppfyllda.

5.5 Betrodda tjänster

5.5.1 De funktioner som utgör betrodda tjänster

Definitionen av betrodda tjänster framgår av artikel 3.16 i förordningen och presenteras i avsnitt 3.1. I det nu aktuella avsnittet och några av de följande avsnitten finns vissa upprepningar från tidigare kapitel. Syftet är att göra dessa avsnitt lättare att förstå.

Betrodda tjänster är enkelt uttryckt elektroniska tjänster som erbjuder vissa utpekade funktioner kopplade till elektroniska underskrifter, elektroniska stämplar, elektroniska tidsstämplingar eller certifikat för autentisering av webbplatser. Dessutom är elektroniska tjänster för rekommenderade leveranser en betrodd tjänst i sig. För att exemplifiera är en tjänst som skapar en avancerad elektronisk underskrift en betrodd tjänst. Den avancerade elektroniska underskriften som skapas, dvs. resultatet av tjänsten, är emellertid inte en betrodd tjänst enligt förordningens definition.

[19] Med produkt i detta sammanhang avses enligt artikel 3.21 i förordningen maskinvara eller programvara, eller relevanta komponenter i maskinvara eller programvara, som är avsedda att användas för tillhandahållande av betrodda tjänster.

De funktioner som, utöver elektroniska tjänster för rekommenderade leveranser, utgör betrodda tjänster är skapande, kontroll, validering och bevarande.

Skapande och kontroll

Funktionerna skapande och kontroll definieras inte i förordningen. Innebörden av skapande är däremot tämligen uppenbar enligt vår mening. Av artikel 3.22 framgår vidare att en anordning för underskriftsframställning är en konfigurerad programvara eller maskinvara som används för att skapa en elektronisk underskrift.

Vad kontroll innebär inom ramen för förordningen är däremot mer oklart. I den engelska språkversionen av förordningen benämns kontroll som ”verification”. Oklarheten kring denna tjänst uppstår i jämförelsen med den nedan beskrivna funktionen validering som innebär kontroll och bekräftelse av giltighet. Vi har inte identifierat någon förekomst av att enbart kontroll förekommer som en enskild betrodd tjänst även om det enligt förordningen är möjligt.

Validering

Funktionen validering definieras i artikel 3.41 i förordningen som en process genom vilken en elektronisk underskrifts giltighet kontrolleras och bekräftas.

Med validering avses alltså en tjänst som kompletterar användningen av t.ex. elektroniska underskrifter och som kontrollerar att en sådan underskrift är äkta. Detaljerade bestämmelser om validering av kvalificerade elektroniska underskrifter finns i artikel 32. Av artikel 40 följer att bl.a. artikel 32 på motsvarande sätt ska gälla för validering och bevarande av kvalificerade elektroniska stämplar. I syfte att illustrera hur valideringen av en elektronisk underskrift går till beskrivs processen nedan på ett övergripande sätt.

Genom valideringen ska alla de komponenter som har använts för att skapa underskriften säkras. Detta innebär bl.a. kontroll av giltighet för certifikatet, att valideringsuppgifterna överensstämmer med de uppgifter som lämnats till den förlitande parten och att den undertecknade eller stämplade informationen inte har förändrats sedan den skrevs under.

Valideringen innebär även att ett flertal olika kontroller görs för att säkerställa att en underskrift är äkta och oförvanskad. Dessa kontroller görs normalt av en intern tjänst i en organisation eller av en, kvalificerad eller icke kvalificerad, betrodd tjänst som tillhandahålls av tredje part. Valideringstjänsten lämnar då vidare ett resultat av valideringen som är undertecknat eller stämplat av valideringstjänsten.

De kontroller som omfattas av valideringen är att certifikatet som underskriften skapats med är utfärdat av en utfärdare som är betrodd, av den egna organisationen eller finns i förteckningen över kvalificerade tillhandahållare av kvalificerade elektroniska underskrifter (se mer om förteckningen i avsnitt 5.8). I eIDAS-förordningen finns även krav gällande kvalificerade valideringstjänster.

Bevarande

Begreppet bevarande som används i artikel 3.16 c definieras inte uttryckligen i förordningen. Av skäl 61 framgår dock att långsiktigt bevarande av uppgifter bör säkerställas genom förordningen, för att säkerställa den rättsliga giltigheten hos elektroniska underskrifter och elektroniska stämplar över längre tidsperioder samt garantera att de kan valideras oavsett kommande tekniska förändringar. Ledning för tolkning av begreppet kan även hämtas från artikel 34, där det föreskrivs att en kvalificerad tjänst för bevarande av kvalificerade elektroniska underskrifter ska göra det möjligt att förlänga underskriftens tillförlitlighet utöver perioden för teknisk giltighet. Det bör noteras att innebörden av begreppet bevarande i förordningen inte överensstämmer med innebörden av begreppet i svensk arkivlagstiftning (se mer om detta i avsnitt 8.5.2).

5.5.2 Elektroniska underskrifter

I artikel 3.10 i förordningen definieras en elektronisk underskrift som uppgifter i elektronisk form som är fogade till eller logiskt knutna till andra uppgifter i elektronisk form och som används av undertecknaren för att skriva under. Detta är den grundläggande definitionen av elektronisk underskrift och det är således en elektronisk underskrift som varken är avancerad eller kvalificerad. I syfte att förtydliga när denna nivå avses väljer vi att inom ramen för detta delbetänkande

benämna detta som en enkel elektronisk underskrift. Detta är dock inget begrepp som förekommer i förordningen.

Avancerade elektroniska underskrifter

Utöver den grundläggande definitionen av elektroniska underskrifter definierar förordningen två andra typer av underskrifter: avancerade och kvalificerade. På dessa ställs krav som går utöver grunddefinitionen. En avancerad elektronisk underskrift ska uppfylla de krav som uppställs i artikel 26:

a) Den ska vara unikt knuten till undertecknaren.

b) Undertecknaren ska kunna identifieras genom den.

c) Den ska vara skapad på grundval av uppgifter för skapande av elektroniska underskrifter som undertecknaren med hög grad av tillförlitlighet kan använda uteslutande under sin egen kontroll.

d) Den ska vara kopplad till de uppgifter som den används för att underteckna på ett sådant sätt att alla efterföljande ändringar av uppgifterna kan upptäckas.

Ytterligare krav än de som framgår ovan ställer förordningen inte upp avseende avancerade elektroniska underskrifter. Förordningen föreskriver inte heller hur det går att leva upp till dessa krav tekniskt. Som nämnts tidigare är förordningen tänkt att vara teknikneutral. Av skäl 27 framgår vidare att den rättsliga verkan som förordningen medför bör vara möjlig att uppnå med alla typer av tekniska medel, förutsatt att kraven i förordningen är uppfyllda. Det är mot bakgrund av det möjligt att med olika tekniska lösningar leva upp till kraven i artikel 26. Kommissionen har dock i ett genomförandebeslut pekat ut ett antal tekniska specifikationer avseende elektroniska underskrifter.[20] Medlemsstaterna ska erkänna avancerade elektroniska underskrifter som är i enlighet med dessa specifikationer (se mer om detta i avsnitt 5.12.1). Beslutet ska dock inte tolkas som att det ute-

[20] Kommissionens genomförandebeslut (EU) 2015/1506 av den 8 september 2015 om fastställande av specifikationer rörande format för avancerade elektroniska underskrifter och avancerade elektroniska stämplar i enlighet med artiklarna 27.5 och 37.5 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden.

slutande är dessa tekniska specifikationer som kan användas för att en avancerad elektronisk underskrift ska uppfylla kraven i artikel 26.

Kvalificerade elektroniska underskrifter

För att en elektronisk underskrift ska vara kvalificerad ställs ytterligare krav. En sådan underskrift ska utöver att uppfylla samma krav som en avancerad elektronisk underskrift därtill skapas med en kvalificerad anordning för underskriftsframställning samt baseras på ett kvalificerat certifikat för elektroniska underskrifter.

De detaljerade kraven återfinns i bilaga I till förordningen. Där framgår att sådana certifikat ska innehålla bl.a. uppgifter om den kvalificerade tillhandahållare av betrodda tjänster som utfärdar certifikaten, undertecknarens namn eller en pseudonym, uppgifter om när certifikatet börjar respektive upphör att gälla samt certifikatets identifieringskod, som måste vara unik för den aktuella kvalificerade tillhandahållaren av betrodda tjänster. Kommissionen får med stöd av artikel 28.6 i genomförandeakter fastställa referensnummer till standarder för kvalificerade certifikat för elektroniska underskrifter. I dagsläget har sådana genomförandeakter inte antagits.

Vidare finns det i artikel 24.1 krav på kvalificerade tillhandahållare att, när de utfärdar ett kvalificerat certifikat för en betrodd tjänst, på lämpligt sätt och i enlighet med nationell rätt kontrollerar identiteten och i förekommande fall eventuella särskilda attribut för den fysiska eller juridiska person till vilken det kvalificerade certifikatet utfärdas. Det finns i dagsläget inga bestämmelser i svenska författningar som utgör ”nationell rätt” i detta avseende. Informationen kan kontrolleras genom fysisk närvaro av den fysiska personen eller fysisk närvaro av en behörig företrädare för en juridisk person. Kontroll kan också under vissa förutsättningar ske på distans med hjälp av medel för elektronisk identifiering eller genom ett certifikat för en kvalificerad elektronisk underskrift eller stämpel som har utfärdats genom fysisk närvaro eller på distans. Informationen kan även kontrolleras med hjälp av andra identifieringsmetoder som erkänns på nationell nivå och som erbjuder garantier som är likvärdiga med fysisk närvaro.

Tabell 5.1 Jämförelse mellan enkla, avancerade och kvalificerade elektroniska underskrifter

	Enkel elektronisk underskrift	Avancerad elektronisk underskrift	Kvalificerad elektronisk underskrift
Rättslig verkan	Ja	Ja	Ja
Unikt knuten till undertecknaren	Inte nödvändigtvis	Ja	Ja
Identifierar undertecknaren	Inte nödvändigtvis	Ja	Ja
Uppgifter för skapande under egen kontroll	Inte nödvändigtvis	Ja	Ja
Kopplad till undertecknade uppgifter så att förändringar kan upptäckas	Inte nödvändigtvis	Ja	Ja
Skapat med kvalificerat certifikat	Inte nödvändigtvis	Inte nödvändigtvis	Ja
Privat nyckel skyddas i säker anordning	Inte nödvändigtvis	Inte nödvändigtvis	Ja

Anordningar för underskriftframställning

En anordning för underskriftframställning definieras i artikel 3.22 som en konfigurerad programvara eller maskinvara som används för att skapa en elektronisk underskrift. Anordningen är en skyddad miljö för lagring och användning av privata nycklar som smarta kort eller s.k. HSM-modul[21]. Förordningen innehåller endast krav på kvalificerade sådana anordningar. Dessa ska uppfylla kraven i bilaga II till förordningen. I bilagan finns ett flertal krav, bl.a. att kvalificerade anordningar för skapande av elektroniska underskrifter genom lämpliga tekniker och förfaranden ska säkerställa att de uppgifter för skapande av elektroniska underskrifter som används för att skapa elektroniska underskrifter i praktiken endast kan förekomma en gång och att den elektroniska underskriften på ett tillförlitligt sätt är skyddad mot förfalskning med den teknik som för närvarande finns tillgänglig.

Anordningar för skapande av kvalificerade elektroniska underskrifter och stämplar ska certifieras av offentliga eller privata organ

[21] Hardware Security Module är benämningen för en skyddad enhet för lagring och användning av krypteringsnycklar.

som utsetts av medlemsstaterna. I Sverige har Sveriges Certifieringsorgan för IT-säkerhet vid Försvarets materielverk (CSEC) den uppgiften.[22] Kommissionen har i ett genomförandebeslut fastställt de standarder för säkerhetsbedömning av informationsteknikprodukter som gäller för certifiering av kvalificerade anordningar för skapande av elektroniska underskrifter eller kvalificerade anordningar för skapande av elektroniska stämplar.[23] I Sverige får PTS med stöd av 3 § första stycket förordningen med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering meddela föreskrifter om certifiering av anordningar för skapande av kvalificerade elektroniska underskrifter och anordningar för skapande av kvalificerade elektroniska stämplar. Enligt 3 § andra stycket samma förordning får MSB meddela föreskrifter om säkerhetsegenskaper som sådana anordningar ska uppfylla. I dagsläget har PTS och MSB inte meddelat sådana föreskrifter.

Validering och bevarande av kvalificerade elektroniska underskrifter

Som framgår ovan innehåller eIDAS-förordningen även krav som avser validering av kvalificerade elektroniska underskrifter. Enligt artikel 32.1 ska en kvalificerad elektronisk underskrifts giltighet bekräftas om vissa förutsättningar är uppfyllda, bl.a. att det certifikat som stöder underskriften vid tidpunkten för undertecknandet var ett kvalificerat certifikat för elektroniska underskrifter som överensstämmer med förordningens bilaga I. Av artikel 32.2 framgår att det system som används för att validera den kvalificerade elektroniska underskriften ska ge den förlitande parten det korrekta resultatet av valideringsförfarandet och göra det möjligt för den förlitande parten att upptäcka eventuella problem som är relevanta för säkerheten. Kommissionen får med stöd av artikel 32.3 genom genomförandeakter fastställa referensnummer till standarder för validering av kvalificerade elektroniska underskrifter. Sådana genomförandeakter har i skrivande stund inte antagits.

[22] 5 § andra stycket förordningen (2007:854) med instruktion för Försvarets materielverk.
[23] Kommissionens genomförandebeslut (EU) 2016/650 av den 25 april 2016 om fastställande av standarder för säkerhetsbedömning av kvalificerade anordningar för skapande av elektroniska underskrifter och stämplar enligt artiklarna 30.3 och 39.2 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden.

Krav avseende kvalificerade valideringstjänster för kvalificerade elektroniska underskrifter finns i artikel 33.1. Även för kvalificerade valideringstjänster har kommissionen, med stöd av artikel 33.2, möjlighet att anta genomförandeakter som fastställer referensnummer för standarder för kvalificerade valideringstjänster. Sådana genomförandeakter har i dagsläget inte antagits.

I artikel 34 ställs krav på kvalificerade tjänster för bevarande av kvalificerade elektroniska underskrifter. Sådana tjänster får som framgår ovan endast tillhandahållas av kvalificerade tillhandahållare av betrodda tjänster som använder förfaranden och tekniker som gör det möjligt att förlänga den kvalificerade elektroniska underskriftens tillförlitlighet utöver perioden för teknisk giltighet. Utöver det innehåller förordningen inga bestämmelser om bevarande, utöver att bevarande av elektroniska underskrifter, stämplar eller certifikat med anknytning till dessa tjänster definieras som en betrodd tjänst (artikel 3.16 c). Kommissionen får enligt artikel 34.2 genom genomförandeakter fastställa referensnummer till standarder för kvalificerade tjänster för bevarande av kvalificerade elektroniska underskrifter men sådana genomförandeakter har för närvarande inte antagits.

5.5.3 Elektroniska stämplar

Sett till både den bakomliggande tekniken och utformningen av de bestämmelser som reglerar elektroniska stämplar och elektroniska underskrifter finns det stora likheter mellan dessa två typer av utställarverifikationer. Den avgörande skillnaden utgörs av vem som skapar en elektronisk underskrift respektive stämpel. Elektroniska stämplar skapas av juridiska personer (artikel 3.24), till skillnad från elektroniska underskrifter som skapas av fysiska personer (artikel 3.9). En elektronisk stämpel definieras i förordningen som uppgifter i elektronisk form som är fogade eller logiskt knutna till andra uppgifter i elektronisk form för att säkerställa den senares ursprung och integritet (artikel 3.25). Definitionen är snarlik den för elektroniska underskrifter men det finns alltså inte någon undertecknare när det gäller stämplar.

I likhet med vad som gäller för elektroniska underskrifter finns det i förordningen olika nivåer av elektroniska stämplar. Utöver grunddefinitionen finns avancerade elektroniska stämplar samt kvalificerade

elektroniska stämplar. Systematiken när det gäller kraven är dessutom densamma. En avancerad elektronisk stämpel ska leva upp till kraven i artikel 36:

a) Den ska vara knuten uteslutande till skaparen av stämpeln.

b) Skaparen av stämpeln ska kunna identifieras genom det.

c) Det ska vara skapat på grundval av uppgifter för skapande av elektroniska stämplar som stämpelns skapare med hög grad av tillförlitlighet under sin kontroll kan använda för skapande av elektroniska stämplar.

d) Den ska vara kopplad till de uppgifter den avser på ett sådant sätt att alla efterföljande ändringar av uppgifterna kan upptäckas.

En kvalificerad elektronisk stämpel ska enligt artikel 3.27, i likhet med vad som gäller för underskrifter, leva upp till kraven på en avancerad elektronisk stämpel samt skapas med hjälp av en kvalificerad anordning för skapande av elektroniska stämplar och som är baserat på ett kvalificerat certifikat för elektroniska stämplar. Kraven för stämplar är i stora delar desamma som för elektroniska underskrifter, med den skillnaden att kraven för stämplarna i relevanta delar hänvisar till skaparen av stämpeln i stället för undertecknaren. Ett illustrerande exempel är kraven på kvalificerade certifikat för elektroniska stämplar som fastställs i bilaga III till eIDAS-förordningen. Den enda skillnaden gentemot underskrifter är att det för stämplar finns krav på att information om skaparen av stämpeln ska finnas (namn och i förekommande fall registreringsnummer) medan det för underskrifter ska finnas information om undertecknaren.

5.5.4 Elektronisk tidsstämpling

I förordningen definieras elektronisk tidsstämpling i artikel 3.33 som uppgifter i elektronisk form som binder andra uppgifter i elektronisk form till en viss tidpunkt och därmed utgör bevis för att de senare uppgifterna existerade vid den tidpunkten. Betrodda tjänster som avser tidsstämpling kan vara kvalificerade eller icke kvalificerade. För icke kvalificerade tjänster innehåller förordningen inga krav utöver definitionen att förhålla sig till. Kvalificerad elektronisk tidsstämpling ska däremot enligt artikel 42 uppfylla följande krav:

a) Den ska binda datumet och tiden till uppgifter så att möjligheten att uppgifterna ändras utan att det går att upptäcka rimligtvis kan uteslutas.

b) Den ska vara grundad på en korrekt tidskälla som är kopplad till samordnad universaltid.

c) Den ska vara undertecknad med hjälp av en avancerad elektronisk underskrift eller förseglad med en avancerad elektronisk stämpel från den kvalificerade tillhandahållaren av betrodda tjänster eller genom en likvärdig metod.

När det kommer till det som i punkt c anges om att använda en likvärdig metod framgår av skäl 62 i förordningens ingress att innovation sannolikt kan leda till ny teknik som kan säkerställa en likvärdig säkerhetsnivå för tidsstämpling. Om en annan metod än avancerade elektroniska stämplar eller avancerade elektroniska underskrifter används bör det, enligt skäl 62, åligga tillhandahållaren av betrodda tjänster att i rapporten om bedömning av överensstämmelse visa att metoden säkerställer en likvärdig säkerhetsnivå och att den är förenlig med skyldigheterna i förordningen.

En kvalificerad elektronisk tidsstämpling ska enligt artikel 41.2 i eIDAS-förordningen omfattas av en presumtion om korrekthet hos det datum och den tid som den anger och integritet hos de uppgifter som datumet och tiden är kopplade till. Vidare ska en kvalificerad elektronisk tidsstämpling som utfärdats i en medlemsstat enligt artikel 41.3 erkännas som en kvalificerad elektronisk tidsstämpling i alla medlemsstater.

Kommissionen får enligt artikel 42.2 anta genomförandeakter som fastställer referensnummer till standarder för bindning av datum och tidpunkt till uppgifter och för korrekta tidskällor avseende kvalificerade elektroniska tidsstämplingar. Sådana genomförandeakter har i skrivande stund inte antagits.

5.5.5 Certifikat för autentisering av webbplatser

Ett certifikat för autentisering av webbplatser definieras i artikel 3.38 i förordningen som ett intyg som gör det möjligt att autentisera en webbplats och koppla webbplatsen till den fysiska eller juridiska person som certifikatet utfärdats för.

Även för autentisering av webbplatser kan certifikaten, och i förlängningen tjänsterna, vara kvalificerade eller icke kvalificerade. Inga särskilda bestämmelser, utöver definitionen, finns för de icke kvalificerade certifikaten. Krav som kvalificerade certifikat för autentisering av webbplatser ska uppfylla finns emellertid. Dels ska ett kvalificerat certifikat utfärdas av en kvalificerad tillhandahållare av betrodda tjänster, dels uppfylla kraven i bilaga IV till förordningen (artikel 3.39 samt artikel 45). Kommissionen får med stöd av artikel 45.2 genom genomförandeakter fastställa referensnummer till standarder för kvalificerade certifikat för autentisering av webbplatser. Sådana genomförandeakter har i dagsläget inte antagits.

5.5.6 Elektroniska tjänster för rekommenderade leveranser

Den sista typen av betrodda tjänster är elektroniska tjänster för rekommenderade leveranser. En sådan tjänst gör, enligt definitionen i artikel 3.36 i förordningen, det möjligt att överföra uppgifter mellan tredje män på elektronisk väg och tillhandahåller bevis avseende de överförda uppgifternas hantering, inklusive bevis för uppgifternas sändning och mottagande, och som skyddar överförda uppgifter mot risken för förlust, stöld, skada eller otillåtna ändringar. Ytterligare vägledning om hur termen ska tolkas och tillämpas ger inte förordningen. Däremot framgår av skäl 66 att det är av avgörande betydelse att det föreskrivs en rättslig ram för att främja gränsöverskridande erkännande mellan befintliga nationella rättssystem för elektroniska tjänster för rekommenderade leveranser. Vidare framgår av samma skältext att den ramen skulle kunna öppna nya marknadsmöjligheter för unionens tillhandahållare av betrodda tjänster att erbjuda nya paneuropeiska tjänster för elektroniska tjänster för rekommenderade leveranser.

Elektroniska tjänster för rekommenderade leveranser kan vara kvalificerade eller icke kvalificerade. Bestämmelser utöver definitionen för icke kvalificerade tjänster saknas i förordningen. De krav som ställs på kvalificerade elektroniska tjänster för rekommenderade leveranser är bl.a. att de ska tillhandahållas av en eller flera kvalificerade tillhandahållare av betrodda tjänster, att de med hög grad av tillförlitlighet ska säkerställa avsändarens identitet och att de ska säkerställa adressatens identitet innan uppgifterna levereras (artikel 44.1).

Om uppgifterna överförs mellan två eller flera kvalificerade tillhandahållare av betrodda tjänster ska kraven gälla för alla involverade kvalificerade tillhandahållare av betrodda tjänster.

Kommissionen får enligt artikel 44.2 anta genomförandeakter som fastställer referensnummer till standarder för processer för att sända och ta emot uppgifter avseende kvalificerade elektroniska tjänster för rekommenderade leveranser. Sådana genomförandeakter har för närvarande inte antagits.

5.6 Tillhandahållare av betrodda tjänster

5.6.1 Kvalificerade och icke kvalificerade tillhandahållare

Tillhandahållare av betrodda tjänster har en central roll i eIDAS-förordningen. En tillhandahållare av betrodda tjänster är enligt artikel 3.19 i eIDAS-förordningen en fysisk eller juridisk person som tillhandahåller en eller flera betrodda tjänster, antingen i egenskap av kvalificerade eller icke kvalificerade tillhandahållare av betrodda tjänster. Som definitionen anger kan en tillhandahållare vara kvalificerad eller icke kvalificerad. Skillnaden mellan de båda framgår bl.a. av artikel 3.20, där det föreskrivs att en kvalificerad tillhandahållare är en tillhandahållare av betrodda tjänster som tillhandahåller en eller flera kvalificerade betrodda tjänster och som beviljats status som kvalificerad av tillsynsorganet.

5.6.2 Gemensamma säkerhetskrav och krav på incidentrapportering

Det finns anledning att hålla isär kvalificerade och icke kvalificerade tillhandahållare av betrodda tjänster eftersom de kvalificerade tillhandahållarna omfattas av betydligt fler bestämmelser och krav än de icke kvalificerade. Vissa av bestämmelserna i eIDAS-förordningen är emellertid gemensamma oavsett tillhandahållarens status.

I artikel 19.1 föreskrivs att tillhandahållare av betrodda tjänster ska vidta lämpliga tekniska och organisatoriska åtgärder för att hantera riskerna för säkerheten hos de betrodda tjänster som de tillhandahåller. Åtgärderna ska säkerställa att säkerhetsnivån står i proportion till graden av risk och den senaste tekniska utvecklingen ska

beaktas. Åtgärder ska i synnerhet vidtas för att förhindra eller minimera säkerhetsincidenters inverkan samt för att informera berörda parter om de negativa effekterna av eventuella sådana incidenter.

Enligt artikel 19.2 ska tillhandahållare av betrodda tjänster, utan otillbörligt dröjsmål och under alla omständigheter inom 24 timmar efter upptäckt, underrätta tillsynsorganet och i förekommande fall andra relevanta organ, såsom det behöriga nationella organet för informationssäkerhet eller dataskyddsmyndigheten, om alla säkerhetsincidenter eller integritetsförluster som i betydande omfattning påverkar den betrodda tjänst som tillhandahålls eller på de personuppgifter som ingår i denna. När det är troligt att säkerhetsincidenten eller integritetsförlusten kommer att ha negativ inverkan på en fysisk eller juridisk person till vilken den betrodda tjänsten har tillhandahållits, ska tillhandahållaren av betrodda tjänster utan onödigt dröjsmål även underrätta den fysiska eller juridiska personen om säkerhetsincidenten eller integritetsförlusten. När det är lämpligt, särskilt om säkerhetsincidenten eller integritetsförlusten rör två eller flera medlemsstater, ska det underrättade tillsynsorganet informera tillsynsorganen i övriga berörda medlemsstater samt ENISA. Det underrättade tillsynsorganet ska informera allmänheten eller kräva att tillhandahållaren av betrodda tjänster gör det, om den slår fast att ett avslöjande av säkerhetsincidenten eller integritetsförlusten ligger i allmänhetens intresse. Enligt artikel 19.4 får kommissionen anta genomförandeakter som ytterligare specificerar säkerhetsåtgärder eller fastställer format, förfaranden och tidsfrister avseende säkerhetsincidenter och liknande. Sådana genomförandeakter har emellertid i skrivande stund inte antagits.

I december 2020 presenterade kommissionen sitt förslag till reviderat direktiv om åtgärder för en hög nivå av cybersäkerhet inom unionen.[24] Förslaget är avsett att ersätta det nuvarande s.k. NIS-direktivet (Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen) och innebär även att artikel 19 i eIDAS-förordningen upphävs. Tillhandahållare av betrodda tjänster är i dagsläget undantagna från direktivets tillämpningsområde.[25] Betrodda tjänster skulle genom förslaget omfattas av direktivets bestämmelser avseende säkerhetsåtgärder och incident-

[24] COM(2020) 823 final av 16 december 2020.
[25] 6 § lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.

rapportering. Innehållet i dessa bestämmelser är i stora delar likt det som framgår av artikel 19 i eIDAS-förordningen, men de är mer detaljerade än den nuvarande regleringen. Detta skulle således innebära att tillhandahållare av betrodda tjänster omfattas av samma krav som tillhandahållare av andra i direktivet utpekade tjänster.

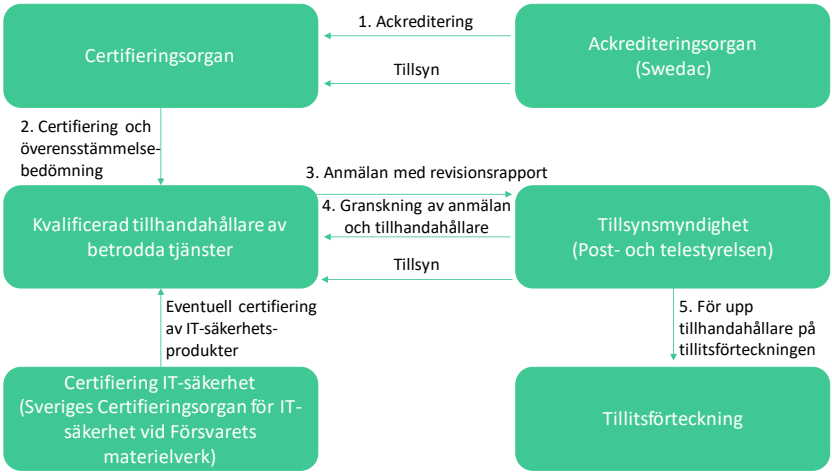
5.6.3 Skillnader i skadeståndsansvar och bevisbörda

Av artikel 13.1 framgår att tillhandahållare av betrodda tjänster omfattas av skadeståndsansvar för skada som åsamkats en fysisk eller juridisk person avsiktligt eller på grund av oaktsamhet genom underlåtenhet att uppfylla kraven i förordningen. Placeringen av bevisbördan skiljer sig åt beroende på om tillhandahållaren är kvalificerad eller inte. Presumtionen vid skada är att bevisbördan ligger på tillhandahållaren om denne är kvalificerad. Det är således den kvalificerade tillhandahållaren som ska bevisa att den skada som uppstått har uppstått utan dennes avsikt eller oaktsamhet. Om tillhandahållaren är icke kvalificerad vilar i stället bevisbördan på den som gör gällande att skada har uppstått.

5.6.4 Krav på kvalificerade tillhandahållare

Som tidigare nämnts omfattas kvalificerade tillhandahållare av betrodda tjänster av betydligt fler krav än icke kvalificerade.

Figur 5.3 Etablering av kvalificerad tillhandahållare av betrodda tjänster



Källa: Post- och telestyrelsen.

För att få status som kvalificerad tillhandahållare krävs enligt artikel 21.1 en anmälan till ett tillsynsorgan (se figur 5.3 för hela gången vid sådan etablering). Tillhandahållaren ska i samband med anmälan även lämna in en rapport om överensstämmelsebedömning som utfärdats av ett organ för bedömning av överensstämmelse. Bedömningen av överenstämmelse ska omfatta både tillhandahållaren som sådan och de betrodda tjänster som tillhandahållaren vill ska vara kvalificerade. Ett sådant organ ska enligt artikel 3.18 vara ackrediterat för att göra bedömningar av sådana tillhandahållare och de tjänster de tillhandahåller. I Sverige ackrediterar den statliga myndigheten Styrelsen för ackreditering och teknisk kontroll (Swedac) sådana organ. PTS får med stöd av 2 § förordningen med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering meddela föreskrifter om krav för ackreditering av organ för bedömning av överensstämmelse, hur bedömningar av överensstämmelse ska göras samt rapportering av bedömningar av överensstämmelse. I skrivande stund har sådana föreskrifter inte meddelats.

Tillsynsorganet ska enligt artikel 21.2 kontrollera om tillhandahållaren och de betrodda tjänster som denne tillhandahåller uppfyller kraven i förordningen. Även inom detta område har kommissionen enligt artikel 21.4 möjlighet att anta genomförandeakter, men sådana genomförandeakter har i dagsläget inte antagits. Det har i sin tur lett

till att de nationella tillsynsorganen själva, på olika sätt, har fått bestämma hur bedömningen ska göras (se mer om detta i avsnitt 5.11). Om tillsynsorganet kommer fram till att tillhandahållaren och de betrodda tjänster som denne tillhandahåller uppfyller kraven i förordningen ska organet bevilja tillhandahållaren status som kvalificerad tillhandahållare av betrodda tjänster. Detsamma gäller de tjänster som den tillhandahåller. I samband med det ska den aktuella medlemsstatens förteckning över kvalificerade tillhandahållare och betrodda tjänster, som avses i artikel 22.1 i förordningen, uppdateras så att tillhandahållaren och tjänsterna förs upp på förteckningen (se mer om förteckningarna i avsnitt 5.8).

Uttryckliga krav som kvalificerade tillhandahållare har att förhålla sig till finns i artikel 24. Kraven avser primärt tillhandahållaren som sådan och flera av dem har starka kopplingar till de certifikat som utfärdas (se avsnitt 5.5.2 för kraven avseende certifikat). Nedan följer några exempel på dessa krav.

Kvalificerade tillhandahållare ska bl.a. använda tillförlitliga system och produkter som är skyddade mot ändringar och säkerställa den tekniska säkerheten och tillförlitligheten hos den process som stöds av systemen (artikel 24.2 e). De ska också ha personal, och i förekommande fall underleverantörer, som har den sakkunskap, tillförlitlighet samt de erfarenheter och kvalifikationer som behövs och som har genomgått lämplig utbildning om regler för säkerhet och skydd för personuppgifter (artikel 24.2 b). Vidare ska kvalificerade tillhandahållare förfoga över tillräckliga ekonomiska medel och/eller skaffa sig lämplig ansvarsförsäkring i enlighet med nationell rätt, detta med anledning av risken för ansvar vid skador (artikel 24.2 c).

Tillhandahållare som utfärdar kvalificerade certifikat ska bl.a. upprätta en certifikatdatabas som hålls uppdaterad (artikel 24.2 k). Om de beslutar att återkalla ett certifikat ska ett sådant återkallande registreras i certifikatdatabasen och offentliggöras i god tid och senast inom 24 timmar efter mottagandet av begäran (artikel 24.3).

Kommissionen får med stöd av artikel 24.5 genom genomförandeakter fastställa referensnummer till standarder för tillförlitliga system och produkter som uppfyller kraven i artikel 24.2 e och f. Sådana genomförandeakter har i skrivande stund inte antagits.

Enligt artikel 20.1 ska kvalificerade tillhandahållare minst en gång vartannat år och på egen bekostnad granskas av ett organ för bedömning av överensstämmelse. Syftet med granskningen är att bekräfta

att tillhandahållaren och de kvalificerade betrodda tjänsterna uppfyller kraven i förordningen. Den rapport som bedömningen resulterar i ska överlämnas till tillsynsorganet.

5.7 Tillsyn

5.7.1 Tillsynsorganens uppgifter

Utöver tillhandahållare av betrodda tjänster har de nationella tillsynsorganen en viktig roll i eIDAS-förordningen. Enligt artikel 17.1 ska medlemsstaterna utse ett tillsynsorgan som är etablerat inom deras territorium som ska ansvara för tillsynsuppgifter i den medlemsstat som utsett organet. Det är även möjligt att utse ett tillsynsorgan som är etablerat i en annan medlemsstat, efter ömsesidig överenskommelse med den medlemsstaten. I Sverige är PTS tillsynsorgan.[26]

eIDAS-förordningen ställer betydligt högre krav på tillsyn över kvalificerade tillhandahållare och betrodda tjänster än tillhandahållare och betrodda tjänster som är icke kvalificerade. När det gäller kvalificerade tillhandahållare och betrodda tjänster ska organen aktivt utöva tillsyn i enlighet med de bestämmelser som finns i förordningen, för att se till att tillhandahållarna och tjänsterna uppfyller kraven i förordningen. För icke kvalificerade tillhandahållare och tjänster är tillsynen emellertid händelsestyrd, således efter rapporterad incident eller vid misstanke om att reglerna inte efterlevs.

Vissa av tillsynsorganens uppgifter har nämnts i tidigare avsnitt, såsom beviljandet av status om kvalificerad tillhandahållare och hantering av säkerhetsincidenter. Organen får dessutom när som helst granska eller begära att ett organ för bedömning av överensstämmelse gör en överensstämmelsebedömning av de kvalificerade tillhandahållarna för att bekräfta att de och de kvalificerade betrodda tjänster som de tillhandahåller uppfyller kraven i förordningen.

Tillsynsorganen i medlemsstaterna ska samarbeta och ge varandra ömsesidigt bistånd när det behövs, exempelvis genom att förse ett annat organ med information eller bistå med tillsynsåtgärder. Det finns även ett forum för tillsynsorganen, Forum of European Supervisory Authorities for trust service providers (FESA) som bl.a. syftar

[26] 4 § förordningen (2016:576) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering.

till att främja samarbetet mellan organen. Utöver tillsynsorgan EU:s medlemsstater deltar också tillsynsorgan från andra länder i forumet, exempelvis Turkiet och Serbien.[27]

5.7.2 Sanktioner

I artikel 16 i eIDAS-förordningen föreskrivs att medlemsstaterna ska fastställa bestämmelser om de sanktioner som ska tillämpas vid överträdelser av förordningen. Sanktionerna ska vara effektiva, proportionella och avskräckande. I Sverige får PTS, i egenskap av tillsynsmyndighet, med stöd av 6 § lagen med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering meddela de förelägganden och förbud som behövs för efterlevnaden av eIDAS-förordningen och tillhörande rättsakter samt den svenska lagen och föreskrifter som har meddelats med stöd av den. Sådana förelägganden och förbud får även förenas med vite.

5.8 Förteckning över tillhandahållare och betrodda tjänster

Enligt artikel 22 i eIDAS-förordningen ska varje medlemsstat upprätta, underhålla och offentliggöra förteckningar med uppgifter om kvalificerade tillhandahållare av betrodda tjänster som den ansvarar för, tillsammans med uppgifter om de kvalificerade betrodda tjänster som dessa tillhandahåller. Dessa förteckningar benämns som ”trusted list” i den engelska språkversionen av förordningen och det är även vanligt att den engelska termen används i Sverige.[28] Vi föreslår att förteckningen i Sverige ska benämnas tillitsförteckning (se avsnitt 8.3.2). Medlemsstaterna ska på ett säkert sätt upprätta, underhålla och offentliggöra elektroniskt undertecknade eller förseglade förteckningar i en form som lämpar sig för automatiserad behandling. Kommissionen har i ett genomförandebeslut fastställt tekniska minimispecifikationer och format för förteckningarna.[29] Syftet med

[27] www.fesa.eu/members.html (hämtad 2021-01-25).
[28] Se t.ex. Dir. 2020:27 s.2.
[29] Kommissionens genomförandebeslut (EU) 2015/1505 av den 8 september 2015 om fastställande av tekniska minimispecifikationer och format rörande förteckningar över betrodda tjänsteleverantörer i enlighet med artikel 22.5 i Europaparlamentets och rådets förordning

förteckningarna är det ska gå att kontrollera vilka tillhandahållare på marknaden som är kvalificerade samt se vilka betrodda tjänster de tillhandahåller.

I Sverige tillhandahålls förteckningen, i enlighet med 5 § förordningen med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering, av PTS. Av samma bestämmelse framgår att kvalificerade tillhandahållare och kvalificerade betrodda tjänster får vara med i förteckningen. I nuläget finns två kvalificerade tillhandahållare på den svenska förteckningen.

Kommissionen tillhandahåller ett webbverktyg, Trusted List Browser, som gör det möjligt att söka i alla medlemsstaters förteckningar.[30]

Av kommissionens genomförandebeslut framgår av artikel 2 att också icke kvalificerade tillhandahållare av betrodda tjänster får föras upp på förteckningen tillsammans med information om de icke kvalificerade betrodda tjänster de tillhandahåller. Det är frivilligt för medlemsstaterna att göra det och det sker då på ”nationell nivå” (skäl 4). Det ska tydligt anges vilka tillhandahållare av betrodda tjänster som inte är kvalificerade och de icke kvalificerade betrodda tjänster de tillhandahåller (se mer om detta i avsnitt 7.6). Vissa medlemsstater har valt att föra upp icke kvalificerade tillhandahållare på sina respektive förteckningar.[31]

5.9 Rättslig verkan

Förordningen innehåller ett flertal bestämmelser om rättslig verkan. Till att börja med föreskrivs i artikel 25.1, 35.1, 41.1 respektive 46 att elektroniska underskrifter, elektroniska stämplar, elektroniska tidsstämplingar och elektroniska dokument inte får förvägras rättslig verkan eller giltighet som bevis vid rättsliga förfaranden enbart på grund av att de har elektronisk form eller, med undantag för elektroniska dokument, för att de inte lever upp till kraven för att vara kvalificerade. För elektroniska tjänster för rekommenderade leveranser gäller enligt artikel 43.1 att uppgifter som sänds och tas emot genom en sådan tjänst inte får förvägras rättslig verkan eller giltighet

(EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden.

[30] https://webgate.ec.europa.eu/tl-browser/ (hämtad 2021-01-13).

[31] Bl.a. Danmark och Ungern.

som bevis vid rättsliga förfaranden enbart på grund av att de har elektronisk form eller för att de inte uppfyller kraven på den kvalificerade elektroniska tjänsten för rekommenderade leveranser. Innebörden av den senare skrivningen är något svårtolkad. Den torde emellertid innebära att uppgifterna inte får förvägras rättslig verkan enbart på grund av att tjänsten som de har sänts eller tagits emot med inte är kvalificerad.

För vissa tjänster finns dessutom egna bestämmelser om tjänsterna är kvalificerade. I artikel 25.2 föreskrivs att en kvalificerad elektronisk underskrift ska ha motsvarande rättsliga verkan som en handskriven underskrift. Denna bestämmelse förtjänar att belysas ytterligare eftersom det under vårt kartläggningsarbete visat sig att det finns olika tolkningar av dess innebörd. Signaturdirektivet innehöll, som framgår av avsnitt 5.3, också en artikel om rättslig verkan för elektroniska signaturer. Av artikeln framgick att medlemsstaterna skulle säkerställa att avancerade elektroniska signaturer som baseras på ett kvalificerat certifikat och som skapas av en säker anordning för skapande av signaturer uppfyller de rättsliga kraven på en signatur i förhållande till uppgifter i elektronisk form, på samma sätt som en handskriven signatur uppfyller samma krav i förhållande till uppgifter på papper. Det skulle även säkerställas att en sådan signatur godtas som bevis vid rättsliga förfaranden. Den senare delen föranledde för svenskt vidkommande inga åtgärder med hänsyn till principen om fri bevisprövning.[32]

Vid remitteringen av den promemoria som lämnade förslag till genomförandet av signaturdirektivet menade vissa remissinstanser att innebörden av artikel 5 var att verkan av en elektronisk signatur måste jämställas med verkan av en egenhändig namnteckning. Enligt regeringens mening kunde dock inte artikeln tolkas isolerat från övriga artiklar i direktivet och att det fick anses klart att direktivet inte inom något rättsområde föreskriver att elektronisk kommunikation måste accepteras.[33]

eIDAS-förordningens bestämmelser om kvalificerade elektroniska underskrifters rättsverkan överensstämmer sett till dess sakinnehåll i stort med regleringen i signaturdirektivet. Likt artikel 5 i signaturdirektivet behöver artikel 25.2 i förordningen tolkas i relation till artikel 2.3 i förordningen där det framgår att förordningen inte påverkar nationell rätt eller unionsrätt som avser ingående av avtal och

[32] Prop. 1999/2000:117 s. 56.
[33] A.a.

deras giltighet eller andra rättsliga eller förfarandemässiga skyldigheter avseende formkrav.

I promemorian som föreslog kompletterande nationella bestämmelser till eIDAS-förordningen avhandlades frågan om förhållandet mellan artikel 25 och nationell rätt.[34] Den bedömning som gjordes där var att det inte finns några regler i svensk rätt som kan sägas förvägra bl.a. elektroniska underskrifter eller andra betrodda tjänster rättslig verkan över huvud taget. Det konstaterades vidare att de formkrav för rättshandlingar som utesluter elektronisk kommunikation är uttryckligen tillåtna enligt artikel 2.3 i eIDAS-förordningen. Det anges där att förordningen inte påverkar nationell rätt eller unionsrätt som avser ingående av avtal och deras giltighet eller andra rättsliga eller förfarandemässiga skyldigheter avseende formkrav. Gällande kravet i artikel 25.2 om att en kvalificerad elektronisk underskrift ska ha motsvarande rättsliga verkan som en handskriven underskrift framfördes att detta i sak överensstämmer med vilken verkan medlemsstaterna ska säkerställa att kvalificerade elektroniska signaturer hade enligt artikel 5.1 a i signaturdirektivet. Förordningen föreskriver enligt promemorian inte att elektronisk kommunikation måste accepteras inom något rättsområde och innebörden av artikel 1 och 2.3 måste anses vara att det även fortsättningsvis är tillåtet för medlemsstaterna att ha formkrav på egenhändiga underskrifter som utesluter användning av elektroniska underskrifter. Artikel 25.2 i förordningen får därmed enligt promemorian tolkas på så sätt att om det är tillåtet att uppfylla ett formkrav med elektroniska rutiner måste kvalificerade elektroniska underskrifter alltid godtas. Vi delar den bedömningen för det fall en myndighet inte anvisar användning av en e-tjänst (se mer om detta i avsnitt 5.10). I förarbetena till lagen med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering behandlas inte frågan utöver att lagstiftaren instämmer i promemorians bedömning att artikel 25 inte bedöms behöva någon kompletterande bestämmelse.[35]

Vidare finns i eIDAS-förordningen för kvalificerade tjänster för elektroniska stämplar (artikel 35.2), elektroniska tidsstämplingar (artikel 41.2) och elektroniska tjänster för rekommenderade leveranser (artikel 43.2) också regler om presumtion om integritet och korrekt-

[34] *Promemoria – Kompletterande bestämmelser till EU-förordningen om elektronisk identifiering*, s. 56.
[35] Prop. 2015/16:72 s. 43.

het. En kvalificerad elektronisk stämpel ska t.ex. enligt ovan nämnd artikel omfattas av en presumtion om integritet hos de uppgifter som den kvalificerade elektroniska stämpeln är kopplad till och om att de har korrekt ursprung.

Slutligen finns bestämmelser om att kvalificerade elektroniska underskrifter och stämplar som baseras på ett kvalificerat certifikat som utfärdats i en medlemsstat ska erkännas som kvalificerad elektronisk underskrift eller stämpel i alla andra medlemsstater (artikel 25.3 och 35.3). Detsamma gäller för en kvalificerad elektronisk tidsstämpling (artikel 41.3).

5.10 Vilka krav ställer eIDAS-förordningen på den offentliga förvaltningen?

Under utredningens kartläggningsarbete har det framkommit att det för vissa aktörer råder osäkerhet rörande i vilka situationer förordningen är tillämplig och vilka krav den ställer på den offentliga förvaltningen. Nedan presenteras de områden där vi identifierat sådana frågeställningar.

Förordningen gäller inte bara för gränsöverskridande användning av betrodda tjänster

En vanlig fråga rörande eIDAS-förordningen är om den endast omfattar gränsöverskridande situationer. Förordningens bestämmelser medför att området betrodda tjänster till stora delar är harmoniserat inom EU. Detta innebär att alla medlemsstater tillämpar samma bestämmelser. Det enda utrymme medlemsstaterna har för att behålla eller införa nationella bestämmelser avseende betrodda tjänster är enligt skäl 24 i förordningens ingress när dessa tjänster inte har harmoniserats fullständigt genom förordningen. Förordningens bestämmelser gäller dock oavsett om situationen eller transaktionen är gränsöverskridande eller inte.

Förordningen uppställer inga krav avseende användning av betrodda tjänster

Förordningen fastställer ett allmänt regelverk för användningen av betrodda tjänster. Det innebär emellertid enligt skäl 21 i förordningens ingress inte en allmän skyldighet att använda betrodda tjänster. Förordningen uppställer alltså inte krav på att betrodda tjänster måste användas. Krav på sådan användning kan emellertid finnas i annan författning och bestämmelserna i eIDAS-förordningen kan därigenom indirekt uppställa krav som ska följas. Ett exempel på detta är svenska författningar som anger att en avancerad elektronisk underskrift i enlighet med artikel 3 i förordningen ska användas för ett visst förfarande.

Krav om att erkänna vissa format av underskrifter och stämplar

Även om förordningen som ovan framgår inte innebär någon allmän skyldighet att använda betrodda tjänster finns det däremot bestämmelser om krav på att erkänna elektroniska underskrifter och stämplar. Av artikel 25.1 respektive 35.1 framgår att elektroniska underskrifter och stämplar inte får förvägras rättslig verkan enbart på grund av att de har elektronisk form eller för att de inte lever upp till kraven för att vara kvalificerade. Om formkrav saknas kan således en myndighet inte vägra att ta emot en elektroniskt undertecknad eller stämplad handling enbart utifrån den grunden att den har elektronisk form. Det kan emellertid finnas andra skäl att inte acceptera en handling. Vad gäller typer av underskrifter, format och metoder anges i artikel 27.1 att om en medlemsstat kräver en avancerad elektronisk underskrift för användningen av en nättjänst som erbjuds av ett offentligt organ eller på ett offentligt organs vägnar, ska medlemsstaten erkänna avancerade elektroniska underskrifter, avancerade elektroniska underskrifter som är baserade på ett kvalificerat certifikat för elektroniska underskrifter och kvalificerade elektroniska underskrifter i åtminstone de format eller med de metoder som anges i genomförandeakter.[36] En motsvarande bestämmelse för elektroniska stämp-

[36] Ett offentligt organ definieras i artikel 3.7 i förordningen som statlig, regional eller lokal myndighet, ett organ som lyder under offentlig rätt eller en sammanslutning som bildats av en eller flera sådana myndigheter eller ett eller flera sådana offentligrättsliga organ, eller en privat enhet som av minst en av dessa myndigheter, enheter eller sammanslutningar har bemyndigats att tillhandahålla offentliga tjänster när de agerar i enlighet med ett sådant bemyndigande.

lar finns i artikel 37.1. Bestämmelserna innebär att om det krävs en avancerad elektronisk underskrift eller stämpel i en nättjänst som exempelvis en myndighet erbjuder ska myndigheten också erkänna de underskrifter som räknas upp, i de format som har angetts i en genomförandeakt. En sådan genomförandeakt har antagits av kommissionen[37] och i det beslutet anges formaten och de tekniska specifikationerna som måste erkännas.[38]

Bakgrunden till bestämmelserna återfinns i skäl 50 i förordningens ingress där det framgår att eftersom behöriga myndigheter i medlemsstaterna använder olika avancerade elektroniska underskrifter av olika format för att underteckna sina dokument elektroniskt är det nödvändigt att se till att åtminstone ett visst antal format av avancerade elektroniska underskrifter (och stämplar) kan stödjas tekniskt av medlemsstaterna, när de erhåller dokument som undertecknats elektroniskt.

I artikel 27.2 föreskrivs vidare att om en medlemsstat kräver en avancerad elektronisk underskrift som är baserad på ett kvalificerat certifikat för användningen av en nättjänst som erbjuds av ett offentligt organ eller på ett offentligt organs vägnar, ska medlemsstaten erkänna avancerade elektroniska underskrifter som är baserade på ett kvalificerat certifikat och kvalificerade elektroniska underskrifter i åtminstone de format eller med de metoder som anges i genomförandeakter. En motsvarande bestämmelse för stämplar finns i artikel 37.2.

Slutligen föreskrivs i artikel 27.3 för underskrifter respektive artikel 37.3 för stämplar att medlemsstaterna för gränsöverskridande användning av nättjänster som erbjuds av offentliga organ inte får kräva en underskrift eller stämpel med högre säkerhetsnivå än den som gäller för kvalificerade elektroniska underskrifter eller stämplar.

Medlemsstaterna avgör vilken nivå som ska krävas

eIDAS-förordningen uppställer inga krav om vilken nivå av underskrift eller stämpel som krävs för en viss nättjänst (notera dock artikel 27.3 samt 37.3 som nämns ovan). Om kravet som uppställs är

[37] Kommissionens genomförandebeslut (EU) 2015/1506.

[38] För XML, CMS (Cryptographic Message Syntax) eller PDF gäller basprofilerna XAdES, CAdES respektive PAdES. Även s.k. underskrifts- eller stämpelbehållare, ASIC, ska kunna hanteras i enlighet med dessa basprofiler. Vad gäller basprofilerna hänvisas i beslutet till diverse ETSI-specifikationer.

avancerade elektroniska underskrifter eller stämplar ska aktören kunna erkänna sådana underskrifter och stämplar i de format och med de specifikationer som anges i genomförandebeslutet. Kräver nättjänsten i stället en kvalificerad elektronisk underskrift eller stämpel gäller samma princip. Däremot behöver tjänsten inte erkänna avancerade elektroniska underskrifter eller stämplar i en sådan situation, eftersom kravet är ställt på en högre nivå.

Oklart om förordningen begränsar offentliga aktörers möjlighet att hänvisa till vissa elektroniska kanaler

Artikel 27 och 37 tillsammans med kommissionens genomförandebeslut (EU) 2015/1506 innebär som tidigare nämnts att offentlig förvaltning måste erkänna elektroniska underskrifter och stämplar på vissa nivåer och i vissa format som följer vissa tekniska specifikationer. Ytterligare en fråga som behöver belysas är vad förordningens bestämmelser innebär vid användning av en viss elektronisk kanal. Det är t.ex. vanligt att svenska myndigheter tillhandahåller e-tjänster där användaren identifierar sig och sedan undertecknar en handling i själva tjänsten. Det kan alltså vara så att ett visst förfarande, t.ex. en ansökan om ett tillstånd, kan genomföras elektroniskt genom att använda en e-tjänst men att alternativa sätt att genomföra förfarandet elektroniskt inte erbjuds av myndigheten. Detta är således ett hinder för den som exempelvis vill skicka in elektroniskt undertecknade handlingar där undertecknandet skett utanför myndighetens e-tjänst.

Artikel 27.1 i förordningen innebär som framgår ovan att en medlemsstat som kräver en avancerad elektronisk underskrift för användningen av en nättjänst ska erkänna sådana underskrifter som föreskrivs i kommissionens genomförandebeslut. Det kan konstateras att artikeln och förordningen i övrigt inte innehåller några bestämmelser om hur en nättjänst ska utformas. Det saknas också bestämmelser som tydliggör om offentliga aktörer själva ska kunna välja hur ett förfarande är uppbyggt, vilket skulle kunna påverka aktörens praktiska möjligheter att erkänna vissa elektroniska underskrifter eller stämplar. Av skäl 23 i förordningen framgår att i den mån förordningen medför en skyldighet att erkänna en betrodd tjänst, får en sådan betrodd tjänst ogillas endast om skyldighetens adressat av tekniska skäl bortom adressatens direkta kontroll är oförmögen att läsa eller kontrollera den. Vidare framgår att denna skyldighet dock inte

i sig bör medföra att ett offentligt organ är tvunget att anskaffa den maskinvara och programvara som krävs för teknisk läsbarhet för alla befintliga betrodda tjänster. Utöver bestämmelserna ovan måste även förordningens bestämmelser om rättslig verkan i artikel 25.1 och 35.1 beaktas i detta sammanhang.

Sammanfattningsvis innehåller eIDAS-förordningen ett antal bestämmelser och skälstexter som när de läses samlat skapar en otydlig bild av vad som egentligen åligger en myndighet när formkrav saknas i författning och en enskild eller juridisk person vill inkomma med en elektroniskt undertecknad eller stämplad handling på annat sätt än den av myndigheten anvisade e-tjänsten. Finns det emellertid formkrav som anger att en e-tjänst ska användas får detta enligt vår bedömning anses innebära att undantaget i artikel 2.3 är tillämpligt och att en vägran att acceptera andra former av elektroniskt inlämnande inte står i strid med förordningens bestämmelser.[39]

I fall där sådana formkrav saknas kan det här noteras att regeringen i förarbetena till nyligen införda ändringar i rättegångsbalken anfört att regleringen i eIDAS-förordningen inte medför någon skyldighet för domstolarna att ta emot ansökningar som är undertecknade med en elektronisk underskrift och att det inte heller i övrigt finns någon sådan skyldighet.[40] När det gäller förutsättningarna för att ta emot olika tekniska format för avancerade elektroniska underskrifter framfördes vidare att detta beror till stor del på vilken teknisk lösning som väljs för det systemstöd som utvecklas.[41]

Trots regeringens ställningstagande får rättsläget rörande om offentliga aktörer, utan att formkrav finns, har möjlighet att hänvisa till en viss elektronisk kanal samt förordningens eventuella påverkan på aktörens möjligheter att inte acceptera att ett förfarande genomförs på annat sätt enligt utredningen bedömas som oklar. Detta är emellertid en fråga för den fortsatta rättstillämpningen och i slutändan EU-domstolen att avgöra.[42]

---

[39] Se t.ex. 1 och 4 § § Skatteverkets föreskrifter (SKVFS 2014:22) om begäran om utbetalning för hushållsarbete, senast ändrade genom (SKVFS 2020:19).
[40] Prop. 2019/20 :189 s. 35, jfr även prop. 2017/18:126 s. 40 f. och 43.
[41] Prop. 2019/20 :189 s. 35. Upplysningsvis kan nämnas att Sveriges Domstolar därefter infört en e-tjänst för dessa förfaranden: www.domstol.se/tjanster-och-blanketter/signera-och-skicka-handlingar-digitalt/ (hämtad 2021-01-18).
[42] Vi har endast hittat ett svenskt domstolsavgörande där dessa frågeställningar berörts, i det fallet frågan om rättslig verkan i artikel 25.1 och då endast i den skiljaktiga meningen (Kammarrätten i Stockholms dom den 11 november 2020 i mål nr 4566-20). Det finns även ett beslut från Justitieombudsmannen (dnr 742-2018) som är värt att notera i sammanhanget.

5.11 Vägledningar som kompenserar bristen på genomförandeakter

Som framgår av avsnitt 5.4.1 har kommissionen getts befogenhet att anta genomförandeakter för att komplettera eIDAS-förordningens bestämmelser för att i enlighet med skäl 70 och 71 i ingressen att på ett flexibelt och snabbt sätt kunna komplettera vissa detaljerade aspekter av förordningen samt att säkerställa enhetliga villkor för genomförandet av förordningen. Kommissionen har i skrivande stund beslutat och publicerat åtta sådana akter, varav fyra av dem avser området betrodda tjänster.[43] Resterande fyra avser elektronisk identifiering. Förordningen ger emellertid kommissionen mandat att besluta om genomförandeakter i betydligt större omfattning än vad den än så länge har valt att göra. Att många genomförandeakter saknas utgör ett problem vid tillämpningen av förordningen.

I avsaknad av sådana genomförandeakter finns det dock vägledningar på både nationell och europeisk nivå som kan ge visst stöd. PTS ger ut en vägledning för betrodda tjänster i Sverige enligt eIDAS.[44] Den innehåller en beskrivning av processen för att etablera sig som tillhandahållare av kvalificerade betrodda tjänster och riktar sig främst till tillhandahållare som vill bli kvalificerade. Även andra aktörer kan använda sig av vägledningen, exempelvis icke kvalificerade tillhandahållare eller myndigheter. I vägledningen framgår att PTS anser att det, i avvaktan på att kommissionen tar fram genomförandeakter, är lämpligt att använda de standarder och specifikationer som European Committee for Standardization (CEN) och European

[43] Kommissionens genomförandeförordning (EU) 2015/806 av den 22 maj 2015 om fastställande av specifikationer för utformningen av EU-förtroendemärket för kvalificerade betrodda tjänster, kommissionens genomförandebeslut (EU) 2015/1505 av den 8 september 2015 om fastställande av tekniska minimispecifikationer och format rörande förteckningar över betrodda tjänsteleverantörer i enlighet med artikel 22.5 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden, kommissionens genomförandebeslut (EU) 2015/1506 av den 8 september 2015 om fastställande av specifikationer rörande format för avancerade elektroniska underskrifter och avancerade elektroniska stämplar i enlighet med artiklarna 27.5 och 37.5 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och kommissionens genomförandebeslut (EU) 2016/650 av den 25 april 2016 om fastställande av standarder för säkerhetsbedömning av kvalificerade anordningar för skapande av elektroniska underskrifter och stämplar enligt artiklarna 30.3 och 39.2 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden.

[44] PTS, *Vägledning för betrodda tjänster i Sverige enligt eIDAS (Utgåva 3)*, 10 juni 2020.

Telecommunications Standards Institute (ETSI) beslutat på området för betrodda tjänster eftersom kommissionen troligen kommer att hänvisa till dessa i framtida genomförandeakter. I vägledningen framgår de standarder kommissionen har pekat ut i genomförandeakter men när sådana saknas framgår i stället vilken standard eller teknisk specifikation PTS anser kan vara lämplig.

ENISA har också publicerat vägledningar som avser etablering av kvalificerade betrodda tjänster[45], tillsyn över dem[46], samt avslutande av sådana tjänster[47]. ENISA har även släppt en rapport som innehåller rekommendationer för hur kvalificerade tillhandahållare av betrodda tjänster genom diverse standarder kan leva upp till kraven i eIDAS-förordningen.[48] I rapporten hänvisas bl.a. till ETSI-specifikationer, EN-standarder[49] samt standarder från International Organization for Standardization (ISO) och International Electrotechnical Commission (IEC). I avsnitt 5.12.1 framgår mer om dessa standarder.

5.12 Standarder, tekniska lösningar och specifikationer

5.12.1 Standarder

Svenska institutet för standarder (SIS) beskriver standarder som en gemensam lösning på ett återkommande problem, vars syfte är att skapa enhetliga och transparenta rutiner.[50] Ett övergripande mål med standardisering är att samla aktörer med specialistkunskap som ser fördelar med att skapa en gemensam specifikation eller vägledning för hur t.ex. en vara, tjänst eller process ska se ut och fungera, samt testas och kontrolleras.[51] Standarder kan vara av olika natur och kan vara horisontella eller sektorsspecifika alternativt produkt- eller tjänstespecifika. De kan avse själva produkterna och tjänsterna eller organisationer som tillhandahåller dem. I det följande använder vi

[45] ENISA, *Guidelines on Initiation of Qualified Trust Services – Technical guidelines on trust services*, 19 december 2017.
[46] ENISA, *Guidelines on Supervision of Qualified Trust Services – Technical guidelines on trust services*, 19 december 2017.
[47] ENISA, *Guidelines on Termination of Qualified Trust Services*, 19 december 2017.
[48] ENISA, *Recommendations for QTSPs based on Standards – Technical guidelines on trust services*, 19 december 2017.
[49] EN-standarder (europeisk norm) är tekniska standarder som har tagits fram av något av de tre europeiska standardiseringsorganen CEN, CENELEC och ETSI.
[50] www.sis.se/standarder/vad-ar-en-standard/ (hämtad 2021-01-25).
[51] Regeringens strategi för standardisering (UD2018/12345/HI), s. 6.

begreppet standarder i vid mening som också inkluderar tekniska specifikationer, trots att det rent formellt kan finnas skillnader mellan dem.[52] Vi anser dock att standardiseringsarbete också innefattar arbete med tekniska specifikationer och liknande.

Standarder kan vara nationella, regionala eller globala. I Sverige finns tre standardiseringsorganisationer: SIS, Svensk Elstandard (SEK) och Svenska Informations- och Telekommunikationsstandardiseringen (ITS). Dessa organisationer har respektive motsvarigheter på både europeisk och global nivå. Europeiska standarder antas av CEN, European Committee for Electrotechnical Standardization (CENELEC) och ETSI.[53] Motsvarande organisationer på global nivå är ISO, IEC och Internationella teleunionen (ITU). Sammanfattningsvis verkar SIS, CEN och ISO respektive SEK, CENELEC och IEC respektive ITS, ETSI och ITU inom samma områden. Vissa standardiseringsorgan erbjuder publicerade standarder mot en kostnad och andra erbjuder dem gratis.

Det finns ett flertal standarder som kan vara relevanta för de områden som omfattas av eIDAS-förordningen. Det finns inte utrymme att i detta delbetänkande redogöra för alla dessa men som konstateras i avsnitt 5.5 kan kommissionen anta genomförandeakter som fastställer referensnummer för standarder. Av skäl 72 i förordningen framgår att när kommissionen antar delegerade akter eller genomförandeakter bör den ta vederbörlig hänsyn till de standarder och tekniska specifikationer som utarbetats av europeiska och internationella standardiseringsorgan, särskilt CEN, ETSI, ISO och ITU, i syfte att säkerställa en hög nivå av säkerhet och interoperabilitet när det gäller elektronisk identifiering och betrodda tjänster. Kommissionen har i linje med detta valt att peka på standarder från olika standardiseringsorgan. Genomförandeakterna som avser betrodda tjänster innehåller hänvisningar till ETSI-specifikationer, EN-standarder och ISO/IEC-standarder, beroende på vilken process, funktion eller liknande som avses. De EN-standarder som finns avseende betrodda tjänster är utarbetade av CEN och ETSI.

[52] www.etsi.org/standards/types-of-standards (hämtad 2021-01-30).
[53] Skäl 4 i ingressen till Europaparlamentets och rådets förordning (EU) nr 1025/2012 av den 25 oktober 2012 om europeisk standardisering och om ändring av rådets direktiv 89/686/EEG och 93/15/EEG samt av Europaparlamentets och rådets direktiv 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG och 2009/105/EG samt om upphävande av rådets beslut 87/95/EEG och Europaparlamentets och rådets beslut 1673/2006/EG.

eIDAS-förordningen är baserad på det som kallas nya metoden. Metoden innebär att det i en EU-rättsakt, t.ex. ett direktiv eller en förordning, fastställs grundläggande säkerhetskrav eller andra krav, men inte hur kraven ska uppfyllas.[54] I stället brukar olika standardiseringsorgan få mandat från kommissionen att ta fram harmoniserade standarder för det aktuella området. I slutet av 2009 beslutade kommissionen att ge CEN, CENLEC och ETSI ett standardiseringsmandat inom området informations- och kommunikationsteknologi som avser elektroniska underskrifter. Mandatets omfattning är att skapa förutsättningar för att uppnå gränsöverskridande interoperabilitet för elektroniska underskrifter, genom att definiera och tillhandahålla ett standardiserat ramverk för europeiska elektroniska underskrifter.[55] Mandatet är visserligen från 2009, dvs. innan eIDAS-förordningen fanns, men gäller fortfarande och det har i enlighet med mandatet publicerats ett antal standarder som är av relevans för betrodda tjänster. Flertalet har publicerats av ETSI, som också anordnar s.k. ”plug tests” för att testa interoperabiliteten för de standarder som avser betrodda tjänster.

Enligt den nya metoden är standarderna frivilliga[56] att följa men att följa dem är förenat med en presumtion om överenstämmelse med de krav som fastställs i det aktuella direktivet eller den aktuella förordningen.[57] Detta under förutsättning att kommissionen har offentliggjort en hänvisning till den harmoniserade standarden i Europeiska unionens officiella tidning, eller i vissa fall hänvisat till den med andra medel.[58]

Standarder tas fram gemensamt av de parter som är engagerade i ett visst standardiseringsorgan. De standardiseringsorgan som omnämns i skäl 72 i eIDAS-förordningen fungerar på lite olika sätt. ETSI är princip öppet för vem som helst att gå med i för att delta i

[54] *EU, Sverige och den inre marknaden – En översyn av horisontella bestämmelser inom varu- och tjänsteområdet* (SOU 2009:71), s. 161 f.
[55] Kommissionens standardiseringsmandat M/460 av den 22 december 2009.
[56] I vissa rättsakter, t.ex. eIDAS-förordningen, kan det dock vara obligatoriskt att följa vissa standarder, såsom de standarder som avser säkra anordningar i kommissionens genomförandebeslut (EU) 2016/650 om fastställande av standarder för säkerhetsbedömning av kvalificerade anordningar för skapande av elektroniska underskrifter och stämplar enligt artiklarna 30.3 och 39.2 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden.
[57] *EU, Sverige och den inre marknaden – En översyn av horisontella bestämmelser inom varu- och tjänsteområdet* (SOU 2009:71), s. 161 f.
[58] Artikel 10.6 i Europaparlamentets och rådets förordning (EU) nr 1025/2012.

standardiseringsarbetet. Medlemmarna i CEN består av de nationella standardiseringsorganen i EU:s medlemsstater samt Storbritannien, Republiken Nordmakedonien, Serbien, Turkiet, Island, Norge och Schweiz. För Sveriges del är det SIS som är medlem i både CEN och ISO.[59]

ITU är en mellanstatlig internationell organisation för global samordning av telenät och teletjänster.[60] Företag, branschorganisationer och sammanslutningar samt myndigheter från många av världens länder deltar i organisationens arbete. Även om ITU anges i skäl 72 har ingen av de genomförandeakter som kommissionen har antagit hittills pekat på ITU-standarder.

Det finns olika sätt att påverka innehållet i en standard när en ny standard ska tas fram, exempelvis genom medlemskap i det aktuella standardiseringsorganet eller genom medlemskap i det nationella standardiseringsorgan som i sin tur är medlem i ett europeiskt eller internationellt standardiseringsorgan. Innan en standard får status som europeisk norm (EN) ska beslut om det fattas i respektive standardiseringsorgan. I CEN är det SIS som röstar för Sveriges del om sådana beslut. I ETSI är det ITS.

Det finns många andra standardiseringsorgan utöver de som anges ovan. Standardiseringen på det digitala området utgår ofta från andra konstellationer och andra informella standardiseringsorganisationer, vilka kan vara starkt marknadsdrivna.[61] Ett tydligt exempel på detta med koppling till betrodda tjänster är utvecklingen rörande certifikat för autentisering av webbplatser (se mer om detta i avsnitt 4.6.1).

5.12.2 Tekniska lösningar och specifikationer

Utöver standarder finns det även vissa tekniska lösningar och specifikationer rörande betrodda tjänster som bör lyftas fram.

[59] www.sis.se/en/standardutveckling/internationell-standardisering/cen/ (hämtad 2021-01-21) och www.sis.se/en/standardutveckling/internationell-standardisering/iso/ (hämtad 2021-01-21).
[60] www.pts.se/sv/om-pts/omvarldslankar/internationella-organisationer/ (hämtad 2021-01-21).
[61] Regeringen, *Regeringens strategi för standardisering* (UD2018/12345/HI), s. 12.

DIGG:s fristående underskriftstjänst

DIGG rekommenderar offentliga aktörer att skaffa en fristående underskriftstjänst.[62] Hur en sådan tjänst fungerar beskrivs i avsnitt 5.2.2. Vidare rekommenderar myndigheten att aktörerna vid upphandling av en sådan tjänst ställer krav på att den ska vara granskad och godkänd av DIGG. Granskningen utgår från DIGG:s normativa specifikation för fristående underskriftstjänst. Den normativa specifikationen som helhet omfattar dokumenten

- Normativ specifikation – Fristående underskriftstjänst.
- Policy – Fristående underskriftstjänst.
- Tjänstespecifikation – Fristående underskriftstjänst.
- Icke funktionella krav – Fristående underskriftstjänst.[63]

Enligt tjänstespecifikationen ska underskriftstjänsten stödja underskrift enligt vissa utpekade format och tekniska specifikationer.[64]

Byggblock inom CEF Digital

Sedan den 1 januari 2014 gäller Europaparlamentets och rådets förordning (EU) nr 1316/2013 av den 11 december 2013 om inrättande av Fonden för ett sammanlänkat Europa. Fonden inrättades på initiativ av Europeiska kommissionen och dess syfte är att främja projekt av gemensamt intresse inom sektorerna för transport-, telekommunikations- och energi.[65] Fonden benämns vanligtvis som CEF, en förkortning som följer av dess engelska namn (Connecting Europe Facility). En del av fondens program är CEF Digital som arbetar för att möjliggöra en digital inre marknad. CEF Digital har ett antal centrala byggblock som tillsammans utgör basen för att uppnå en sådan marknad. Byggblocken kan bestå av ett ramverk, en standard, mjukvara, mjukvara som en tjänst eller en kombination av dessa.[66] Bygg-

[62] www.digg.se/digital-identitet/e-underskrift/offentlig-aktor (hämtad 2021-01-13).
[63] DIGG, *Normativ specifikation – Fristående Underskriftstjänst* (version 1.40), 22 april 2020.
[64] XML Advanced Electronic Signatures(XAdES) BES i enlighet med ETSI EN 319 132 samt PDF Advanced Electronic Signatures (PAdES) enlighet med ETSI EN 319 142 (Normativ specifikation fristående underskrifts tjänst – Tjänstespecifikation, s. 15).
[65] Artikel 1 i Europaparlamentets och rådet förordning (EU) nr 1316/2013.
[66] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/CEF+Digital+Home (hämtad 2021-01-13).

blocken finns inom en rad områden, exempelvis elektroniskt informationsutbyte (eDelivery), elektroniska underskrifter (eSignature) och elektronisk identifiering (eID).

eDelivery är baserat på en distribuerad modell som innebär att deltagarna blir en nod i ett nätverk genom att använda standardiserade protokoll och säkerhetsrutiner. eDelivery möjliggör kommunikation direkt mellan deltagare utan behov att sätta upp bilaterala kanaler.[67] Byggblocket togs fram med koppling till eIDAS-förordningens elektroniska tjänster för rekommenderade leveranser för att visa hur författningen är tänkt att fungera och för att publicera öppen programvara som alla kan använda.[68] Exempel på användningsområden så här långt är i viss mån e-CODEX[69], som är ett system för utbyte av rättslig information inom EU, och i dess helhet PEPPOL[70], som är ett internationellt nätverk för elektroniska inköp. Ett annat exempel på dess användning inom Sverige är projektet SDK som beskrivs i avsnitt 4.5.2.

Byggblocket eSignature möjliggör exempelvis skapande och validering av elektroniska underskrifter. En komponent i byggblocket är Digital Signature Services (DSS). DSS är en öppen källkodsbaserad lösning som kan användas för att skapa och validera elektroniska underskrifter. DSS använder aktuella ETSI-specifikationer och blir på så sätt en referensimplementering av dessa standarder.

Förteckningar som tillhandahålls av privata aktörer

Det finns ett antal företag, som erbjuder diverse tekniska lösningar, som har egna förteckningar över tillhandahållare. Dessa förteckningar påminner i många avseenden om de förteckningar som EU:s medlemsstater ska tillhandahålla (se mer om sådana förteckningar i avsnitt 5.8). Exempelvis tillhandahåller de amerikanska företagen Adobe och Microsoft förteckningarna Adobe Approved Trust List[71] respektive Trusted root program[72]. Förteckningar av detta slag används t.ex. av mjukvaror som läser PDF-filer eller av webbläsare. För att komma

[67] DIGG m.fl., *Säkert och effektivt elektroniskt informationsutbyte inom den offentliga sektorn*, DIGG, (DIGG dnr 2019-100), s. 54.
[68] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EU+Legislation (hämtad 2021-01-13).
[69] e-Justice Communication via Online Data Exchange.
[70] Pan-European Public Procurement On-Line.
[71] https://helpx.adobe.com/se/acrobat/kb/approved-trust-list2.html (hämtad 2021-01-13).
[72] https://docs.microsoft.com/sv-se/security/trusted-root/participants-list (hämtad 2021-01-13).

med i dessa förteckningar måste tillhandahållarna vanligen leva upp till vissa krav, bl.a. tekniska. För en förlitande part som använder t.ex. en webbläsare eller en PDF-läsare som nyttjar dessa förteckningar är det svårt att veta om det finns fog att lita på dessa certifikat.

Mer om dessa förteckningar som tillhandahålls av privata aktörer och de potentiella informationssäkerhetsrisker som är förenade med användning av dem finns i avsnitt 9.2.8.

6 Behov och utmaningar vid användning av betrodda tjänster i den offentliga förvaltningen

6.1 Drivkrafterna bakom det ökade behovet av betrodda tjänster i den offentliga förvaltningen

Samhället har under lång tid blivit alltmer digitaliserat. Denna utveckling har samtidigt även skett i varierande takt i den offentliga förvaltningen. Det av riksdagen för snart tio år sedan beslutade målet att Sverige ska vara bäst i världen på att använda digitaliseringens möjligheter gäller alltjämt.[1] Digitaliseringen är givetvis den starkaste drivkraften bakom användningen av betrodda tjänster. Som framgår av utredningens direktiv utgör betrodda tjänster samhällskritisk infrastruktur och är en förutsättning för fortsatt utveckling av digital offentlig service till privatpersoner och företag.[2] Exempelvis är elektroniska underskrifter som går att lita på och som är enkla att använda grundläggande i ett alltmer digitaliserat samhälle.

Vårt kartläggningsarbete har även visat att det finns en tydlig uppfattning inom den offentliga förvaltningen att behovet av att kunna använda betrodda tjänster enbart kommer att öka. Detta beror delvis på att alltfler processer och arbetsmoment digitaliseras, delvis på att allmänhetens förväntan om att genomföra sina ärenden digitalt ökar. Det förekommer även författningsbestämmelser som uppställer krav om användning av vissa betrodda tjänster.[3]

---

[1] Prop. 2011/12:1, utg. omr. 22, bet. 2011/12:TU1, rskr. 2011/12:87.
[2] Dir. 2020:27.
[3] Exempel på lagkrav är artikel 1.7 i Europaparlamentets och rådets direktiv (EU) 2019/1151 av den 20 juni 2019 om ändring av direktiv (EU) 2017/1132 vad gäller användningen av digitala verktyg och förfaranden inom bolagsrätt. Genom artikeln införs en ny artikel i det gamla direktivet, artikel 16a, där det i fjärde punkten föreskrivs att medlemsstaterna ska säkerställa

Den i skrivande stund pågående pandemin har även accelererat den offentliga förvaltningens digitaliseringstakt.[4] I Internetstiftelsens undersökning Svenskarna och internet 2020 konstateras att utvecklingen för användning av olika digitala tjänster samt förändringar i svenskarnas beteende på nätet i stora drag följer en tidigare trend, men att trenden har i många fall påskyndats under pandemin.[5] Vi delar denna bild. Många av de offentliga aktörer vi varit i kontakt med har uppgett att de bl.a. behövt ställa om sina arbetssätt till följd av ett allt större behov av att kunna genomföra vissa arbetsuppgifter på distans. Ett återkommande exempel har varit möjligheten att kunna skriva under interna dokument eller beslut elektroniskt. Pandemin har emellertid inte bara lett till rent interna förändringar hos förvaltningens aktörer. Den har också lett till ett tryck utifrån om att utveckla verksamheterna. Förfaranden eller verksamheter med mänskliga möten har i många fall bytts ut mot digitala alternativ. Vissa aktörer har dessutom fått skapa helt nya e-tjänster till följd av pandemin. Användningen av betrodda tjänster har varit en viktig komponent som bidragit till den omställning som förvaltningen behövt göra.

6.2 Kartläggning av behov och utmaningar vid användning av betrodda tjänster

Utredningens uppdrag har delvis varit att genomföra en kartläggning av den offentliga förvaltningens behov av åtgärder för ökad och standardiserad användning av betrodda tjänster. En närmare beskrivning av hur kartläggningen genomförts framgår av avsnitt 2.2. Det har inom ramen för kartläggningen inte varit möjligt att identifiera behov och utmaningar som varje enskild aktör inom förvaltningen har eller upplever. Kartläggningen har emellertid enligt vår bedömning visat på tillräckligt många gemensamma nämnare mellan olika aktörers behov och utmaningar att de får anses relevanta för den offentliga förvaltningen i stort.

Nedan presenteras resultatet av kartläggningen i form av en redogörelse för utmaningar som aktörer inom förvaltningen upplever med

att elektroniska kopior och utdrag ur handlingar och information från registret har autentiserats genom betrodda tjänster enligt eIDAS-förordningen.

[4] Se t.ex. PTS, *Digital omställning till följd av covid-19 (PTS-ER-2021:1)*, för exempel på digital omställning inom utbildningssektorn samt vård- och omsorgssektorn till följd av pandemin.

[5] Internetstiftelsen, *Svenskarna och internet 2020*, s. 5.

koppling till användning av betrodda tjänster samt de behov vi har identifierat att aktörerna har. Redogörelsen är, efter den inledande sammanfattningen, uppdelad utifrån olika betrodda tjänster samt med ett avslutande avsnitt om standardiseringsarbete.

6.3 Sammanfattad behovsbild

Vår kartläggning visar att den offentliga förvaltningen i dagsläget upplever störst behov av att på olika sätt kunna använda och hantera elektroniska underskrifter. När det gäller elektroniska tidsstämplingar, certifikat för autentisering av webbplatser och elektroniska tjänster för rekommenderadeleveranser har kartläggningen inte visat att förvaltningen upplever något behov av åtgärder avseende dessa specifika betrodda tjänster.

Många aktörer upplever osäkerhet kring vissa eller alla steg i hanteringen av elektroniska underskrifter. Det kan gälla allt från bedömningen av om underskrifter krävs till bevarandet av elektroniska underskrifter. Vi bedömer att det finns ett stort behov av ett mer samlat och utvecklat stöd för förvaltningen att tillgå för dessa frågor.

Vidare visar kartläggningen att det finns ett behov av stöd som gör det enklare att kunna validera elektroniska underskrifter, framför allt sådana som lämnas in till den offentliga förvaltningen. Det har framkommit att vissa upplever en osäkerhet kring om en betrodd tjänst som har skapat en underskrift, eller tillhandahållaren av tjänsten, lever upp till de krav som ställs i eIDAS-förordningen.

Många elektroniska underskrifter i den offentliga förvaltningen genereras inom ramen för aktörernas e-tjänster. Vissa tillhandahållare av betrodda tjänster har framfört att deras kunder i och med detta upplever hinder mot att kunna använda andra elektroniska underskrifter än de som skapas i e-tjänsterna. I tjänsterna är det vidare vanligt att autentisering genom elektronisk identifiering är ett krav. Att det inte är möjligt för alla att få tillgång till, eller kunna använda, elektronisk identifiering har av många aktörer framförts som ett problem.

Elektroniska stämplar används än så länge i begränsad omfattning i förvaltningen. Eftersom flera aktörer har framfört att de ser ett behov av att i framtiden kunna använda stämplar finns det dock ett behov av stöd i användningen av dessa tjänster. Behoven är enligt vår bedömning likartade som för elektroniska underskrifter men stödet

kan behöva anpassas, bl.a. mot bakgrund av att användningsfallen kan skilja sig åt.

Med beaktande av att standarder har en betydande påverkan på området betrodda tjänster finns även ett behov av att myndigheter deltar i standardiseringsarbetet i större utsträckning än i dagsläget.

6.4 Den offentliga förvaltningen ser inget tydligt behov av att använda vissa betrodda tjänster

Kartläggningsarbetet har visat att aktörer inom den offentliga förvaltningen inte ser något tydligt behov av vissa betrodda tjänster. Det innebär inte att förvaltningen inte kan ha användning för dessa tjänster. Varken vi eller de vi haft kontakt med har emellertid identifierat potentiella användningsområden där dessa tjänster i dagsläget hade kunnat skapa nytta. Vi ser inte heller att det finns behov av att föreslå åtgärder avseende dessa specifika betrodda tjänster. Nedan beskrivs kortfattat behovsbilden avseende dessa tjänster.

Elektroniska tidsstämplingar

Elektroniska tidsangivelser skapas ofta inom den offentliga förvaltningen, t.ex. när en handling inkommer elektroniskt. Vi har genom kartläggningsarbetet emellertid inte identifierat ett behov av att kunna använda betrodda tjänster för elektroniska tidsstämplingar inom förvaltningen. Det kan finnas ett behov av att kunna tidsstämpla med sådana tjänster men det verkar vara inom ramen för andra funktioner, exempelvis när elektroniska underskrifter eller stämplar används. Det är för övrigt för bl.a. underskrifter och stämplar som tidsstämplingstjänster enligt eIDAS-förordningen används, vilket innebär att en tredje part lägger till en tidsuppgift som är kryptografiskt skyddad med en egen underskrift eller stämpel.

Certifikat för autentisering av webbplatser

En stor majoritet av aktörerna inom offentlig förvaltning använder certifikat för autentisering av sina webbplatser. Vår bedömning är att aktörerna upplever nuvarande marknad som välfungerande och att

deras behov tillgodoses. Det bör påpekas att nuvarande marknad och de certifikat som används inte nödvändigtvis är utformade efter eIDAS-förordningens krav. För vissa typer av gränsöverskridande informationsutbyten krävs emellertid kvalificerade certifikat som lever upp till kraven i förordningen. Vi har dock bara identifierat ett fall när ett sådant certifikat har krävts (se mer om detta i avsnitt 4.7).

Med hänsyn till att kommissionen själva och även via ENISA arbetar för att främja användningen av certifikat för autentisering av webbplatser samt att krav på användning av sådana certifikat har börjat dyka upp i EU-rättsakter kan behovet på sikt bli större. Vidare kommer sannolikt användningen att öka som en följd av ett ökat utbyte av information mellan nationella myndigheter inom EU.

Elektroniska tjänster för rekommenderade leveranser

Definitionen av elektroniska tjänster för rekommenderade leveranser i eIDAS-förordningen är enligt vår bedömning så pass bred att den kan fånga upp tjänster som möjliggör elektronisk kommunikation inom den offentliga förvaltningen och mellan förvaltningen och externa aktörer. De uppgifter som överförs ska emellertid enligt definitionen i artikel 3.36 i förordningen vara mellan tredje män, vilket innebär att exempelvis en e-tjänst som en myndighet erbjuder för att skicka in uppgifter till den myndigheten inte omfattas. Utifrån vårt kartläggningsarbete kan vi även konstatera att termen elektronisk tjänst för rekommenderad leverans inte är välkänd inom förvaltningen. De offentliga aktörerna har behov av att kunna skicka och ta emot uppgifter elektroniskt, men de har inte framfört att de behöver tjänster som utformas på ett sätt som medför att de utgör elektroniska tjänster för rekommenderade leveranser enligt eIDAS-förordningens definition.

6.5 Behov avseende elektroniska underskrifter

Av vårt kartläggningsarbete framkommer att den kategori betrodda tjänster som den offentliga förvaltningen anser sig ha störst behov av är tjänster med koppling till elektroniska underskrifter. Behovet av att kunna använda elektroniska underskrifter väntas dessutom öka, både för inkommande handlingar och för interna processer.

Användningen av elektroniska underskrifter får emellertid redan i dag anses utbredd inom förvaltningen. Omfattningen varierar dock mellan olika sektorer och aktörer.

6.5.1 Osäkerhet rörande om elektroniska underskrifter ska eller får användas

Vi kan konstatera att aktörer inom den offentliga förvaltningen upplever att användning av elektroniska underskrifter är förenat med ett flertal utmaningar. Till att börja med är det emellertid viktigt att lyfta fram att kartläggningen visar att det finns en uppfattning inom den offentliga förvaltningen att autentisering genom elektronisk identifikation i många fall kan räcka och att en elektronisk underskrift då inte behövs. Vår uppfattning är att det i första hand är verksamheterna som bäst kan bedöma sina behov och om de gör den bedömningen att autentisering räcker, finns det som vi ser det ingen anledning att komplettera det aktuella förfarandet med en underskrift.

Ett tydligt hinder mot att kunna använda elektroniska underskrifter är av naturliga skäl bestämmelser i författningar som inte tillåter att sådana används (se mer om detta i avsnitt 8.9.1). Genom kartläggningsarbetet har vi endast identifierat ett fåtal sådana bestämmelser (se mer om detta i avsnitt 8.9.5). Trots att kraven på underskrift genom penna på papper i svenska författningar är få bedömer vi att det råder en osäkerhet kring när elektroniska underskrifter får användas. Att göra den bedömningen upplever vissa som en utmaning. Dessutom har det framförts en osäkerhet avseende hur man ska leva upp till olika författningskrav när elektroniska underskrifter uttryckligen får eller ska användas. Detta avser framför allt avancerade elektroniska underskrifter, för vilka detaljregleringen är mindre omfattande än för kvalificerade.

Kartläggningen visar också att det kan råda oklarhet om en handling behöver skrivas under över huvud taget. Denna osäkerhet beskrevs även som tidigare nämnts i avsnitt 4.2.1 av Digitaliseringsrättsutredningen, som även framhöll att närmast rutinmässiga krav på undertecknande vid pappersförfaranden i vissa fall synes ha uppställts av myndigheter utan att det funnits krav i lag eller förordning som anger att det behövs.[6] Vi instämmer i det, men kan också kon-

[6] *Juridik som stöd för förvaltningens digitalisering* (SOU 2018:25), s. 79 och 461.

statera att många aktörer inom förvaltningen reflekterar över om underskrifter faktiskt behövs, eftersom en övergång från pappershantering till digital hantering inte nödvändigtvis måste innebära att ett krav på underskrift bibehålls.

Ytterligare en utmaning som vissa aktörer i förvaltningen har beskrivit är att andra aktörer inom offentlig förvaltning som de kommunicerar med inte alltid accepterar elektroniska underskrifter, vilket försvårar en övergång till helt digital hantering.

6.5.2 Oklara krav och komplexitet

När offentliga aktörer ska införa elektroniska underskrifter i sin verksamhet sker det vanligtvis genom att tjänsterna upphandlas eller avropas. Att införa underskrifter i verksamheten upplevs som komplext vilket också gör det svårt att ställa rätt krav på tillhandahållarna. Flera aktörer menar vidare att det finns många lösningar för elektroniska underskrifter att välja mellan och att det är en utmaning att välja en lämplig lösning. Det kompliceras ytterligare av att många känner sig osäkra på om de underskrifter som skapas lever upp till eIDAS-förordningens krav på främst avancerade elektroniska underskrifter. Att göra den bedömningen upplevs av flera aktörer inom förvaltningen som svårt och ett flertal anser att någon form av bedömning av tredje part hade underlättat detta.

Kartläggningen visar vidare att för det fåtal aktörer som har berättat att de har övervägt att införa kvalificerade elektroniska underskrifter har det inte varit en framkomlig väg, främst mot bakgrund av bristande utbud vid upphandlingstillfället.

Svårt att bedöma underskrifter från externa aktörer

Utmaningarna kopplade till underskrifter som kommer från externa aktörer är delvis desamma som för skapandet av egna underskrifter. Vissa aktörer har uppfattat det som att det finns oklarheter när en underskriftstjänst ska införas inom ramen för en e-tjänst. Även här kan det röra sig om svårigheter att bedöma om den underskrift som skapas är en avancerad elektronisk underskrift, om den bedömningen inte redan är gjord.

Att bedöma om en underskrift är avancerad upplevs också av många som ett problem när externa aktörer inkommer med elektroniskt undertecknade handlingar. Det kan exempelvis påstås att en elektronisk underskrift är avancerad, men flera aktörer inom förvaltningen har påtalat att det är svårt att kontrollera att så verkligen är fallet. En annan utmaning för verksamheterna kan vara att de helt enkelt inte har processer eller it-stöd på plats för att kunna hantera underskrifter som inkommer på det sättet.

Ett behov som har framkommit under kartläggningen är möjligheten att kunna koppla en viss person och personens elektroniska underskrift till en viss behörighet. Att kunna göra den kopplingen kan i vissa fall vara en förutsättning för en fullt ut digital hantering av ärenden.

Aktörer inom förvaltningen har också berättat att det ibland inkommer handlingar där det är tveksamt om de är försedda med elektroniska underskrifter som går att knyta till en fysisk person på det sätt som krävs. Handlingarna verkar i stället snarare vara stämplade av en juridisk person samt kompletterad med information om att fysiska personer har skrivit under. Detta förfaringssätt har väckt frågan om krav på att något ska skrivas under med avancerad elektronisk underskrift då kan anses uppfyllt.

Vissa tillhandahållare av betrodda tjänster har framfört att de upplever att deras kunder utestängs från att lämna in elektroniskt undertecknade handlingar till vissa myndigheter. Detta då många elektroniska underskrifter i förvaltningen genereras inom ramen för myndigheters e-tjänster och att de som har sådana tjänster kan vara ovilliga att godta inlämnande av elektroniskt undertecknade handlingar på annat sätt.

6.5.3 Bristande tillgång till elektronisk identifiering

Flera aktörer har beskrivit utmaningar och hinder kopplade till tillgången till elektronisk identifiering, som påverkar möjligheterna att använda elektroniska underskrifter. Det är vanligt att autentisering med e-legitimation är första steget i en process där något ska skrivas under elektroniskt. Något som också bekräftas av inkomna svar på

en enkät genomförd av Föreningen XBRL Sweden.[7] Vår kartläggning visar också att eftersom inte alla i Sverige har möjlighet att anskaffa en vanligt accepterad e-legitimation eller är helt utestängda från att skaffa e-legitimation, stängs vissa personer ute från att kunna använda e-tjänster där det först krävs autentisering via e-legitimation.[8] Samma sak kan gälla anskaffande av vanligt accepterade underskriftscertifikat. Det kan i sin tur leda till ett krångligare förfarande för den enskilde, men också till mer manuell hantering hos den offentliga aktören.

6.5.4 Svårigheter med validering

Kartläggningsarbetet visar att förvaltningen upplever utmaningar att validera underskrifter som inkommer från externa parter. De kan delvis kopplas till utmaningen att avgöra om det rör sig om en avancerad elektronisk underskrift eller inte, men det verkar även råda osäkerhet kring vad det är som ska valideras, dvs. vilka uppgifter som ska valideras. Det framstår även som osäkert för många vilka underskrifter samt tillhandahållare av betrodda tjänster som de kan lita på.

Tillgång till it-stöd är en utmaning och det har framförts att det inte är effektivt att varje enskild aktör inom den offentliga förvaltningen själv ska behöva göra dessa bedömningar samt införskaffa tjänster för validering. Många aktörer inom förvaltningen har uttalat att de ser ett stort behov av stöd avseende validering av elektroniska underskrifter. Det kan röra sig om tekniskt stöd eller stöd i form av exempelvis förteckningar över tillhandahållare och tjänster som det går att lita på.

Vi kan för övrigt i anslutning till detta konstatera att det verkar vara mycket ovanligt att underskrifter på papper som inkommer till offentliga aktörer kontrolleras. Med rätt förutsättningar är det lättare att kontrollera elektroniska underskrifter än underskrifter på papper.

[7] Av sammanställningen av inkomna svar framgår att underskriftstjänster ofta tillämpar underskrift med stöd av legitimering. Sammanställningen finns att hämta på XBRL Swedens webbplats: www.xbrl.se/nyheter/resultat-av-enkat-till-leverantorer-av-losningar-for-digital-signering/ (hämtad 2021-01-26).
[8] Se t.ex. SKR, *Rapport enkät e-legitimationer – 2019 kommuner och regioner*, s. 19.

6.5.5 Problem avseende vad som ska bevaras och hur det ska bevaras

Avsaknad av elektroniska arkiv försvårar givetvis bevarandet av och, i vissa fall, ett eventuellt införande av elektroniska underskrifter. För att kunna hantera elektroniska underskrifter krävs dessutom ofta en översyn av verksamhetens dokumenthantering i stort. Flera av de aktörer vi har talat med har lyft att de ser utmaningar med att bevara elektroniska underskrifter. En bild som också bekräftas av E-legitimationsenkäten från 2019.[9] Utmaningarna med bevarandet kan dels kopplas till svårigheter med att avgöra vad som ska bevaras och hur länge, dels hur bevarandet av elektroniska underskrifters giltighet över tid ska ske (se mer om dessa frågeställningar i avsnitt 8.5).

6.5.6 Avsaknad av stöd

Flera aktörer inom den offentliga förvaltningen har lyft att det kan vara komplext och resurskrävande att införa elektroniska underskrifter i verksamheten. Både när det gäller underskrifter som endast har ett internt syfte och när det gäller underskrifter som tillfogas handlingar som är avsedda för, eller lämnas in av, externa aktörer. Det stora informationsbehovet avseende tjänster för elektroniska underskrifter framgår också av E-legitimationsenkäten, där drygt 40 procent av de svarande angav att de har behov av mer information inom detta område.[10] Olika överväganden behöver göras och det stöd som finns att tillgå i dag ger inte alltid svar på de frågor som måste besvaras. Flera aktörer har framfört att det är svårt att veta var man ska börja för att ta sig an ett införande. Det finns ett tydligt behov av att få stöd genom hela kedjan av att införa underskriftshantering. Detta gäller i synnerhet mindre aktörer. Kompetensen kan också behöva höjas inom organisationen för att ta sig an området på ett tillfredsställande sätt. Att få stöd i kompetenshöjande åtgärder skulle underlätta för vissa aktörer.

Ett särskilt område där vi identifierat ett behov rör eIDAS-förordningen som sådan. Vi har kunnat se att kännedomen och kunskapen om förordningen varierar stort. Det finns därtill flera exempel på att det i myndighetsföreskrifter förekommer obsoleta hänvisningar

[9] DIGG, *E-legitimering inom den offentliga förvaltningen – Enkätundersökning 2019*, s. 25.
[10] A.a. s. 24.

till den upphävda lagen (2000:832) om kvalificerade elektroniska signaturer eller e-nämndens grundläggande vägledning för myndigheternas användning av e-legitimationer och elektroniska underskrifter (e-nämnden 04:02) från 2004. Även bland dem som känner till förordningen och dess bestämmelser råder osäkerhet rörande vilka krav som förordningen ställer på aktörer i den offentliga förvaltningen (se mer om detta i avsnitt 5.10).

6.6 Behov avseende elektroniska stämplar

Elektroniska stämplar är juridiska personers motsvarighet till elektroniska underskrifter. Stämplar kan därför med fördel användas av myndigheter, kommuner och regioner när det behövs en utställarverifikation och det inte är nödvändigt att en enskild handläggare undertecknar en viss handling.

Eftersom användningen av stämplar, utifrån det vår kartläggning visat, är begränsad inom förvaltningen är erfarenheterna av att använda dem än så länge likaledes begränsade. Ett flertal aktörer inom förvaltningen har emellertid framfört att det finns många situationer då stämplar är att föredra framför användning av underskrifter. Ett behov av, eller snarare en önskan om, att i större utsträckning kunna använda elektroniska stämplar finns alltså.

6.7 Behov av att påverka standardiseringsarbetet

Som framkommer i avsnitt 5.12.1 används i många fall olika tekniska standarder inom området betrodda tjänster. Kopplat till det ökade behovet av att använda betrodda tjänster visar kartläggningen att det finns ett behov av att från myndighetshåll kunna påverka arbetet med att ta fram eller revidera relevanta standarder i större utsträckning än vad som sker i dag.

7 Utrymmet för nationell reglering av betrodda tjänster

7.1 Behovet av att utreda utrymmet för nationell reglering av betrodda tjänster

Utredningen om effektiv styrning av nationella digitala tjänster föreslog att regeringen skulle tillsätta en utredning som ser över behovet av svensk reglering av betrodda tjänster som är icke kvalificerade.[1] Utredningen ansåg att om en nationell säkerhetsnivå fastställs i regelverk underlättar det såväl möjligheten att avgöra vilka underskrifter som godtas i offentliga e-tjänster nationellt som vilka tjänster som kan godtas internationellt.[2] Utredningen gjorde ingen bedömning om huruvida en sådan reglering var möjlig att införa i nationell rätt. Vi delar uppfattningen att en nationell reglering hade varit ett sätt att tillgodose vissa av den offentliga förvaltningens behov rörande användning av betrodda tjänster. Vi ser därför anledning att utreda vilket utrymme det finns för nationell reglering rörande icke kvalificerade tillhandahållare och betrodda tjänster.

7.2 EU-rätten och förhållandet till nationell lagstiftning

Sverige är som medlemsstat i EU bunden av det EU-rättsliga regelverket. Regelverket delas in i det som kallas primärrätten, som utgörs av EU:s fördrag, och sekundärrätten, som utgörs av andra rättsakter såsom direktiv och förordningar. En av flera grundläggande principer som medlemsstaterna ska följa är den s.k. lojalitetsplikten. Den

[1] *reboot – omstart för den digitala förvaltningen* (SOU 2017:114), s. 385 ff.
[2] A.a. 387.

innebär att medlemsstaterna ska vidta alla lämpliga åtgärder för att säkerställa att de skyldigheter som följer av fördragen eller av unionens institutioners akter fullgörs.[3] Det EU har bestämt är medlemsstaterna således skyldiga att följa. Det är emellertid inte ovanligt att enskilda bestämmelser i direktiv eller förordning lämnar utrymme för tolkning. I samband med ett genomförande av ett direktiv i svensk rätt kan det således vara nödvändigt för lagstiftaren att ibland göra en tolkning av en viss bestämmelse. Ytterst är det dock EU-domstolen som tolkar EU-rätten. Vidare har kommissionen i uppgift att övervaka och säkerställa tillämpningen av EU-rätten. Kommissionen har även möjlighet att initiera överträdelseärenden mot enskilda medlemsstater.

EU-förordningar är direkt tillämpliga i medlemsstaterna och ska, till skillnad från direktiv, inte implementeras i nationell lagstiftning. Påverkan på nationell rätt kan däremot bli aktuell om befintliga bestämmelser kan anses strida mot en förordning, om en förordning föreskriver en skyldighet eller möjlighet att vidta lagstiftningsåtgärder eller om det behövs andra åtgärder till stöd för förordningens syfte. Det kan alltså i vissa fall vara nödvändigt att komplettera en EU-förordning med nationella bestämmelser. Sådana bestämmelser får emellertid inte ändra eller gå emot vad som föreskrivs i den aktuella förordningen.

7.3 Betrodda tjänster är reglerade på EU-nivå

eIDAS-förordningens bestämmelser om betrodda tjänster och tillhandahållare av betrodda tjänster innebär att utrymmet för Sverige och andra medlemsstater att vidta olika typer av åtgärder på området är begränsat. Förordningen ger emellertid uttryckligen medlemsstaterna möjlighet att vidta vissa åtgärder och några av förordningens bestämmelser hänvisar till nationell rätt. Formkrav i nationell rätt faller exempelvis enligt artikel 2.3 utanför förordningens tillämpningsområde och av artikel 17.5 följer att medlemsstaterna får kräva att tillsynsorganet ska inrätta, underhålla och uppdatera en infrastruktur för betrodda tjänster, i enlighet med villkoren i nationell rätt. Vidare framgår av artikel 24.1 att när kvalificerade tillhandahållare av betrodda tjänster utfärdar ett kvalificerat certifikat, ska de kontrollera

[3] Artikel 4.3 i fördraget om Europeiska unionen.

identiteten och i förekommande fall eventuella särskilda attribut för den fysiska eller juridiska person till vilken det kvalificerade certifikatet utfärdas. Det ska enligt artikeln göras på lämpligt sätt och i enlighet med nationell rätt.

Hänvisningarna till nationell rätt påverkar inte det faktum att tjänsterna och tillhandahållarna är reglerade genom förordningen. Däremot finns det i vissa fall alltså uttryckligt utrymme för medlemsstaterna att vidta nationella åtgärder.

7.4 Tidigare bedömningar om kompletterande bestämmelser till eIDAS-förordningen

Av 2 § förordningen (2016:576) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering framgår bl.a. att PTS får meddela föreskrifter om krav för ackreditering av organ för bedömning av överensstämmelse, hur bedömningar av överensstämmelse ska göras samt rapportering av bedömningar av överensstämmelse. Detta är sådant som kommissionen enligt artikel 20.4 i eIDAS-förordningen får anta genomförandeakter om. I förarbetena till lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering konstateras att det inte är obligatoriskt för kommissionen att anta de aktuella genomförandeakterna och att det var oklart huruvida sådana akter skulle finnas på plats när eIDAS-förordningen skulle börja tillämpas.[4] Det konstaterades vidare att i den mån det då saknas EU-rättslig reglering måste det införas nationell reglering i stället samt att det kan finnas behov av nationell reglering även om kommissionen utnyttjar möjligheten att anta genomförandeakter, t.ex. i form av kompletterande bestämmelser till genomförandeakterna eller närmare föreskrifter i vissa avseenden som inte omfattas av genomförandeakter. Det tydliggjordes emellertid att det är viktigt att de föreskrifter som kan komma att behövas i så stor utsträckning som möjligt tar hänsyn till internationellt standardiseringsarbete för att inte harmoniseringssträvandet ska äventyras.[5] PTS har i dagsläget inte använt möjligheten att utfärda föreskrifter på området.

[a] Prop. 2015/16:72 s. 45.
[5] A.a.

7.5 Kan medlemsstaterna vidta nationella åtgärder avseende betrodda tjänster?

Utredningens bedömning: Utrymmet för medlemsstaterna att införa nationella bestämmelser avseende de betrodda tjänster som inte är fullständigt harmoniserade är mycket begränsat och eventuella nationella bestämmelser får inte äventyra varken strävandet efter harmonisering inom området eller den fria rörligheten.

Skälen för utredningens bedömning

Syftet med eIDAS-förordningen är att säkerställa en väl fungerande inre marknad samt uppnå en lämplig säkerhetsnivå för medel för elektronisk identifiering och betrodda tjänster. I artikel 1 anges att förordningen fastställer regler för betrodda tjänster, i synnerhet för elektroniska transaktioner. Enligt skäl 21 i ingressen bör genom förordningen ett allmänt regelverk för användningen av betrodda tjänster upprättas. Av samma skäl framgår att någon allmän skyldighet att använda sådana tjänster eller att installera en accesspunkt för alla befintliga betrodda tjänster dock inte bör skapas genom förordningen. Enligt skäl 24 får medlemsstaterna behålla eller införa nationella bestämmelser, i överensstämmelse med unionsrätten, avseende betrodda tjänster så länge dessa tjänster inte har harmoniserats fullständigt genom förordningen. Det är enligt vår bedömning inte uppenbart hur skäl 24 ska tolkas. En rimlig tolkning är dock att förordningen harmoniserar vissa tjänster fullständigt, medan andra inte är fullständigt harmoniserade. Det skulle i sin tur innebära att det finns utrymme för medlemsstaterna att införa nationella bestämmelser avseende de tjänster som inte är fullständigt harmoniserade.

Vilka tjänster som harmoniseras fullständigt genom förordningen är inte i alla delar tydligt. Ett flertal tjänster faller inom kategorin betrodda tjänster och nivån av detaljreglering i eIDAS-förordningen skiljer sig åt. Genomgående ställer förordningen fler och mer detaljerade krav på tjänster som är kvalificerade, detsamma gäller tillhandahållare som är kvalificerade. Det kan tolkas som att de tjänster som är fullständigt harmoniserade är de kvalificerade tjänster som om-

fattas av förordningen.[6] Det skulle i sin tur innebära att det finns ett omfattande utrymme för medlemsstaterna att, i enlighet med skäl 24, införa nationella bestämmelser avseende betrodda tjänster som är icke kvalificerade så länge bestämmelserna överensstämmer med unionsrätten. En sådan tolkning kan dock enligt vår mening inte anses förenlig med förordningens syfte och struktur. I förordningen särskiljs mellan olika tjänster och tillhandahållare. Icke kvalificerade tjänster och tillhandahållare ska inte omfattas av krav i lika stor utsträckning som kvalificerade. Syftet med förordningen kan enligt vår mening inte vara att det oreglerade tomrum som uppstår mellan exempelvis kvalificerade och icke kvalificerade tillhandahållare ska kompenseras med nationell reglering i varje medlemsstat. Risken skulle då vara stor att det uppstår en marknad för icke kvalificerade betrodda tjänster i varje medlemsstat i stället för en gemensam inre marknad för dessa tjänster. Något som hade varit i strid med förordningens övergripande syfte.

En central unionsrättslig princip som även måste beaktas är principen om fri rörlighet, som artikel 4 i förordningen ger uttryck för. Innebörden av artikel 4.1 är att en tillhandahållare av betrodda tjänster som är etablerad i en annan medlemsstat inte får begränsas att tillhandahålla tjänster i en annan medlemsstat, förutsatt att tillhandahållandet faller inom ramen för det som regleras av förordningen. Vidare framgår av artikel 4.2 att produkter och betrodda tjänster som överensstämmer med förordningen ska omfattas av fri rörlighet på den inre marknaden. I linje med resonemanget ovan är vår uppfattning att syftet med förordningen är att även icke kvalificerade tillhandahållare av betrodda tjänster ska kunna erbjuda tjänsterna på hela den inre marknaden.

Även med beaktande av det som anförts ovan går det inte att bortse från att skäl 24 medger ett utrymme för medlemsstaterna att införa nationella bestämmelser avseende de betrodda tjänster som inte har harmoniserats fullständigt. Utrymmet är enligt vår bedömning dock mycket begränsat och vi anser, i likhet med vad som framfördes i förarbetena till lagen med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering, att eventuella nationella

[6] Det kan här noteras att enligt skäl 25 kan medlemsstaterna bestämma att andra typer av betrodda tjänster än de som ingår i förordningens förteckning över betrodda tjänster är erkända som kvalificerade betrodda tjänster på nationell nivå. Det kan således i teorin finnas andra typer av kvalificerade betrodda tjänster på nationell nivå vars reglering inte är harmoniserad.

bestämmelser inte får äventyra strävandet efter harmonisering inom området. De får inte heller uppställa hinder för den fria rörligheten.

7.6 Vilka åtgärder rörande icke kvalificerade tillhandahållare kan vidtas?

Utredningens bedömning: Det är förenligt med EU-rätten att införa nationella bestämmelser som tillåter att icke kvalificerade tillhandahållare och betrodda tjänster förs upp på den förteckning som avses i artikel 22 i eIDAS-förordningen. Det är vidare förenligt med EU-rätten att uppställa vissa kriterier och tekniska krav för icke kvalificerade tillhandahållare och betrodda tjänster som förs upp på förteckningen.

Skälen för utredningens bedömning

Som framgår av avsnitt 7.1 har behovet av att utreda utrymmet för nationell reglering av betrodda tjänster sin grund i ett behov av att skapa förutsättningar för ökad struktur för icke kvalificerade tillhandahållare och betrodda tjänster. Enligt artikel 22.1 i eIDAS-förordningen ska varje medlemsstat upprätta, underhålla och offentliggöra förteckningar med uppgifter om kvalificerade tillhandahållare av betrodda tjänster som den medlemsstaten ansvarar för, tillsammans med uppgifter om de kvalificerade betrodda tjänster som dessa tillhandahåller. Kommissionen har med stöd av artikel 22.5 antagit ett genomförandebeslut som fastställer tekniska minimispecifikationer och format för dessa förteckningar.[7] Av artikel 2 i beslutet framgår även att medlemsstaterna får föra in information om icke kvalificerade tillhandahållare av betrodda tjänster i förteckningen, tillsammans med information om de icke kvalificerade betrodda tjänster som de tillhandahåller. Det ska då i förteckningen tydligt anges vilka tillhandahållare av betrodda tjänster som är icke kvalificerade samt de icke kvalificerade betrodda tjänster de tillhandahåller. Bland de medlems-

[7] Kommissionens genomförandebeslut (EU) 2015/1505 av den 8 september 2015 om fastställande av tekniska minimispecifikationer och format rörande förteckningar över betrodda tjänsteleverantörer i enlighet med artikel 22.5 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden.

stater som har fört upp icke kvalificerade tillhandahållare på sina förteckningar återfinns Danmark, Österrike och Ungern. I kommissionens webbverktyg för att söka i medlemsstaternas tillitsförteckningar (Trusted List Browser) anges dessa som ”recognised at national level”, dvs. erkänd på nationell nivå.

Genom att föra upp icke kvalificerade tillhandahållare och betrodda tjänster på förteckningen kan den aktuella medlemsstaten anses gå i god för att tillhandahållaren eller tjänsten är erkänd på nationell nivå. Det är i och med det enligt vår mening naturligt att medlemsstaten kan förena detta med vissa villkor. Vi bedömer därför att medlemsstaterna har ett utrymme att uppställa vissa kriterier och tekniska krav, förutsatt att dessa inte kan anses äventyra strävandet efter harmonisering inom området eller hindra den fria rörligheten, för att icke kvalificerade tillhandahållare och betrodda tjänster ska kunna föras upp på förteckningen. Samma bedömning gäller även för att föra upp icke kvalificerade betrodda tjänster som tillhandahålls av kvalificerade tillhandahållare.

8 Utredningens förslag

8.1 Utgångspunkter för utredningens förslag

8.1.1 Utredningens uppdrag

Utredningen har i uppdrag att kartlägga och analysera den offentliga förvaltningens behov av åtgärder för ökad och standardiserad användning av betrodda tjänster samt lämna förslag på sådana åtgärder. En slutsats som kan dras av kartläggningsarbetet är att det inte finns något isolerat värde i en ökad användning av betrodda tjänster i den offentliga förvaltningen. Värdet av en ökad användning kommer i stället när betrodda tjänster utifrån verksamhetens behov används på ett ändamålsenligt sätt (se mer utvecklade resonemang kring detta i avsnitt 8.2 och 8.6). Utredningens förslag fokuserar därmed i stort på sådana åtgärder som leder till en enkel och ändamålsenlig användning av betrodda tjänster i den offentliga förvaltningen.

Vad gäller standardiserad användning anser vi att det med detta får avses enhetlig användning. Användningen av tekniska standarder är redan utbredd inom området och formerna för hur standarder tas fram och beslutas är sedan länge etablerat (se mer om framtagandet av standarder i avsnitt 5.12.1). Vi lämnar emellertid ett förslag rörande svenska myndigheters deltagande i standardiseringsarbete med koppling till betrodda tjänster (se avsnitt 8.8).

Utredningen har vidare i uppdrag att särskilt lämna förslag rörande åtgärder för att kunna validera och bevara elektroniska underskrifter. De tekniska behov och utmaningar som finns inom dessa områden är emellertid lika relevanta för elektroniska stämplar då den grundläggande tekniska funktionaliteten är densamma. I avsnitt 8.4 och 8.5 som berör validering och bevarande avhandlas därför underskrifter och stämplar samlat.

8.1.2 Autentisering av webbplatser, elektroniska tidsstämplingar och elektroniska tjänster för rekommenderade leveranser

Vi har i vårt kartläggningsarbete inte identifierat några behov som föranleder förslag avseende tjänster för autentisering av webbplatser.

När det gäller elektroniska tidsstämplingar utgör dessa ofta en komponent inom andra betrodda tjänster. I samband med vår kartläggning har det inte framkommit några behov som enbart gäller denna typ av tjänst.

Som framgår av avsnitt 4.5.2 förekommer många informationsutbyten inom den offentliga förvaltningen och det går inte att utesluta att en eller flera av dessa tekniska lösningar för informationsöverföring omfattas av definitionen av elektronisk tjänst för rekommenderad leverans i enlighet med eIDAS-förordningen. Det är tydligt att det finns ett stort behov av ökat informationsutbyte mellan aktörer i den offentliga förvaltningen samt mellan myndigheter och enskilda. Trots detta, och även med beaktande av att befintliga utbyten ofta bygger på någon form av certifikatslösning, behöver de dock inte nödvändigtvis ske med stöd av elektroniska tjänster för rekommenderade leveranser. Vår kartläggning har inte heller visat att något sådant behov föreligger. Några förslag som specifikt rör denna tjänst kommer därför inte heller att lämnas.

8.1.3 Ökad användning kräver även ökad digital delaktighet

En ökad användning av betrodda tjänster innefattar enligt vår bedömning både den offentliga förvaltningens användning av sådana tjänster och invånarnas nyttjande av dem i sina interaktioner med det offentliga. Det är utifrån detta perspektiv viktigt att beakta de som av olika skäl inte kan eller har svårigheter att använda betrodda tjänster.

Internetstiftelsen publicerar varje år en studie över svenskarnas internetvanor. I juni 2020 publicerades en delrapport om digitalt utanförskap.[1] Även om studien visar att fler och fler använder internet bedöms sällan- och ickeanvändarna av internet utgöra sammantaget 6 procent av befolkningen, ca 3 procent vardera. Gemensamt för gruppen sällan- och ickeanvändare är att många är pensionärer och lever i låginkomsthushåll. Störst andel sällan- och ickeanvändare (17 procent) återfinns bland personer med funktionsnedsättning.

[1] https://svenskarnaochinternet.se/rapporter/digitalt-utanforskap-2020/ (hämtad 2021-01-14).

Även bland dem som mer frekvent använder internet finns det enligt studien behov av olika former av hjälp och stöd. Nära 1 av 5 svenskar anger att de behöver hjälp med att installera ett mobilt BankID. Ser man endast till sällananvändarna behöver ca 6 av 10 hjälp med att installera mobilt BankID och 5 av 10 hjälp med att boka ett läkarbesök på internet.

För personer med funktionsnedsättning kan problem med att använda tjänster även vara kopplade till hur dessa tjänster är utformade. Under pandemin har detta bl.a. visat sig i form av att synskadade haft svårigheter att digitalt boka provtagning för Covid-19.[2]

Det finns i svensk rätt olika bestämmelser avseende tillgänglighet som även kan tillämpas på betrodda tjänster och de e-tjänster där betrodda tjänster används. Exempelvis utgör bristande tillgänglighet en diskrimineringsgrund enligt diskrimineringslagen (2008:567). Enligt 1 kap. 4 § första stycket 3 diskrimineringslagen är bristande tillgänglighet att en person med en funktionsnedsättning missgynnas genom att sådana åtgärder för tillgänglighet inte har vidtagits för att den personen ska komma i en jämförbar situation med personer utan denna funktionsnedsättning. Detta gäller även för myndigheters e-tjänster.[3]

Webbplatser, mobila applikationer och e-tjänster som tillhandahålls av den offentliga förvaltningen omfattas även av lagen (2018:1937) om tillgänglighet till digital offentlig service. Av regelverket framgår att offentliga aktörer, vilket även innefattar många privata utförare inom offentlig sektor, ska uppfylla vissa krav på tillgänglighet som kan uppnås genom att följa en särskild europeisk standard.[4] För webbplatser gäller kraven sedan slutet av september 2020 och för mobila applikationer börjar kraven gälla den 23 juni 2021.

Enligt 9 kap. 2 § lagen (2016:1145) om offentlig upphandling ska vidare, i de fall då det som anskaffas ska användas av fysiska personer, de tekniska specifikationerna bestämmas med beaktande av samtliga användares behov, däribland tillgängligheten för personer med funktionsnedsättning.

Det är viktigt att notera att ovan angivna exempel på svenska författningsbestämmelser som uppställer krav på tillgänglighet inte

[2] Sveriges radios rapportering om att det är svårt för många synskadade att boka coronatest: https://sverigesradio.se/sida/artikel.aspx?programid=83&artikel=7530060 (hämtad 2021-01-14).
[3] Stockholms tingsrätts dom den 11 september 2018 i mål nr T 16972-16.
[4] 5 § Myndigheten för digital förvaltnings föreskrifter om tillgänglighet till digital offentlig service (MDFFS 2019:2).

är uttömmande. Även eIDAS-förordningen innehåller bestämmelser om tillgänglighet. Av artikel 15 följer att betrodda tjänster som tillhandahålls och slutanvändarprodukter som används i samband med tillhandahållandet av dessa tjänster, när det är genomförbart, ska göras tillgängliga för personer med funktionsnedsättning.

I Sverige arbetar många myndigheter och andra aktörer med att öka tillgängligheten till digital offentlig service. Utöver Myndigheten för delaktighets uppgifter med koppling till dessa frågor har exempelvis PTS i uppgift att stärka utvecklingen av fler och bättre kommunikationslösningar för personer med funktionsnedsättning.

Vi anser det vara av central betydelse för en ökad användning av betrodda tjänster att arbetet med att öka den digitala delaktigheten för olika samhällsgrupper fortsätter. Det är därtill viktigt att den offentliga förvaltningen vid utveckling eller upphandling av nya e-tjänster i enlighet med de rättsliga krav som finns alltid beaktar tillgänglighetsperspektivet.

En annan form av digitalt utanförskap är om en person är förhindrad eller har svårigheter att få en e-legitimation. Detta då det hindrar åtkomst till många myndigheters e-tjänster eftersom de inte kan identifiera sig digitalt.[5] Vi vill här betona att det finns vissa problem med koppling till identifikation och identitetsbegreppet som ligger utanför ramen för detta delbetänkande och som därför inte kommer beröras djupare. Det kan dock konstateras att det krävs ett personnummer för att skaffa en svensk e-legitimation. Till detta kan det finnas ytterligare krav, exempelvis måste en person vara kund i en ansluten bank för att få ett BankID. Det är även stor skillnad mellan i vilken grad olika e-legitimationer kan användas i olika tjänster. Således kan en person inneha en svensk e-legitimation men ändå inte kunna använda de e-tjänster som den offentliga förvaltningen erbjuder. Det finns också många individer som saknar personnummer. De är därmed förhindrade att använda den offentliga förvaltningens e-tjänster eller att underteckna handlingar elektroniskt med stöd av en e-legitimation. Behovet av att ge dessa individer möjlighet att anskaffa en e-legitimation måste dock givetvis vägas mot de risker för missbruk som uppstår om e-legitimationer utfärdas utan en tillräckligt säker grundidentifiering (se mer om detta i avsnitt 10.3).

Det kan i sammanhanget noteras att eIDAS-förordningen uppställer krav om att utländska e-legitimationer som anmälts enligt ett

[5] SKR, *Rapport enkät e-legitimationer – 2019 kommuner och regioner*, mars 2020, s. 11.

särskilt förfarande ska kunna användas för att logga in i den offentliga förvaltningens e-tjänster. Detta innebär emellertid inte att den som loggat in på detta sätt i praktiken alltid har möjlighet att använda tjänsterna.[6]

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

8.2.1 Inledning

I eIDAS-förordningen definieras utöver grunddefinitionen av elektroniska underskrifter, i delbetänkandet benämnda som enkla underskrifter, även avancerade respektive kvalificerade elektroniska underskrifter (se mer om de olika nivåerna i avsnitt 5.5.2). Utredningen ska enligt direktiven tydliggöra när avancerade respektive kvalificerade elektroniska underskrifter bör användas i den offentliga förvaltningen. Vi anser att frågan är lika aktuell för elektroniska stämplar och de resonemang som i detta avsnitt förs om elektroniska underskrifter har därför likvärdig relevans för elektroniska stämplar. För att inte tynga texten hänvisas i avsnittet emellertid bara till elektroniska underskrifter.

I bedömningen av när avancerade eller kvalificerade elektroniska underskrifter behövs ligger även motsatsvis en bedömning av när de inte behövs. Vi kommer inte i detta avsnitt att fördjupa oss i denna fråga men om andra alternativ bedöms tillräckliga utifrån de bedömningsgrunder vi anser relevanta kan enkla elektroniska underskrifter eller andra typer av tekniska lösningar vara fullgoda alternativ (se mer om detta i avsnitt 6.5.1).

8.2.2 Vad är skillnaden mellan avancerade och kvalificerade elektroniska underskrifter?

För att kunna bedöma vilken nivå av elektronisk underskrift som bör användas är det av vikt att ha förståelse för skillnaderna mellan dem. I avsnitt 5.5.2 presenteras i större detalj vilka krav som gäller för avan-

[6] Skatteverket, *Fördjupad utredning rörande koppling mellan utländska eID-handlingar och svenska identitetsbeteckningar* (dnr 2 02 27351-19/113), 21 januari 2019, s. 31.

cerade respektive kvalificerade elektroniska underskrifter. Nedan kommer endast att redogöras för skillnaderna på en övergripande nivå.

En kvalificerad elektronisk underskrift är en avancerad elektronisk underskrift som skapas av betrodda tjänster som är kvalificerade och med hjälp av en anordning för skapande av kvalificerade elektroniska underskrifter. Vidare ska en kvalificerad elektronisk underskrift vara baserad på ett kvalificerat certifikat.

En avancerad elektronisk underskrift skapas av betrodda tjänster som inte nödvändigtvis är kvalificerade. Vidare saknas krav på anordning. Det innebär att de tjänster som skapar kvalificerade elektroniska underskrifter omfattas av fler och mer detaljerade bestämmelser än de som skapar avancerade elektroniska underskrifter. Detsamma gäller de kvalificerade tillhandahållarna.

När det gäller icke kvalificerade tillhandahållare ska de vidta lämpliga säkerhetsåtgärder med hänsyn till teknik och kostnad. Säkerhetskraven avseende kvalificerade tillhandahållare är mer detaljerade och ställer krav på policy, processer och rutiner. Dessutom finns för kvalificerade tillhandahållare krav på återkommande överensstämmelsebedömning av ett ackrediterat organ. Det finns även skillnader i tillsyn. För kvalificerade betrodda tjänster får tillsynen vara planlagd eller händelsestyrd, för icke kvalificerade är tillsynen begränsad till att vara händelsestyrd, exempelvis om det kommer till tillsynsmyndighetens kännedom att en säkerhetsincident inträffat.

Skadeståndsbestämmelserna i eIDAS-förordningen skiljer sig också åt beroende på om en betrodd tjänst är kvalificerad eller inte. Något förenklat har den drabbade parten bevisbördan om tjänsten är icke kvalificerad, men om tjänsten är kvalificerad har tillhandahållaren bevisbördan och måste ha finansiell förmåga att bära den ekonomiska risk det innebär.

Ytterligare en tydlig skillnad mellan kvalificerade och avancerade elektroniska underskrifter är att eIDAS-förordningens syfte att åstadkomma gränsöverskridande användning av bl.a. betrodda tjänster är uppbyggt kring en användning av kvalificerade betrodda tjänster. De fler och mer detaljerade kraven för kvalificerade elektroniska underskrifter och kvalificerade tillhandahållare medför bättre förutsättningar för interoperabilitet i gränsöverskridande situationer.[7] Både vad gäller rent teknisk interoperabilitet, och ur ett rättsligt perspektiv

[7] För liknande resonemang se ENISA, *Security guidelines on the appropriate use of qualified electronic signatures*, 29 juni 2017, s. 21.

då en kvalificerad elektronisk underskrift tillerkänns en särskild rättslig status inom EU.

Sammanfattningsvis ska användning av en kvalificerad tjänst utifrån regelverket bl.a. garantera en viss säkerhetsnivå. Den nivå som en icke kvalificerad tjänst måste uppfylla för att t.ex. en elektronisk underskrift ska anses vara avancerad är mycket lägre. Det kan genom detta ligga nära till hands att dra slutsatsen att kvalificerade elektroniska underskrifter alltid är säkrare än avancerade elektroniska underskrifter. Detta är enligt vår uppfattning en förenklad slutsats. Det kan visserligen vara så i enskilda fall vid en jämförelse mellan två olika alternativ, men det innebär inte att så alltid är fallet. En icke kvalificerad tillhandahållare kan välja att leva upp till samma krav som en kvalificerad, eller ännu högre krav, utan att för den delen ha status som kvalificerad tillhandahållare. En avancerad elektronisk underskrift kan leva upp till kraven i artikel 26 och dessutom ha många andra säkerhetsfunktioner som gör den lika säker, eller säkrare, än de krav som ställs på en kvalificerad elektronisk underskrift. Det kan också bero på att säkerheten oftast avtalas mellan tillhandahållaren och den som anskaffar tjänsten. Detta innebär en möjlighet för den enskilda verksamheten att vid behov ställa ytterligare säkerhetskrav på tjänsten och tillhandahållaren av tjänsten. För den som ska anskaffa en tjänst för skapande av elektroniska underskrifter kan det emellertid vara lättare att göra det om kraven är kända och gäller lika för alla, snarare än att behöva se till vilken säkerhetsnivå en enskild tillhandahållare uppfyller eller genom avtalsvillkor kan erbjuda. I synnerhet om man saknar den kompetens som krävs för att genom avtal ställa egna krav på den tjänst som anskaffas. Utredningens förslag i avsnitt 8.3 syftar emellertid till att skapa en tydligare kravbild för icke kvalificerade tillhandahållare och för tjänster avseende bl.a. avancerade elektroniska underskrifter.

8.2.3 Användning av kvalificerade respektive avancerade elektroniska underskrifter i andra länder

Vid en bedömning av när det är lämpligt att använda en viss typ av elektroniska underskrifter är det intressant att jämföra med hur användningen ser ut i andra länder. Den övergripande bild vi har fått är att användningen av avancerade elektroniska underskrifter respektive kvalificerade skiljer sig åt mellan olika medlemsstater.

Till följd av Nordiska ministerrådets arbete med att främja utvecklingen av gränsöverskridande digitala tjänster startades ett gemensamt projekt mellan de nordiska och baltiska länderna (NOBID). Som ett led i detta arbete publicerades i november 2020 en rapport om användningen av betrodda tjänster i dessa länder.[8] Av rapporten framgår att användningen av kvalificerade elektroniska underskrifter är mer utbredd i de baltiska länderna än de nordiska.[9] En tydlig skiljelinje som kan antas ligga bakom detta är att de nordiska länderna, med undantag för Island, i motsats till de baltiska länderna inte i lagstiftning direkt eller indirekt främjat användning av kvalificerade elektroniska underskrifter.[10]

Vad avser antalet tillhandahållare av kvalificerade elektroniska underskrifter finns det inga i Danmark, en vardera i Finland, Island, Estland och Lettland samt två i Litauen. Det land som verkligen utmärker sig är Norge där det finns åtta utfärdare av kvalificerade certifikat för elektroniska underskrifter. Detta är en följd av att alla banker som är en del av det norska BankID-samarbetet måste ha denna kvalifikation.[11] Den mest frekvent använda typen av elektroniska underskrifter i Norge är dock avancerade elektroniska underskrifter med kvalificerade certifikat eftersom ingen av tillhandahållarna i dagsläget erbjuder anordningar för skapande av kvalificerade elektroniska underskrifter.[12]

I Italien används kvalificerade elektroniska underskrifter i stor utsträckning, både av den offentliga förvaltningen och av näringslivet. Något som har drivit på användningen i Italien är enligt vår kontakt med företrädare för den italienska digitaliseringsmyndigheten att nationella bestämmelser om bevisbörda innebär att den som hävdar att en kvalificerad elektronisk underskrift inte är skapad av rätt person också måste kunna visa det.[13] Kvalificerade elektroniska underskrifter används i synnerhet för dokument och avtal som anses vara av särskild vikt. Avancerade elektroniska underskrifter används också, men främst inom vissa sektorer, t.ex. inom bankväsendet och sjukvården. Kvalificerade elektroniska underskrifter har emellertid en mycket starkare ställning än avancerade elektroniska underskrifter

[8] Hinsberg, Hille m.fl., *Study on Nordic-Baltic Trust Services*, 2020.
[9] A.a. s. 7 f.
[10] A.a. s. 14 ff.
[11] A.a. s. 26 ff.
[12] A.a. s. 23.
[13] Uppgift lämnad vid digitalt möte med The Agenzia per l'Italia Digitale den 23 juli 2020.

i Italien. I Italien finns ett 20-tal kvalificerade tillhandahållare av betrodda tjänster.

I Spanien finns bestämmelser som innebär att det vid kontakt med den offentliga förvaltningen går att identifiera sig med system som är baserade på kvalificerade elektroniska certifikat eller andra erkända system.[14] Likaså går det att skriva under elektroniskt med kvalificerade elektroniska underskrifter eller avancerade elektroniska underskrifter baserade på kvalificerade certifikat, eller med andra erkända system.[15] I dagsläget finns 36 kvalificerade tillhandahållare av betrodda tjänster i Spanien, varav vissa är myndigheter.

8.2.4 Användning av kvalificerade respektive avancerade elektroniska underskrifter i Sverige

I Sverige är användningen av avancerade elektroniska underskrifter i den offentliga förvaltningen mycket utbredd. Användningen av kvalificerade elektroniska underskrifter förekommer endast i begränsad omfattning. I sin återrapportering av uppdraget att vidta stödjande åtgärder vid nationellt införande av eIDAS-förordningen konstaterade DIGG att marknaden för kvalificerade betrodda tjänster inte utvecklats på det sätt som eIDAS-förordningen förutsätter.[16] Utbudet av kvalificerade betrodda tjänster i Sverige är litet i jämförelse med andra betrodda tjänster. Fram till oktober 2020 fanns det endast en tillhandahållare av kvalificerade betrodda tjänster i Sverige. I dagsläget finns det två. Vi bedömer att i huvudsak tre faktorer har bidragit till att användningen av betrodda tjänster utvecklat sig på detta sätt. Dessa faktorer presenteras nedan och utgörs av utformning av författningsbestämmelser, behov och utbud.

[14] Artikel 9 Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
[15] Artikel 10 Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
[16] DIGG, *Uppdrag om stödjande åtgärder vid nationellt införande av eIDAS-förordningen* (dnr 2019-90), s. 20.

Författningsbestämmelser som kräver eller främjar användning av kvalificerade elektroniska underskrifter saknas

Det finns i svenska författningar endast bestämmelser som uppställer krav om, eller möjliggör, användning av enkla eller avancerade elektroniska underskrifter. Några författningsbestämmelser som kräver att kvalificerade elektroniska underskrifter ska användas finns inte.

I förarbeten förekommer flera exempel på bedömningar avseende vilken underskriftsnivå som krävs. Det har bl.a. framförts att kvalitetskraven bör bestämmas med hänsyn till vilka behov underskriften ska fylla, det vill säga vad den ska användas till och vad som ska visas med den.[17] Som tidigare nämnts finns det bestämmelser som kräver användning av avancerade elektroniska underskrifter. Detta har motiverats på olika sätt. En motivering som används är att det på avancerade elektroniska underskrifter ställs höga krav på säkerhet och kryptering.[18] Sådana resonemang kompletteras ibland med konstateranden att det inte har framkommit behov av att gå längre än dessa krav genom att i stället föreskriva användning av kvalificerad elektronisk underskrift.[19] Vi har även noterat motiveringar som grundar sig i att de typer av e-legitimationer som i dagsläget är allmänt spridda och använda i Sverige anses ”uppfylla kraven på en avancerad elektronisk underskrift”.[20]

Det går att se som gemensam nämnare i länder med utbredd användning av kvalificerade elektroniska underskrifter att de genom lagstiftning krävt eller främjat denna utveckling. Det är tydligt att avsaknaden av sådana bestämmelser är en starkt bidragande orsak till att det finns en låg efterfrågan för denna typ av underskrifter.

Det bör noteras att ett författningskrav om användning av avancerade eller enkla elektroniska underskrifter givetvis även tillgodoses genom användning av kvalificerade elektroniska underskrifter. Sådana bestämmelser utesluter således inte användningen av kvalificerade elektroniska underskrifter. Det är emellertid förståeligt att myndigheter inte självmant väljer en högre nivå än den som bestämmelserna kräver om de för egen del inte ser ett behov av det.

[17] Prop. 2017/18:126 s. 29.
[18] Se t.ex. prop. 2015/16:125 s. 209.
[19] Prop. 2019/20:189 s. 35.
[20] Se. t.ex. prop. 2015/16:125 s. 209 och prop. 2019/20:189 s. 64 och s. 68.

Den offentliga förvaltningen ser inget stort behov av att använda sig av kvalificerade elektroniska underskrifter

I förarbetena till genomförandet av signaturdirektivet framfördes att det är naturligt att olika slags elektroniska underskrifter med olika säkerhetsnivå utvecklas och accepteras beroende på i vilket syfte de används.[21] Detta speglar väl vår uppfattning om hur den offentliga förvaltningen i stort har hanterat bedömningar rörande om elektroniska underskrifter ska användas och vilken typ av elektronisk underskrift som då ska användas. I avsaknad av uttryckliga krav har behoven fått styra.

Förekomst av uttryckliga krav i författningar är inte heller den enda anledningen till att förvaltningen använder sig av avancerade elektroniska underskrifter. Vi har under vår kartläggning stött på exempel där krav i författning inte specificerar typ av elektronisk underskrift, men där myndigheter själva valt att använda avancerade elektroniska underskrifter. Vi kan vidare konstatera att det finns exempel på att myndigheterna själva i sina föreskrifter väljer att föreskriva om användning av avancerade elektroniska underskrifter, i fall då nivån inte fastställs i lag eller förordning.[22]

Många av de situationer där elektroniska underskrifter används eller behövs är oreglerade. Det finns då utrymme för aktörer inom förvaltningen att själva välja om de vill använda elektroniska underskrifter och om det i så fall ska vara enkla, avancerade eller kvalificerade elektroniska underskrifter. Vår kartläggning visar att aktörerna även i dessa situationer många gånger bedömer att avancerade elektroniska underskrifter lever upp till verksamheternas krav. Vår slutsats är mot bakgrund av detta att den offentliga förvaltningen i stort bedömer att kraven som eIDAS-förordningen ställer på avancerade elektroniska underskrifter oftast tillgodoser deras behov.

Ett begränsat utbud

Det kan enligt vår mening inte uteslutas att det råder ett moment 22 på området med innebörden att utbudet av kvalificerade betrodda tjänster är begränsat eftersom efterfrågan är begränsad, men att efter-

[21] Prop. 1999/2000:117 s. 58.
[22] Se t.ex. 3 § Bolagsverkets föreskrifter (BOLFS 2018:1) om elektronisk ingivning av årsredovisningshandlingar för aktiebolag.

frågan också är begränsad eftersom utbudet är begränsat. Oavsett om så är fallet eller inte visar vår kartläggning att vissa aktörer inom förvaltningen som har övervägt att använda kvalificerade elektroniska underskrifter också har upplevt svårigheter med att införskaffa dem. Det kan även noteras att bristen på tillhandahållare har skapat problem för svenska företag när de vill lämna anbud i andra länder och det uppställs krav om att anbuden ska skrivas under med kvalificerad elektronisk underskrift.[23]

8.2.5 Behoven ska avgöra när avancerade eller kvalificerade elektroniska underskrifter används

Utredningens bedömning: Avancerade respektive kvalificerade elektroniska underskrifter bör användas när det utifrån författningskrav, verksamhetens behov eller informationssäkerhetshänseende är påkallat.

Skälen för utredningens bedömning

Som framgår av avsnitt 8.2.4 används kvalificerade elektroniska underskrifter för närvarande endast i begränsad omfattning i den offentliga förvaltningen. En naturlig följdfråga är om detta i sig utgör ett problem som måste åtgärdas?

I dagsläget finns det ett relativt stort antal tillhandahållare av betrodda tjänster i Sverige (se mer om detta i avsnitt 10.9.1), varav flera erbjuder avancerade elektroniska underskrifter. Det finns emellertid endast två tillhandahållare som är kvalificerade och införande av krav på ökad användning av kvalificerade betrodda tjänster hade uteslutit användning av många tillhandahållares tjänster. Detta hade även, i vart fall inledningsvis, skapat en situation där den offentliga förvaltningen hade fått förlita sig på ett begränsat antal tillhandahållare. Något som både ur konkurrens- och informationssäkerhetshänseende hade varit negativt. DIGG har exemplifierat vad som kan göras för att åtgärda en sådan situation.[24] Vi ser emellertid inget självändamål i

[23] Hinsberg, Hille m.fl., *Study on Nordic-Baltic Trust Services*, 2020, s. 46.
[24] DIGG, *Uppdrag om stödjande åtgärder vid nationellt införande av eIDAS-förordningen* (dnr 2019-90), s. 20.

en ökad användning av kvalificerade elektroniska underskrifter i den offentliga förvaltningen i nuläget.[25] Inte heller i att uppställa någon målbild rörande en ökad användning av sådana underskrifter över tid. Detta eftersom andra underskrifter i många fall, som framgår ovan, kan tillgodose de behov aktörer inom den offentliga förvaltningen har. Det kan därmed inte anses befogat att regelmässigt ställa högre krav på de elektroniska underskrifter som används i förvaltningen. Dessutom bedömer vi att det finns andra mer lämpliga sätt att minska den osäkerhet som råder avseende avancerade elektroniska underskrifter samt främja interoperabilitet (se våra förslag i avsnitt 8.3 och 8.4).

Enligt vår uppfattning är det inte lämpligt att på en generell nivå slå fast när avancerade respektive kvalificerade elektroniska underskrifter bör användas. Detta kräver en kartläggning av vilka behov en specifik verksamhet har och vilka krav externa regelverk uppställer. Utifrån en sådan kartläggning går det sedan att bedöma om elektroniska underskrifter bör användas samt eventuell nivå för sådana underskrifter. Utan att ha full insyn i behoven går det enligt vår uppfattning inte att göra en fullgod bedömning om det är mest lämpligt att använda avancerade eller kvalificerade elektroniska underskrifter. Det är således behoven i de enskilda processerna där underskrifterna ska användas som måste avgöra. Detta gäller både när aktörer inom offentlig förvaltning fattar besluten på egen hand och vid utformning av författningsbestämmelser som reglerar användning av elektroniska underskrifter (se mer om utformning av författningsbestämmelser i avsnitt 8.9.5).

Även om vi inte anser det lämpligt att fastställa när respektive nivå ska användas kan vi utifrån vår kartläggning dra vissa slutsatser om faktorer som bör påverka bedömningen och som framstår som gemensamma för många aktörer inom den offentliga förvaltningen. Dessa faktorer presenteras nedan.

[25] Det kan här noteras att ID-kortsutredningen (*Ett säkert statligt ID-kort – med e-legitimation*, SOU 2019:14, s. 336 ff.) föreslog att det skulle uppställas ett krav om att den statliga e-legitimation de föreslog skulle kunna användas för att skapa en avancerad elektronisk underskrift. De motiverade detta med att med den nuvarande behovsbilden när det gäller elektroniska underskrifter i svenska e-tjänster är det svårt att motivera den ökade komplexitet och kostnad som följer av kraven på särskilda tekniska och säkerhetsmässiga egenskaper i e-legitimationen för att kunna framställa kvalificerade elektroniska underskrifter.

Författningskrav måste identifieras först

En myndighet som överväger att digitalisera en process som innefattar underskrifter måste först undersöka om det aktuella förfarandet omfattas av författningskrav avseende användning av elektroniska underskrifter. Ett område där den offentliga förvaltningen enligt vår kartläggning ofta överväger att använda elektroniska underskrifter är i samband med beslutsfattande. Krav på att myndigheters beslut ska vara undertecknade är dock inte vanligen förekommande.[26]

Det finns som tidigare nämnts ett flertal svenska författningar som anvisar användning av avancerade elektroniska underskrifter. Bestämmelserna kan skilja sig något åt i hur de är utformade. De kan ibland vara formulerade som att avancerade elektroniska underskrifter ska användas och ibland att de får användas. Om avancerade elektroniska underskrifter pekas ut i författning kan den offentliga aktören enligt vår bedömning utgå från den nivån i det fortsatta arbetet, eftersom lagstiftaren i en sådan situation redan får anses ha gjort en bedömning avseende vilken nivå av underskrift som är lämplig.

Författningskrav som pekar mot en nivå av elektronisk underskrift behöver inte enbart finnas i svenska författningar. Den aktuella aktören måste naturligtvis även undersöka om det finns bestämmelser på EU-nivå som påverkar valet. Om underskrifterna ska användas inom ramen för ett gränsöverskridande informationsutbyte bör det även undersökas om det inom ramen för det utbytet ställs krav på nivå av underskrift, t.ex. genom en överenskommelse eller användarvillkor.

Kontroll och tillgång till kompletterande uppgifter kan påverka bedömningen

Om den offentliga aktören bedömer att det finns ett utrymme att själv bestämma vilken nivå av underskrift som ska användas är en faktor som bör påverka valet vilken kontroll aktören har över förfarandet som underskriften ska användas i. En bedömning bör även göras av vilka juridiska funktioner underskriften ska fylla och om den potentiellt kan behöva presenteras som bevisning (se mer om underskrifters juridiska funktion i avsnitt 4.2.2).

Elektroniska underskrifter kan användas för olika förfaranden och på olika sätt. Om det rör sig om ett förfarande där externa parter

[26] eSam, *Juridisk vägledning för införande av e-legitimering och e-underskrifter 1.1,* juni 2018, s. 28.

ska skriva under elektroniskt kan kontrollen, potentiellt, vara mindre än om det rör sig om ett rent internt förfarande där t.ex. aktörens medarbetare skriver under. Hur förfarandet är uppbyggt kan påverka vilken kontroll den offentliga aktören har, vilket i sin tur kan påverka bedömningen om vilken nivå av underskrift som är lämplig. Här bör även tillgången till kompletterande uppgifter vägas in. Skillnaden kan illustreras med en jämförelse mellan en e-tjänst och ett förfarande där en enskild skickar in elektroniskt undertecknade handlingar, exempelvis i PDF-format. Vid användningen av e-tjänsten kan det finnas krav på att användaren först måste autentisera sig, dessutom kan det användaren gör i tjänsten loggas vilket genererar kompletterande uppgifter. Sammantaget kan detta ge goda möjligheter till kontroll som kan hjälpa till att säkerställa att det är rätt person som skriver under. Något som kan tala för att avancerade elektroniska underskrifter, eller t.o.m. enkla elektroniska underskrifter, som i kombination med sådana kontrollmöjligheter kan vara fullt tillräckliga utifrån behovsbilden. Om den offentliga aktören i stället väljer att låta externa aktörer inkomma med elektroniskt undertecknade dokument via exempelvis e-post kan nivån av kontroll vara lägre. Tillgången till kompletterande uppgifter kan i sådana fall också vara mer begränsad. Det kan tala för att det kan vara lämpligt att kräva kvalificerade elektroniska underskrifter, särskilt om personer eller företag från andra EU-länder förväntas inkomma med undertecknade handlingar.

Användningen måste vägas in

En annan faktor som vi har identifierat som gemensam för många aktörer inom den offentliga förvaltningen är hur de elektroniska underskrifterna, och framför allt det de har använts för att skriva under, ska användas och av vem. Till att börja med bör användningen av undertecknade handlingar delas upp mellan de handlingar som inkommer till aktörer inom förvaltningen och de handlingar som skapas av aktörer inom förvaltningen. För handlingar som inkommer till en aktör inom ramen för ett förfarande behöver aktören avgöra hur handlingarna kan komma att användas. Om det bara är den aktuella aktören som kommer att använda handlingarna kan det i enlighet

med vad som framgår ovan tala för avancerade elektroniska underskrifter, om kontrollen i övrigt är tillfredsställande.

För handlingar som skrivs under elektroniskt av offentliga aktörers medarbetare blir användningen viktig. Handlingar som skrivs under skulle exempelvis kunna vara beslut eller intyg. Det kan vara så att beslutet eller intyget kan behöva användas gentemot tredje part, parter som i sin tur behöver kunna validera underskriften. Om så är fallet kan det tala för att kvalificerade elektroniska underskrifter är lämpliga att använda, framför allt om användningen kan komma att ske i andra EU-länder. Det bör då i bedömningen vägas in vilka möjligheter tredje part har till fullgod validering. Vår kartläggning visar att de aktörer som ser behov av att använda kvalificerade elektroniska underskrifter framför allt gör det mot bakgrund av gränsöverskridande användning, exempelvis betyg från lärosäten. Vi ser också att det framför allt är vid gränsöverskridande användning som det är tydligt att kvalificerade elektroniska underskrifter kan vara mer lämpliga att använda än avancerade.

8.3 En utökad tillitsförteckning

8.3.1 Inledning

Vår kartläggning visar att många aktörer inom den offentliga förvaltningen upplever det som svårt att bedöma om vissa betrodda tjänster lever upp till kraven i eIDAS-förordningen. Detta påverkar bl.a. möjligheterna att anskaffa tjänster för skapande av avancerade elektroniska underskrifter och förutsättningarna för att validera dessa underskrifter.

Utredningen om effektiv styrning av nationella digitala tjänster konstaterade även att kraven i eIDAS-förordningen på certifikat som inte är kvalificerade är otydliga, vilket innebär en svårighet för en mottagare av en avancerad elektronisk underskrift att avgöra vilken kvalitet och säkerhet som en sådan underskrift har, t.ex. hur väl identifierad undertecknaren är.[27] Vi instämmer i den beskrivningen och menar att utökade möjligheter till att göra dessa kontroller hade underlättat och effektiviserat den offentliga förvaltningens använd-

[27] *reboot – omstart för den digitala förvaltningen* (SOU 2017:114), s. 385.

ning av betrodda tjänster. Det hade även varit ett sätt att höja säkerheten och stärka tilliten vid användning av betrodda tjänster.

En tänkbar lösning vore en övergång till en mer utbredd användning av kvalificerade elektroniska underskrifter eller stämplar eftersom dessa omfattas av en mer detaljerad reglering. Som en del av detta mer detaljerade regelverk ingår den förteckning som sköts av PTS och som innehåller kvalificerade tillhandahållare av betrodda tjänster och de kvalificerade betrodda tjänster som dessa aktörer tillhandahåller. Liknande förteckningar tillhandahålls av alla medlemsstater. Genom förteckningarna går det att hitta tillhandahållare av betrodda tjänster samt betrodda tjänster, för den som vill köpa eller förlita sig på dem. Det främsta användningsområdet för förteckningarna är att de möjliggör kontroll och validering av de kvalificerade betrodda tjänsterna. Den som t.ex. tar emot en handling som undertecknats med en kvalificerad elektronisk underskrift och som behöver validera den kan använda förteckningen som stöd. En viktig fråga som besvaras är om tillhandahållaren går att lita på eller inte, vilket det går att utgå ifrån eftersom tillhandahållaren är kvalificerad och lever upp till kraven i eIDAS-förordningen.

Som konstateras i avsnitt 8.2 är användningen av kvalificerade betrodda tjänster i dagsläget begränsad i den offentliga förvaltningen och myndigheter bedömer att deras behov oftast kan tillgodoses genom användning av avancerade elektroniska underskrifter eller stämplar. Mot denna bakgrund bedömer vi att en mer utbredd övergång till användning av kvalificerade elektroniska underskrifter eller stämplar inte hade varit en proportionerlig åtgärd för att åstadkomma den önskade effekten.

En europeisk infrastruktur finns redan på plats för medlemsstaterna att använda

Givet att den offentliga förvaltningen fortsatt ser ett behov av att kunna använda och hantera avancerade elektroniska underskrifter och till viss del avancerade elektroniska stämplar kvarstår frågan vad som kan göras för att underlätta anskaffandet och användningen av dessa tjänster?

Utredningen om effektiv styrning av nationella digitala tjänster framförde att en nationell säkerhetsnivå som fastställs i regelverk skulle underlätta möjligheten att avgöra vilka underskrifter som godtas i

offentliga e-tjänster nationellt samt vilka som kan godtas internationellt.[28] Vidare framförde utredningen att kraven på elektroniska underskrifter bör samordnas med kraven på elektronisk identifiering och på ett motsvarande sätt med tillitsramverk genom lagstiftning med övergripande krav, samt förordning med mandat att utfärda föreskrifter.[29]

En annan tänkbar lösning är att införa en form av kvalitetsmärkning för betrodda tjänster, i likhet med den kvalitetsmärkning som redan existerar för e-legitimationer.[30] Utfärdare av e-legitimation kan låta sig kvalitetsgranskas av DIGG. Granskningen är frivillig och görs utifrån DIGG:s tillitsamverk. Syftet med förfarandet och märket är att offentliga och privata aktörer med e-tjänster som kräver e-legitimation ska kunna lita på e-legitimationer som har kvalitetsmärket.[31] Användarna ska också kunna känna sig trygga i att det är en säker identitetshandling. Ett kvalitetsmärke för betrodda tjänster skulle tjäna samma syften.

Ytterligare ett alternativ är att införa en nationell förteckning över tillhandahållare av betrodda tjänster och betrodda tjänster som den offentliga förvaltningen kan lita på. En förteckning som det ska gå att göra maskinella kontroller gentemot. En sådan förteckning skulle möjligen kunna kombineras med ett kvalitetsmärke enligt ovan.

Gemensamt för lösningarna ovan är att de hade varit nationella juridiska konstruktioner utan tydlig förankring i det EU-rättsliga regelverket. Som framgår av kapitel 7 är betrodda tjänster reglerade på EU-nivå och det nationella utrymmet att vidta åtgärder är begränsat. De åtgärder som vidtas måste överensstämma med eIDAS-förordningen och det övergripande syftet om en harmoniserad marknad för betrodda tjänster. Principen om fri rörlighet måste även beaktas. Vår bedömning är att de alternativ som redovisas ovan antingen riskerar att stå i strid med eIDAS-förordningen eller potentiellt utgöra hinder för den fria rörligheten. Dessa lösningar skulle inte heller främja acceptans i övriga Europa av i Sverige skapade elektroniska underskrifter och stämplar eftersom det hade varit rent nationella företeelser.

Vi ser emellertid att det finns en lösning som både tillgodoser behoven och som är förenlig med EU-rätten. Varje medlemsstat i EU

[28] *reboot – omstart för den digitala förvaltningen* (SOU 2017:114), s. 387.
[29] A.a.
[30] www.digg.se/digital-identitet/e-legitimering#kvalitetsmarket_svensk_e-legitimation (hämtad 2021-01-14).
[31] A.a.

ska tillhandahålla ovan nämnda förteckningar och det finns sedan tidigare tekniska krav för förteckningarna. I dagsläget är det endast kvalificerade tjänster och tillhandahållare som kan föras upp på den svenska förteckningen. Någon sådan begränsning finns emellertid inte i eIDAS-förordningen och det finns flera exempel på medlemsstater som tillåter icke kvalificerade tillhandahållare på deras förteckningar (se mer om detta i avsnitt 7.6).

En europeisk infrastruktur finns alltså redan på plats som möjliggör de kontroller som förvaltningen efterfrågar och som fyller de syften ett nationellt kvalitetsmärke och en nationell förteckning skulle göra. Vi anser därför att en utökning av den förteckning som redan existerar i Sverige är det bästa sättet att tillgodose behoven och även det lämpligaste alternativet sett till de EU-rättsliga aspekterna.

Vidare är enbart det faktum att förteckningen redan existerar ett starkt skäl till utökad användning av den. Förteckningarna är dessutom interoperabla inom EU vilket möjliggör för aktörer i andra medlemsstater att ta del av informationen. En rent nationell förteckning skulle sakna sådan interoperabilitet. Genom att använda den europeiska infrastrukturen i större utsträckning än i dag finns dessutom bättre förutsättningar för att främja den fria rörligheten.

8.3.2 Förteckningen ska benämnas tillitsförteckning

Utredningens förslag: Den förteckning som avses i artikel 22 i eIDAS-förordningen ska i Sverige benämnas som tillitsförteckning.

Skälen för utredningens förslag

Den förteckning som framgår av artikel 22 i eIDAS-förordningen benämns i den svenska språkversionen av förordningen som förteckning över betrodda tjänsteleverantörer. I den engelska språkversionen av förordningen benämns dessa förteckningar som ”trusted lists”. Det är vanligt att den engelska termen används också i Sverige. I 5 § förordningen (2016:576) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering föreskrivs att PTS

ska sköta denna förteckning i Sverige. PTS har valt att presentera denna förteckning som förteckning över anmälda aktörer.[32]

Även om förteckningen genom förordningen har ett formellt namn används det inte i någon större utsträckning. Som framgår ovan är det vanligare att den engelska termen används. Vi anser därför att förteckningen bör få en beteckning på svenska som på ett mer koncentrerat och tydligt sätt beskriver dess syfte. Att anamma den engelska termen ”trusted list” anser vi inte vara lämpligt. Att benämna förteckningen ”förteckningen enligt artikel 22 i eIDAS-förordningen” skulle för någon som inte är bekant med förordningen eller den aktuella artikeln inte ge tillräcklig information om vad förteckningen syftar till och det är därtill ett onödigt långt namn. Ett annat alternativ skulle kunna vara att låta förteckningen heta ”förteckning över tillhandahållare av betrodda tjänster samt betrodda tjänster”, eller enbart ”förteckning över tillhandahållare av betrodda tjänster”. Dessa alternativ skulle tydligare förmedla vad förteckningen innehåller, men ligger språkligt nära förordningens beteckning. Ytterligare ett alternativ skulle vara att benämna förteckningen som betrodd förteckning. Vi anser emellertid inte att det är en lämplig lösning rent språkligt.

Syftet med att använda betrodda tjänster är att skapa tillit mellan aktörer. Tillhandahållarna av betrodda tjänster har en central roll i att skapa denna tillit. Eftersom syftet är tillit anser vi att en lämplig benämning för förteckningen på svenska är tillitsförteckning. Det signalerar vad förteckningen syftar till och ligger även språkligt nära den engelska beteckningen ”trusted list”. Det är inte heller en term som i dagsläget förekommer i någon svensk författning.

[32] www.pts.se/sv/bransch/internet/betrodda-tjanster-eidas/forteckning-over-anmalda-aktorer/ (hämtad 2021-01-14).

8.3.3 Icke kvalificerade tillhandahållare ska kunna föras upp på tillitsförteckningen

Utredningens förslag: Tillhandahållare som är icke kvalificerade ska under vissa förutsättningar kunna föras upp på tillitsförteckningen.

Skälen för utredningens förslag

Av kommissionens genomförandebeslut (EU) 2015/1505 som fastställer tekniska minimispecifikationer och format för tillitsförteckningarna framgår att medlemsstaterna på frivillig basis och på nationell nivå får infoga information om icke kvalificerade tillhandahållare av betrodda tjänster, tillsammans med information om de icke kvalificerade betrodda tjänster som dessa tillhandahåller (skäl 4 och artikel 2). Vidare ska det tydligt anges vilka tillhandahållare av betrodda tjänster som inte är kvalificerade, och de icke kvalificerade betrodda tjänster de tillhandahåller. I kommissionens webbverktyg Trust Service Browser anges det att sådana betrodda tjänster är erkända på nationell nivå (”recognised at national level”).[33]

Vi föreslår en utökning av den svenska tillitsförteckningen genom att även tillåta att icke kvalificerade tillhandahållare av betrodda tjänster förs upp på listan. I dag innehåller förteckningen, i enlighet med de krav som ställs i eIDAS-förordningen, kvalificerade tillhandahållare av betrodda tjänster och betrodda tjänster som de tillhandahåller. Genom att låta även icke kvalificerade tillhandahållare samt icke kvalificerade betrodda tjänster föras upp på den svenska tillitsförteckningen bör det bli lättare för den offentliga förvaltningen att kunna genomföra de kontroller och bedömningar som behövs. Vilket bör underlätta användningen av betrodda tjänster i den offentliga förvaltningen. Vi ser även att det kan underlätta för nya tillhandahållare att ta sig in på marknaden då en extern kontroll av om en tjänst uppfyller förordningens krav kan underlätta att marknadsföra tjänsten. Det kan även vara till fördel för tillhandahållare som vill sälja sina tjänster i andra länder.

När det gäller möjligheterna att ställa upp krav för att sådana tillhandahållare och tjänster ska få vara med i förteckningen gör vi följande

[33] https://webgate.ec.europa.eu/tl-browser/#/ (hämtad 2021-01-14).

bedömning. Bestämmelserna i eIDAS-förordningen samt förordningens syfte måste givetvis beaktas. Vilka krav som ställs på tillhandahållare av betrodda tjänster som inte är kvalificerade framgår av artikel 19. Upplysningsvis kan här nämnas att det finns ett förslag om att upphäva artikel 19 (se mer om detta i avsnitt 5.6.2). Kraven i artikeln gäller för alla tillhandahållare, oavsett om de är kvalificerade eller inte. Kraven är emellertid i stora delar allmänt hållna. Möjligheten enligt artikel 2 i kommissionens genomförandebeslut att ha med icke kvalificerade tillhandahållare och betrodda tjänster i tillitsförteckningen måste enligt vår bedömning innebära en möjlighet för medlemsstaterna att kontrollera att tillhandahållarna lever upp till kraven i eIDAS-förordningen. Sådana kontroller skulle vara i princip omöjliga om det saknas mer detaljerade krav att kontrollera mot. Skrivningen om ”nationell nivå” i skäl 4 i kommissionens beslut samt att icke kvalificerade betrodda tjänster anges vara erkända på nationell nivå i kommissionens Trusted List Browser anser vi ytterligare talar för det. Vår bedömning är att medlemsstater som väljer att tillåta icke kvalificerade tillhandahållare och betrodda tjänster i sina tillitsförteckningar kan ställa upp krav som tillhandahållarna och tjänsterna måste leva upp till för att vara med i förteckningen.

8.3.4 Icke kvalificerade betrodda tjänster som får föras upp på förteckningen

Utredningens förslag: De icke kvalificerade betrodda tjänster som ska kunna föras upp på tillitsförteckningen är tjänster som skapar eller validerar avancerade elektroniska underskrifter alternativt avancerade elektroniska stämplar.

Skälen för utredningens förslag

Definitionen av betrodda tjänster i eIDAS-förordningen omfattar olika funktioner inom olika områden. Vår kartläggning visar att de områden där aktörer inom offentlig förvaltning ser störst behov och flest utmaningar är elektroniska underskrifter och elektroniska stämplar. När det gäller elektroniska underskrifter är det den avancerade nivån som utmärker sig. En återkommande utmaning är svårigheten

att bedöma om en betrodd tjänst skapar avancerade elektroniska underskrifter. Vi tror dessutom att det finns potential till ökad användning av elektroniska stämplar både inom förvaltningen och i utbyten mellan enskilda och förvaltningen. Vi gör vidare bedömningen att det framför allt är avancerade elektroniska stämplar vars användning kommer öka.

Mot denna bakgrund föreslår vi att betrodda tjänster som skapar eller validerar avancerade elektroniska stämplar och avancerade elektroniska underskrifter får föras upp på den svenska tillitsförteckningen. Om en sådan tjänst, som finns med i förteckningen har använts av en extern part för att skapa en underskrift eller stämpel, bör det underlätta valideringen av underskriften eller stämpeln. Detsamma gäller om en aktör i förvaltningen har använt en sådan tjänst för att skapa en underskrift eller stämpel och en annan part behöver validera underskriften eller stämpeln. De betrodda tjänster som skapar eller validerar avancerade elektroniska underskrifter eller stämplar och som kan föras upp på tillitsförteckningen kan tillhandahållas både av kvalificerade och icke kvalificerade tillhandahållare.

Vi föreslår att det i förordning föreskrivs att det är betrodda tjänster som skapar eller validerar avancerade elektroniska underskrifter och stämplar som får vara med i förteckningen. Det har i vår kartläggning inte framkommit behov eller utmaningar avseende andra betrodda tjänster som föranleder oss att föreslå att dessa tjänster i nuläget bör få vara med i den svenska förteckningen. Om behov uppstår att låta andra betrodda tjänster vara med i tillitsförteckningen kan det möjliggöras genom en ändring av förordningen.

Som framgår av avsnitt 5.12.2 granskar DIGG fristående underskriftstjänster utifrån den normativa specifikation för sådana tjänster som myndigheten har tagit fram. Dessa tjänster bör falla inom definitionen av betrodda tjänster. För det fall de kan ingå i den svenska tillitsförteckningen bör det granskningsförfarande och godkännande som DIGG i dag utför utmönstras då tillitsförteckningen kommer att fylla samma funktion som godkännandet.

8.3.5 En ansökan om att föras upp på tillitsförteckningen ska handläggas av tillsynsmyndigheten

Utredningens förslag: Det ska vara frivilligt för icke kvalificerade tillhandahållare att vara med i förteckningen.

En ansökan om att en tillhandahållare eller en betrodd tjänst ska föras upp på tillitsförteckningen ska handläggas av tillsynsmyndigheten.

Om en tillhandahållare av betrodda tjänster begär det ska tillhandahållaren eller en betrodd tjänst denne tillhandahåller avföras från tillitsförteckningen.

Skälen för utredningens förslag

Till skillnad från vad som gäller för kvalificerade tillhandahållare av betrodda tjänster, som ska finnas med i respektive medlemsstats tillitsförteckning när de beviljas status som kvalificerade, ska det vara frivilligt för icke kvalificerade tillhandahållare av betrodda tjänster att föras upp på förteckningen. Vi föreslår därmed inte att det införs ett krav som innebär att icke kvalificerade tillhandahållare måste finnas med i tillitsförteckningen för att få tillhandahålla betrodda tjänster i Sverige.

En tillhandahållare av betrodda tjänster som vill vara med i den svenska tillitsförteckningen ska ansöka om det. Det krävs således en aktiv handling från tillhandahållaren. Ansökan ska omfatta tillhandahållaren som sådan och de betrodda tjänster denne vill ska vara med i förteckningen. PTS har till uppgift att tillhandahålla den nuvarande svenska tillitsförteckningen.[34] Vi ser ingen anledning att flytta denna uppgift till en annan myndighet. I egenskap av tillsynsmyndighet har PTS i dagsläget också till uppgift att bedöma om en tillhandahållare av betrodda tjänster ska beviljas status som kvalificerad. Vår bedömning är att den möjlighet vi föreslår för icke kvalificerade tillhandahållare av betrodda tjänster att vara med i den svenska tillitsförteckningen är nära förknippat med de uppgifter PTS redan utför på området. Det är därför naturligt att ansökningsförfarandet hanteras av PTS med beaktande av den kompetens och de befintliga strukturer för att

[34] 5 § förordningen (2016:576) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering.

hantera processer avseende kvalificerade tillhandahållare och tjänster som myndigheten redan besitter. För att en icke kvalificerad tillhandahållare och icke kvalificerade betrodda tjänster ska få vara med i förteckningen ska det krävas ett beslut om det av PTS, efter det att myndigheten har bedömt tillhandahållarens ansökan.

8.3.6 Kriterier och krav för icke kvalificerade tillhandahållare och betrodda tjänster

Utredningens förslag: För att föras upp på förteckningen måste icke kvalificerade tillhandahållare leva upp till vissa kriterier och tekniska krav. Detta gäller även icke kvalificerade betrodda tjänster som tillhandahålls av kvalificerade tillhandahållare.

Skälen för utredningens förslag

De icke kvalificerade tillhandahållare som vill föras upp på tillitsförteckningen behöver leva upp till vissa kriterier och tekniska krav. Detsamma gäller de icke kvalificerade betrodda tjänster som ska vara med i förteckningen. Oavsett om de tillhandahålls av en kvalificerad eller icke kvalificerad tillhandahållare. För tillhandahållarna är utgångspunkten artikel 19.1 i eIDAS-förordningen, där det föreskrivs att tillhandahållare av betrodda tjänster ska vidta lämpliga tekniska och organisatoriska åtgärder för att hantera riskerna för säkerheten hos de betrodda tjänster som de tillhandahåller. Vidare framgår att med beaktande av den senaste tekniska utvecklingen ska dessa åtgärder säkerställa att säkerhetsnivån står i proportion till graden av risk. I synnerhet ska åtgärder, enligt bestämmelsen i förordningen, vidtas för att förhindra eller minimera säkerhetsincidenters inverkan samt för att informera berörda parter om de negativa effekterna av eventuella sådana incidenter. Vår bedömning är att eIDAS-förordningen ger medlemsstaterna utrymme att specificera hur tillhandahållare kan leva upp till dessa krav, i synnerhet om en medlemsstat väljer att låta icke kvalificerade tillhandahållare vara med i sin tillitsförteckning. Hur tillhandahållarna kan leva upp till kraven fordrar sådan detaljreglering att det lämpligen fastställs i myndighetsföreskrifter.

För betrodda tjänster gäller olika bestämmelser för respektive tjänst. Vilka tjänster vi föreslår ska få vara med i förteckningen framgår av avsnitt 8.3.4. Även för tjänsterna kommer detaljnivån för hur de kan leva upp till kraven vara sådan att detaljerna lämpligen fastställs i myndighetsföreskrifter. Vi föreslår därför att PTS får föreskriftsrätt för detta ändamål.

Det kommer således vara upp till PTS att genom föreskrifter fastställa detaljerna i det som kommer att ligga till grund för myndighetens bedömning om en tillhandahållare eller en betrodd tjänst lever upp till uppställda kriterier och tekniska krav och därigenom får föras upp på tillitsförteckningen. Det är enligt vår mening viktigt att kommande kriterier och tekniska krav i myndighetsföreskrifter är välbalanserade. De måste uppnå sitt syfte, dvs. att de leder till tillit, och samtidigt gå att leva upp till genom ansträngningar som är rimliga att begära av tillhandahållarna. Kriterierna och de tekniska kraven bör inte vara lika omfattande som de som ställs på kvalificerade tillhandahållare och kvalificerade betrodda tjänster, eftersom syftet med att tillåta icke kvalificerade tillhandahållare och tjänster på förteckningen då skulle gå förlorat. Kriterierna och de tekniska kraven behöver självfallet också beakta EU-rätten i allmänhet och eIDAS-förordningen i synnerhet. Kriterier som t.ex. per automatik utestänger tillhandahållare som är etablerade i andra medlemsstater än Sverige kan inte anses förenliga med bestämmelserna om fri rörlighet och riskerar att äventyra strävandet efter harmonisering inom området. För det fall myndigheten väljer att peka mot standarder kan det därför vara lämpligt att i möjligaste mån peka mot europeiska standarder eller andra internationella standarder vars användning är utbredd i Europa. Det är emellertid samtidigt viktigt att beakta den princip om teknikneutralitet som förordningen ger uttryck för.

PTS har i dagsläget ingen föreskriftsrätt avseende de krav som kvalificerade tillhandahållare ska leva upp till. I stället hänvisar PTS i sin vägledning avseende betrodda tjänster till sätt för tillhandahållare att leva upp till kraven i eIDAS-förordningen.[35] Eftersom kraven på kvalificerade tillhandahållare är mer omfattande i eIDAS-förordningen, och behovet av kompletterande bestämmelser därigenom mindre, ser vi ingen motsättning i att PTS får föreskriftsrätt avseende kriterierna och de tekniska kraven för icke kvalificerade tillhandahållare att tas upp i förteckningen.

[35] PTS, *Vägledning för betrodda tjänster i Sverige enligt eIDAS (Utgåva 3)*, 10 juni 2020.

8.3.7 Kontroll av efterlevnad m.m.

Utredningens förslag: Tillsynsmyndigheten ska återkommande bedöma om en icke kvalificerad tillhandahållare eller icke kvalificerad betrodd tjänst som finns med i tillitsförteckningen fortfarande lever upp till uppställda kriterier och tekniska krav. Tillsynsmyndigheten ska ha möjlighet att förelägga en tillhandahållare om att säkerställa att den, eller en betrodd tjänst, lever upp till dessa kriterier och tekniska krav.

Tillsynsmyndigheten får också besluta om att avföra en tillhandahållare eller betrodd tjänst som inte längre lever upp till uppställda kriterier och tekniska krav från tillitsförteckningen. Tillsynsmyndigheten får bestämma att ett sådant beslut ska gälla omedelbart.

Tillsynsmyndighetens beslut får överklagas till allmän förvaltningsdomstol. Prövningstillstånd krävs vid överklagande till kammarrätten.

Skälen för utredningens förslag

Tillsyn över betrodda tjänster regleras i eIDAS-förordningen. För tillsyn över kvalificerade tillhandahållare finns i artikel 20 särskilda bestämmelser. Kraven på medlemsstaternas tillsynsorgan när det gäller tillsyn är betydligt mer omfattande för kvalificerade tillhandahållare än för icke kvalificerade. Det innebär inte per automatik att det finns ett utrymme för medlemsstaterna att införa mer omfattande tillsyn för icke kvalificerade tillhandahållare. Utgångspunkten bör enligt vår bedömning i stället vara att anse tillsynen över betrodda tjänster som harmoniserad på EU-nivå, eftersom tillsynsbestämmelserna i förordningen rör både kvalificerade och icke kvalificerade tillhandahållare.

Med hänsyn till att eIDAS-förordningen tillåter medlemsstaterna att ha även icke kvalificerade tillhandahållare på sina tillitsförteckningar måste det dock finnas utrymme för någon form av kontroll förenat med det. Enligt vårt förslag ska en icke kvalificerad tillhandahållare som vill vara med på den svenska förteckningen ansöka om det hos tillsynsmyndigheten PTS. PTS ska därför bedöma om en icke kvalificerad tillhandahållare och/eller betrodd tjänst uppfyller de kriterier och tekniska krav som föreskrivs i eIDAS-förordningen och i myn-

dighetsföreskrifter. Om det efter en sådan bedömning saknas möjligheter till återkommande uppföljning riskerar tilliten till tillhandahållarna och deras betrodda tjänster att minska ju längre tiden går. Det skulle med andra ord inte vara tillfredsställande ur ett tillitsperspektiv om en tillhandahållare eller tjänst som har genomgått bedömningen kan vara med i förteckningen för all framtid utan uppföljning. Vi föreslår mot bakgrund av det att PTS återkommande gör en ny bedömning om den aktuella tillhandahållaren eller tjänsten lever upp till uppställda kriterier och tekniska krav. För kvalificerade tillhandahållare gäller enligt artikel 20.1 i eIDAS-förordningen att de minst en gång vartannat år och på egen bekostnad ska granskas av ett organ för bedömning av överensstämmelse. Vi bedömer att det kan vara ett lämpligt tidsintervall också för bedömningen avseende icke kvalificerade tillhandahållare och betrodda tjänster. Till det kommer kravet i artikel 19.2 i förordningen på alla tillhandahållare att utan dröjsmål och senast inom 24 timmar rapportera säkerhetsincidenter eller integritetsförluster som i betydande omfattning påverkar den betrodda tjänst som tillhandahålls eller på de personuppgifter som ingår i denna till PTS. Sådana incidenter kan, beroende på sin karaktär och omfattning, påverka bedömningen om tillhandahållaren eller tjänsten fortsatt lever upp till kraven.

För det fall en tillhandahållare eller tjänst konstateras inte längre leva upp till uppställda kriterier och tekniska krav för att vara med i förteckningen måste det finnas sanktionsmöjligheter. PTS bör ha möjlighet att förelägga en tillhandahållare om att säkerställa att den eller en betrodd tjänst lever upp till det som åligger dem. Sådana möjligheter finns redan i 6 § lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering. Enligt paragrafens första stycke får tillsynsmyndigheten meddela de förelägganden och förbud som behövs för efterlevnaden av lagen och föreskrifter som har meddelats med stöd av lagen samt efterlevnaden av eIDAS-förordningen och rättsakter som har meddelats med stöd av den. PTS kommer, i egenskap av tillsynsmyndighet, att med stöd av bestämmelsen kunna meddela nödvändiga förelägganden och förbud också avseende de icke kvalificerade tillhandahållare och betrodda tjänster som förs upp på tillitsförteckningen.

Det bör emellertid också vara möjligt för PTS att besluta om att avföra en icke kvalificerad tillhandahållare eller en icke kvalificerad tjänst från tillitsförteckningen om de inte längre bedöms leva upp till

uppställda kriterier och tekniska krav. Med anledning av att det kan leda till allvarliga säkerhetsrisker att ha tillhandahållare eller tjänster kvar i förteckningen som inte lever upp till kriterierna eller de tekniska kraven bör tillsynsmyndigheten få bestämma att ett beslut om att avföra en icke kvalificerad tillhandahållare eller tjänst från förteckningen ska gälla omedelbart. För kvalificerade tillhandahållare samt kvalificerade betrodda tjänster är förekomsten på tillitsförteckningen enligt eIDAS-förordningen kopplat till statusen som kvalificerad. Att tillhandahållare och tjänster kan förlora statusen som kvalificerad regleras redan i artikel 20.3 i förordningen, där det också framgår att tillitsförteckningen då ska uppdateras.

PTS beslut rörande tillitsförteckningen ska kunna överklagas till allmän förvaltningsdomstol. I likhet med vad som är huvudregeln för överklagande av förvaltningsbeslut bör prövningstillstånd krävas för överprövning i kammarrätten. Bestämmelser om detta finns redan i 8 § i lagen med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering och någon ändring av lagen krävs således inte av denna anledning.

8.4 En nationell valideringstjänst

8.4.1 Inledning

Utredningen om effektiv styrning av nationella digitala tjänster framförde att skyldigheten att erkänna elektroniska underskrifter och stämplar från andra medlemsstater innebär ett behov för svenska tillhandahållare av e-tjänster, dvs. aktörer inom offentlig förvaltning, att kunna validera dessa.[36] Utredningen anförde även att det är både svårt och betungande för varje statlig myndighet, kommun och region att själva upphandla den nödvändiga funktionaliteten som krävs för att validera elektroniska underskrifter och stämplar.[37] Vårt kartläggningsarbete har visat att dessa svårigheter inte bara gäller validering av elektroniska underskrifter från andra länder utan även validering av svenska elektroniska underskrifter. Många aktörer inom förvaltningen beskriver att de upplever svårigheter med valideringen och har framfört att en gemensam tjänst skulle underlätta hanteringen. En förvaltningsgemensam valideringstjänst bör också leda till

[36] *reboot – omstart för den digitala förvaltningen* (SOU 2017:114), s. 385 f.
[37] A.a.

att varje aktör inom förvaltningen inte var för sig behöver lösa frågor rörande vad som ska valideras och hur. Flera andra medlemsstater, däribland Danmark, Nederländerna och Österrike har centrala valideringstjänster som den offentliga förvaltningen inom respektive land kan nyttja.[38] Vissa av tjänsterna är tillgängliga även för enskilda individer. Utredningen om effektiv styrning av nationella digitala tjänster föreslog att en sådan samlad valideringstjänst bör införas i Sverige eller åtminstone upphandlas centralt för nyttjande av den offentliga förvaltningen. Utredningen föreslog vidare att det som sedermera blev DIGG skulle ges detta uppdrag.[39] Vid remissbehandlingen av betänkandet tillstyrktes förslaget av Bolagsverket och Statskontoret, men kommenterades inte av övriga remissinstanser. En valideringstjänst i enlighet med utredningens förslag har inte tagits fram.

Sedan utredningen lämnade förslaget har det pågått olika arbeten med valideringstjänster, bl.a. har Vinnova finansierat utveckling av en sådan tjänst.[40] Den valideringstjänst som finansierats av Vinnova har etablerats inom SUNET (Swedish University Computer Network), som är en del av Vetenskapsrådet, för användning av universitet och högskolor. DIGG har även angett att de har som mål att under åren 2021 till 2022 ta fram en valideringstjänst.[41]

8.4.2 Myndigheten för digital förvaltning ska tillhandahålla en nationell valideringstjänst

Utredningens förslag: Myndigheten för digital förvaltning ska tillhandahålla en nationell valideringstjänst. Tjänsten ska regleras i författning.

[38] Se t.ex. https://validatie.justid.nl (hämtad 2021-01-14) och www.rtr.at/TKP/was_wir_tun/vertrauensdienste/Signatur/signaturpruefung/Pruefung.en.html (hämtad 2021-01-14).
[39] *reboot – omstart för den digitala förvaltningen* (SOU 2017:114), s. 385 f.
[40] www.vinnova.se/p/arkiveringsbara-digitala-underskrifter/ (hämtad 2021-01-14).
[41] DIGG, *Uppdrag om stödjande åtgärder vid nationellt införande av eIDAS-förordningen* (dnr 2019-90), s. 20.

Skälen för utredningens förslag

Sett till vad som framkommit inom ramen för vårt kartläggningsarbete anser vi att behovet av en förvaltningsgemensam valideringstjänst kvarstår och därtill har stärkts sedan Utredningen om effektiv styrning av nationella digitala tjänster lämnade sitt förslag. Mot denna bakgrund föreslår vi att DIGG ska tillhandahålla en nationell valideringstjänst. Det har under vårt kartläggningsarbete inte framkommit skäl att göra användningen av valideringstjänsten tvingande och det ska därför vara upp till respektive aktör att avgöra om de vill nyttja tjänsten.

Behov av författningsreglering

I motsats till det förslag som lämnades av Utredningen om effektiv styrning av nationella digitala tjänster anser vi att den nationella valideringstjänsten bör regleras i författning. Reglering av tjänsten i författning ger förutsättningar för transparens och förutsebarhet. Tjänsten kommer vidare att vara en viktig komponent i den gemensamma infrastrukturen som tillgodoser den offentliga förvaltningens behov och genom författningsreglering ges bättre förutsättningar för tydlig styrning inom området. Vi bedömer även att författningsreglering av tjänsten skapar bättre förutsättningar för acceptans i andra medlemsstater av sådant som tjänsten framöver eventuellt kan användas för att skapa, exempelvis valideringsintyg (se mer om sådana intyg i avsnitt 8.5.4).

Detaljreglering kopplad till tjänsten bör regleras i förordning eller myndighetsföreskrifter. Vi föreslår att det i förordning föreskrivs vad den nationella valideringstjänsten ska utföra, dvs. validera underskrifter och stämplar som inkommer respektive skapas av offentliga aktörer. Genom att reglera användningsområdet i förordning går det att i framtiden utöka eller begränsa det genom en enklare process än om det hade krävts en lagändring. Merparten av den detaljreglering av tjänsten som vi bedömer kommer vara nödvändig bör lämpligen regleras genom myndighetsföreskrifter. DIGG bör därför ha föreskriftsrätt avseende tjänsten. Hur valideringstjänsten ska fungera i detalj och vilka funktioner och gränssnitt den erbjuder användarna bör alltså enligt vår uppfattning, med beaktande av offentliga aktörers och övriga användares behov, lämnas till DIGG att närmare

bestämma. Vi kan emellertid utifrån vår kartläggning dra vissa slutsatser om vilka behov tjänsten bör tillgodose.

De behov som finns kan skilja sig åt mellan olika aktörer och mellan olika verksamhetsgrenar inom en och samma aktör. Vidare hanterar olika aktörer olika typer av uppgifter, inte sällan kan sådana uppgifter av olika anledningar bedömas som känslig. Tjänsten bör därför finnas i en central version samt i en version som går att installera lokalt. Vi kan konstatera att vissa aktörer inom förvaltningen har behov av att kunna validera automatiskt, dvs. från maskin till maskin. Det bör därför vara möjligt att utföra genom tjänsten. Det bör också vara möjligt att validera manuellt, dvs. när en användare aktivt måste utföra vissa moment för att en validering ska kunna genomföras.

8.4.3 Användning av den nationella valideringstjänsten

Utredningens förslag: Den nationella valideringstjänsten ska kunna användas av offentliga aktörer för validering av elektroniska underskrifter och stämplar samt enskilda som behöver validera elektroniskt undertecknade eller stämplade handlingar som skapats av offentliga aktörer.

Myndigheten för digital förvaltning ska ges möjlighet att ta ut en avgift för användning av valideringstjänsten.

Skälen för utredningens förslag

Till skillnad från det förslag som lämnades av Utredningen om effektiv styrning av nationella digitala tjänster anser vi utifrån de behov vi identifierat att tjänsten även bör omfatta validering av elektroniska stämplar samt validering av elektroniska underskrifter eller stämplar som är skapade i Sverige. De situationer vi anser att den nationella valideringstjänsten ska kunna användas för är när elektroniskt undertecknade eller stämplade handlingar inkommer till den offentliga förvaltningen samt när externa aktörer behöver validera elektroniskt undertecknade eller stämplade handlingar som har skapats av offentliga aktörer (se mer nedan om vilka aktörer som ingår i denna krets).

Elektroniskt undertecknade eller stämplade handlingar som inkommer till den offentliga förvaltningen kan inkomma antingen inom ramen för en e-tjänst som den aktuella aktören tillhandahåller eller via exempelvis e-post. Vår kartläggning visar att behovet av att kunna validera dessa handlingar är stort och att många aktörer upplever svårigheter eller hinder mot att kunna validera dem. För dessa situationer ska valideringstjänsten kunna användas.

Den andra situationen som valideringstjänsten ska kunna användas till är när aktörer inom förvaltningen skapar elektroniska underskrifter eller stämplar. I dessa situationer ser vi primärt att det är externa parter, exempelvis privatpersoner, företag eller andra aktörer inom förvaltningen som har behov av att kunna validera underskrifterna eller stämplarna. Det kan exempelvis vara ett elektroniskt undertecknat eller stämplat beslut av en myndighet i digital form som skickas digitalt till ett företag. Företaget kan då ha behov av att kunna validera underskriften eller stämpeln. Beslutet kan också vara av sådan karaktär att det behöver användas av tredje part, exempelvis en bank, som har ett behov av att kunna validera underskriften eller stämpeln. I sådana situationer bör den nationella valideringstjänsten kunna användas. Vi kan heller inte utesluta att det även kan finnas situationer när underskrifterna eller stämplarna måste valideras av den aktör vars tjänst har skapat dem.

Vår uppfattning är att det i dagsläget inte finns anledning att göra det tvingande för den offentliga förvaltningen att endast använda sig av elektroniska underskrifter och stämplar som går att validera i den nationella valideringstjänsten. Det kan exempelvis finnas situationer där det av olika anledningar inte är lämpligt. Vår bedömning är emellertid att möjligheten att kunna erbjuda externa parter tillfälle att använda den nationella valideringstjänsten kommer att vara ett starkt incitament för aktörer inom den offentliga förvaltningen att skapa underskrifter och stämplar som kan valideras i tjänsten.

I linje med det som framförs ovan föreslår vi att den nationella valideringstjänsten ska vara avsedd att användas dels av den offentliga förvaltningen, dels av externa parter om underskriften eller stämpeln härrör från förvaltningen. Utöver detta anser vi att kretsen som kan nyttja tjänsten bör utökas ytterligare. Anledningen till detta är att det under utredningsarbetets gång framförts att det även finns behov av att låta bl.a. privata utförare använda en nationell valideringstjänst. Framför allt inom utbildnings- och vårdsektorerna. Vad

avser frågan om vilka aktörer som ska omfattas gör utredningen följande överväganden.

Genom lagen om tillgänglighet till digital offentlig service (se mer om denna lag i avsnitt 8.1.3) uppställs krav om tillgänglighetsanpassning av webbplatser och mobila applikationer. I lagens förarbeten bedömde regeringen att tillämpningsområdet, i relation till det EU-direktiv lagen genomför i svensk rätt, skulle utvidgas till att även omfatta privata aktörer som yrkesmässigt bedriver verksamhet inom särskilt utpekade områden och som till någon del är offentligt finansierad.[42]

I en nyligen publicerad departementspromemoria föreslås att valfrihetssystem enligt lagen (2013:311) om valfrihetssystem i fråga om tjänster för elektronisk identifiering ska ersättas av auktorisationssystem för sådana tjänster och att regleringen ska utvidgas till att omfatta digital post.[43] Vidare föreslås att även samma krets privata aktörer som omfattas av lagen om tillgänglighet till digital offentlig service ska kunna få använda de tjänster för elektronisk identifiering och för digital post som tillhandahålls inom auktorisationssystemen.[44] Detta motiveras bl.a. med att den privata sektorns medverkan när det gäller digitala tjänster kan bidra till ökad användarnytta, tillväxt och innovation. I promemorian anförs vidare att stora delar av den kommunala verksamheten utförs i privat regi. De aktörer som verkar inom skolområdet, hälso- och sjukvårdsområdet samt socialtjänstområdet består till stor del av privata aktörer. Dessa behöver enligt promemorian ha samma förutsättningar att erbjuda digitala tjänster som de offentliga aktörer som verkar inom samma område.[45] Ytterligare en aspekt som lyfts fram i promemorian är att för att dessa aktörer ska kunna tillhandahålla digital service i form av digitala tjänster och digitala utskick krävs att de har tillgång till tjänster för elektronisk identifiering och för digital post. En fördel med att låta samma, tydligt definierade, krets som omfattas av kraven på tillgänglighet till digital offentlig service använda tjänster inom auktorisationssystem är enligt promemorian att de privata utförare som omfattas av kraven därmed får möjlighet att erbjuda denna service på

[42] Prop. 2017/18:299 s. 33.
[43] Promemoria *Auktorisationssystem för elektronisk identifiering och för digital post*, 21 december 2020, s.1.
[44] A.a. s. 29.
[45] A.a. s. 30.

samma villkor som de utförare som bedriver sin verksamhet i offentlig regi.[46] Vi anser att den ovan redovisade argumentationen även kan tillämpas på åtkomsten till den nationella valideringstjänsten. Framför allt med beaktande av att det medför att alla utförare av offentligt finansierad verksamhet ges möjlighet att erbjuda offentlig service med hjälp av digitala tjänster på lika villkor. Mot denna bakgrund anser vi att samma krets aktörer som omfattas av kraven i lagen om tillgänglighet till digital offentlig service ska kunna använda tjänsten och att de på samma sätt som i den lagen tillsammans med myndigheterna som omfattas samlat ska benämnas offentliga aktörer.

Den krets av privata aktörer som ges tillgång till valideringstjänsten blir då privata aktörer inom vissa områden som yrkesmässigt bedriver verksamhet som till någon del är offentligt finansierad. Med offentlig finansiering avses ett direkt stöd eller betalning från det allmänna för att driva verksamheten. Det kan t.ex. vara fråga om bidrag till skolor med enskild huvudman som ges med stöd av skollagen, ersättning som ges med stöd av lagen (1993:1651) om läkarvårdsersättning eller verksamhet som upphandlas av det allmänna av privata utförare. Ett krav bör vara att finansieringen är kopplad till själva driften av verksamheten. Om viss ekonomisk ersättning från det allmänna inte avser själva driften av verksamheten bör alltså ersättningen inte medföra att verksamheten anses vara offentligt finansierad.[47] Att verksamheten är yrkesmässigt bedriven innebär att verksamheten bedrivs kontinuerligt och i förvärvssyfte.[48]

De aktörer som omfattas är de som bedriver verksamhet som

- aktören bedriver i egenskap av enskild huvudman inom skolväsendet eller huvudman för en sådan internationell skola som avses i 24 kap. skollagen (2010:800),
- utgör hälso- och sjukvård enligt hälso- och sjukvårdslagen (2017:30) eller tandvård enligt tandvårdslagen (1985:125), eller
- bedrivs enligt socialtjänstlagen (2001:453), lagen (1988:870) om vård av missbrukare i vissa fall, lagen (1990:52) med särskilda bestämmelser om vård av unga, lagen (1993:387) om stöd och service till vissa funktionshindrade eller utgör personlig assistans som utförs med assistansersättning enligt 51 kap. socialförsäkringsbalken.

[46] A.a. s. 31 f.
[47] Prop. 2016/17:31 s. 28.
[48] Prop. 2017/18:299 s. 87.

Därtill omfattas enskilda utbildningsanordnare med tillstånd att utfärda examina enligt lagen (1993:792) om tillstånd att utfärda vissa examina, och som till största delen har statsbidrag som finansiering av högskoleutbildning på grundnivå eller avancerad nivå eller för utbildning på forskarnivå.

Att erbjuda möjlighet att använda tjänsten till samma krets aktörer som omfattas av kraven i lagen om tillgänglighet till digital offentlig service innebär att även offentligt styrda organ omfattas. Med offentligt styrt organ avses en sådan juridisk person som tillgodoser behov i det allmännas intresse, under förutsättning att behovet inte är av industriell eller kommersiell karaktär och som uppfyller vissa krav avseende finansiering, kontroll eller styrelserepresentation.[49]

DIGG bör ges möjlighet att ta ut en avgift för användning av valideringstjänsten. Vi anser dock inte att avgifter ska tas ut för enskildas validering av underskrifter och stämplar som skapats av offentliga aktörer. Vi anser vidare att möjligheten att ta ut avgifter av offentliga aktörer inte bör användas, i vart fall inte inledningsvis. Detta då det kan motverka användning av tjänsten och således även inverka negativt på de nyttor som den kan medföra för den offentliga förvaltningen.[50]

Eftersom vi inte föreslår en tjänst som är avsedd att användas för andra typer av validering än som anges ovan kommer det krävas lämpliga lösningar för att säkerställa att dessa begränsningar upprätthålls. Även om vi inte föreslår en valideringstjänst som är öppen för alla på så sätt som finns i vissa andra av EU:s medlemsstater kan vi inte utesluta att det finns behov av en allmänt tillgänglig valideringstjänst. Sådan användning av valideringstjänsten får emellertid anses falla utanför vårt uppdrag att föreslå.

[49] Se mer om definitionen av offentligt styrt organ i prop. 2017/18:299 s. 30 f.
[50] Se DIGG m.fl. *Delredovisning – Uppdrag att etablera en förvaltningsgemensam digital infrastruktur för informationsutbyte* (AD 2019:582), 29 januari 2021, s. 51 ff. för ett mer utvecklat resonemang kring nackdelarna med avgiftsuttag för förvaltningsgemensamma tjänster.

8.4.4 Tillitsförteckningen, format och erkännande av underskrifter och stämplar

Utredningens förslag: Den nationella valideringstjänsten ska kunna validera underskrifter och stämplar som har skapats av betrodda tjänster i den svenska tillitsförteckningen samt förteckningar i andra länder som upprättats i enlighet med artikel 22 i eIDAS-förordningen.

Utredningens bedömning: Den nationella valideringstjänsten bör kunna validera olika format.

Valideringstjänsten bör utformas på ett sådant sätt att underskrifter och stämplar kan valideras även från utlandet.

Skälen för utredningens förslag och bedömning

Det finns tekniska aspekter och aspekter kopplade till tillit att ta hänsyn till vid framtagandet av tjänsten. För att tjänsten ska fungera ändamålsenligt behöver den kunna avgöra vilka tillhandahållare och i förlängningen betrodda tjänster som det går att lita på. På EU-nivå finns som nämnts tidigare medlemsstaternas tillitsförteckningar. Tjänsten bör enligt vår bedömning som utgångspunkt förlita sig på dessa. Det innebär att vårt förslag att utöka den svenska tillitsförteckningen blir viktigt för validering av svenska underskrifter. Om den svenska tillitsförteckningen utökas till att omfatta även icke kvalificerade tillhandahållare av betrodda tjänster kommer exempelvis avancerade elektroniska underskrifter, som är skapade av tjänster som tillhandahålls av dessa aktörer, att kunna valideras genom valideringstjänsten. Genom att ha tillitsförteckningen som utgångspunkt kommer utländska elektroniska underskrifter och stämplar att kunna valideras i tjänsten, dock primärt sådana som är kvalificerade eftersom den absoluta merparten av de tillhandahållare och tjänster som är uppförda på andra medlemsstaters tillitsförteckningar är kvalificerade. Som framgår av avsnitt 8.3.1 är vår bedömning att användning av den infrastruktur och det ramverk som redan finns på europeisk nivå, i och med tillitsförteckningen, minskar risken för negativ påverkan på den inre marknaden i dessa avseenden. Det kan emellertid enligt vår uppfattning finnas behov hos enskilda aktörer inom för-

valtningen att kunna validera underskrifter och stämplar som har skapats av tjänster som inte finns med i tillitsförteckningen, detta borde vara möjligt vid användning av lokalt installerade versioner av valideringstjänsten.

Enligt vår bedömning bör tjänsten kunna hantera och validera olika tekniska format och specifikationer. Mot bakgrund av att den offentliga förvaltningen behöver kunna hantera de format och specifikationer som anges i kommissionens genomförandebeslut (EU) 2015/1506 bör tjänsten kunna validera dessa. På så sätt säkerställs att den svenska offentliga förvaltningen lever upp till kraven i artikel 27 och 37 i eIDAS-förordningen om att erkänna dessa format. Även andra format och specifikationer kan emellertid vara aktuella för valideringstjänsten. Vilka format tjänsten kan validera bör lämnas till DIGG att ange i myndighetsföreskrifter.

Vår bedömning är vidare att valideringstjänsten har potential att kunna öka möjligheterna för aktörer i den offentliga förvaltningen att få de underskrifter och stämplar som används erkända av aktörer i andra medlemsstaters offentliga förvaltningar. Detta eftersom det av artikel 2 och 4 i kommissionens genomförandebeslut (EU) 2015/1506 föreskrivs att en medlemsstat som begär en avancerad elektronisk underskrift eller en avancerad elektronisk underskrift, respektive stämpel, som är baserad på ett kvalificerat certifikat ska erkänna andra format av elektroniska underskrifter än de som listas i beslutet. Detta under förutsättning att den medlemsstat där tillhandahållaren av betrodda tjänster som användes av undertecknaren är etablerad erbjuder andra medlemsstater möjligheter till kostnadsfri validering av underskrift som är lämpad, när så är möjligt, för automatiserad behandling. Vår bedömning är att den nationella valideringstjänsten har potential att vara en sådan valideringstjänst som avses. Därför bör de krav som finns i genomförandebeslutet avseende möjligheter till validering (artikel 2.2 och artikel 4.2) beaktas vid framtagandet av den nationella valideringstjänsten.

8.4.5 Informationssäkerhetshetsaspekter

Valideringstjänsten kommer att vara en viktig komponent i den infrastruktur som byggs upp för betrodda tjänster och den offentliga förvaltningen i stort. Det är rimligt att anta att många aktörer inom

förvaltningen kommer att använda sig av tjänsten för validering av underskrifter och stämplar. Således är det mycket viktigt att tjänsten har en hög säkerhet och att tillgången till den inte hindras eller störs. Det är mot denna bakgrund lämpligt med säkerhetsgranskningar och penetrationstester vid etablering av tjänsten och därefter även vid omfattande förändringar av tjänsten. Vid framtagandet av tjänsten blir därför frågor om informationssäkerhet, redundans och geografisk spridning viktiga för DIGG att beakta. Med redundans menas att den finns i flera likvärdiga instanser som vid bortfall av en instans kan ta hela lasten om den andra eller någon annan instans blir otillgänglig av något skäl. Med geografisk spridning menas att det finns instanser på flera geografiska platser i landet så att bortfall av en instans på en geografisk plats inte medför otillgänglighet.

Tjänsten kan komma att hantera säkerhetsskyddskänslig information vilket även det är en viktig aspekt att väga in och bedöma vid framtagandet och tillhandahållandet av tjänsten. I detta sammanhang blir det viktigt att beakta principer om t.ex. dataminimering. Det finns enligt vår uppfattning skäl som talar för att aktörer inom förvaltningen som har för avsikt att validera underskrifter och stämplar där handlingarna innehåller särskilt känslig information bör använda sig av en lokalt installerad version av valideringstjänsten.

8.4.6 Behandling av personuppgifter

Utredningens förslag: Stöd för nödvändning behandling av personuppgifter i den nationella valideringstjänsten ska föreskrivas i lag.

Skälen för utredningens förslag

En viktig fråga som kommer att behöva hanteras vid en eventuell realisering av valideringstjänsten är hur personuppgifter behandlas samt hur ansvarsfördelningen ska se ut. Vad som utgör en personuppgift definieras i 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 (allmän

dataskyddsförordning), härefter kallad dataskyddsförordningen. Av artikel 4.1 i dataskyddsförordningen följer att en personuppgift är varje upplysning som avser en identifierad eller identifierbar fysisk person, varvid en identifierbarfysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet. Personuppgiftsansvarig är enligt artikel 4.7 i dataskyddsförordningen en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter; om ändamålen och medlen för behandlingen bestäms av unionsrätten eller medlemsstaternas nationella rätt kan den personuppgiftsansvarige eller de särskilda kriterierna för hur denne ska utses föreskrivas i unionsrätten eller i medlemsstaternas nationella rätt.

Behandling av personuppgifter kan komma att aktualiseras främst vid validering av elektroniska underskrifter eftersom underskriften ska vara knuten till undertecknaren, dvs. en viss person. Beroende på utformning av tjänsten kan även behandling av de undertecknade eller stämplade handlingarnas innehåll komma att ske.

Den ena typen av användning vi ser framför oss är som tidigare nämnts validering av undertecknade och stämplade handlingar som inkommer till en offentlig aktör. För de handlingar som har lämnats in till aktören är den personuppgiftsansvarig vid behandling av de aktuella personuppgifterna. Validering i tjänsten kommer alltid att ske på uppdrag av respektive offentlig aktör och det är på så sätt inte en självständig process. Vår bedömning är att DIGG i egenskap av tillhandahållare av tjänsten måste anses vara personuppgiftsbiträde och inte personuppgiftsansvarig i en sådan situation. Ett personuppgiftsbiträde är enligt artikel 4.8 i dataskyddsförordningen en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning.

Mot den bakgrunden kommer det att behövas ett personuppgiftsbiträdesavtal mellan den offentliga aktören och DIGG. Ett sådant avtal skulle kunna ingås i samband med att aktören ges tillgång till tjänsten. Vid användning av förvaltningsgemensamma tjänster är det inte ovanligt att det är personuppgiftsbiträdet, som också kan vara

den part som utvecklar och förvaltar tjänsten i fråga, som utformar personuppgiftsbiträdesavtalen.[51] Det förefaller rimligt att denna modell används gällande den nationella valideringstjänsten.

Vi bedömer därför att det inte behövs något särskilt författningsstöd avseende DIGG och personuppgiftsbehandlingen i dessa situationer. Varje offentlig aktör som avser att behandla personuppgifter med stöd av valideringstjänsten måste själv säkerställa att den har stöd för behandlingen, t.ex. i aktuell registerförfattning.

För underskrifter som skapas av en offentlig aktör kan situationen emellertid vara en annan om underskriften skickas till en extern part, t.ex. om ett elektroniskt undertecknat beslut skickas som ett PDF-dokument till en privatperson. Om en enskild person vill validera underskriften kan det saknas en aktör som är personuppgiftsansvarig. DIGG kan i dessa situationer då bli personuppgiftsansvarig. Att myndigheten ska tillhandahålla den nationella valideringstjänsten kommer att föreskrivas i författning, likaså att det i tjänsten bl.a. ska gå att validera elektroniska underskrifter. Det går därför att argumentera för att eventuell personuppgiftsbehandling har stöd i och med att det grundar sig i en sådan rättslig förpliktelse som anges som rättslig grund för personuppgiftsbehandling i artikel 6.1 c i dataskyddsförordningen. Vi anser emellertid att det för tydlighetens skull bör föreskrivas i lag att personuppgifter får behandlas och att det endast får ske i den mån det är nödvändigt för att kunna validera den aktuella underskriften. Den författningsreglering vi föreslår avser endast den eventuella personuppgiftsbehandling DIGG kommer att utföra.

Behandling av personuppgifter av DIGG kan också bli aktuellt beroende på vilken lösning som används för att ge tillgång till valideringstjänsten. Eftersom vi föreslår att myndigheten genom myndighetsföreskrifter fastställer villkoren för användning kan vi inte bedöma vilka uppgifter som kan komma att behandlas och hur. Vi föreslår dock att det i lag föreskrivs att personuppgifter får behandlas för detta ändamål i den mån det är nödvändigt.

Vid framtagandet av den nationella valideringstjänsten måste det även säkerställas att tillämpliga bestämmelser och principer avseende skydd för behandling av personuppgifter beaktas och att tjänsten lever upp till dem.

[51] *Juridik som stöd för förvaltningens digitalisering* (SOU 2018:25), s. 109 f.

8.4.7 Offentlighet och sekretess

Utredningens bedömning: Validering av elektroniska underskrifter och stämplar i den nationella valideringstjänsten bör omfattas av undantagen för teknisk bearbetning och lagring i 2 kap. 13 § första stycket tryckfrihetsförordningen respektive 11 kap. 4 a § och 40 kap. 5 § offentlighets- och sekretesslagen (2009:400).

Skälen för utredningens bedömning

Hur regelverken för offentlighet och sekretess påverkar användning av den nationella valideringstjänsten går enligt vår uppfattning inte att besvara fullt ut eftersom detaljerade bestämmelser om tjänsten rörande dess funktion och villkor för användning ännu inte är framtagna. Det är däremot möjligt att göra vissa allmänna bedömningar utifrån vårt förslag.

Allmänhetens rätt till tillgång till allmänna handlingar (handlingsoffentligheten) är grundlagsskyddad och regleras i 2 kap. tryckfrihetsförordningen (TF). Syftet med bestämmelserna är i huvudsak att ge allmänheten insyn i myndigheternas verksamhet. Handlingen är enligt 2 kap. 4 § TF allmän om den förvaras hos en myndighet och är inkommen till eller upprättad hos myndigheten.

De undertecknade eller stämplade handlingar som aktörer inom den offentliga förvaltningen önskar validera genom tjänsten kommer att vara inkomna till den aktuella aktören och således som huvudregel vara att anse som allmänna. Om underskriften eller stämpeln ska valideras i valideringstjänsten kommer emellertid även DIGG hantera sådana handlingar eller delmängder av deras innehåll. Av 2 kap. 13 § första stycket TF framgår att en handling som förvaras hos en myndighet endast som ett led i en teknisk bearbetning för någon annans räkning inte anses som allmän handling hos den myndigheten. Vi bedömer att valideringen av underskriften eller stämpeln bör utgöra en sådan teknisk bearbetning som skulle innebära att handlingen inte anses som inkommen hos DIGG. Detsamma bör gälla om en aktör vars verksamhet till någon del är offentligt finansierad vill validera en underskrift eller en stämpel, eftersom förvaringen hos DIGG även då utgör ett led i teknisk bearbetning för någon annans räkning. Det beror emellertid, som påpekas ovan, på hur tjänsten och

villkoren för användningen utformas. Samma resonemang bedömer vi är relevant i de fall enskilda vill validera en underskrift eller stämpel som är skapad av en aktör i den offentliga förvaltningen och tjänsten är skapad på ett sådant sätt att användaren som ska validera kan anses ha tillgång till ett s.k. eget utrymme.[52]

Uppgifter hos myndigheter kan omfattas av sekretess. Sekretess gäller som huvudregel även mellan myndigheter och en myndighet får i ett sådant läge inte lämna uppgiften till en annan myndighet om detta inte medges särskilt. I 11 kap. 4 a § offentlighets- och sekretesslagen (2009:400, OSL) finns emellertid en bestämmelse som likt bestämmelsen i tryckfrihetsförordningen ovan medger undantag för teknisk bearbetning och lagring. Tillämpningsområdet för bestämmelsen är detsamma som för undantagsbestämmelsen i tryckfrihetsförordningen.[53] Bestämmelsen gäller emellertid enligt 11 kap. 8 § OSL inte om en primär sekretessbestämmelse redan är tillämplig på uppgifterna hos den mottagande myndigheten. I sådant fall ska i stället den primära sekretessbestämmelsen tillämpas.

Av 11 kap. 4 a § OSL följer att om en myndighet i verksamhet för enbart teknisk bearbetning eller teknisk lagring för en annan myndighets räkning får en uppgift som hos den senare myndigheten är sekretessreglerad av hänsyn till ett allmänt intresse, blir sekretessbestämmelsen tillämplig även hos den mottagande myndigheten. Det skydd som kan aktualiseras när sekretessen överförs med stöd av bestämmelsen är en tystnadsplikt, som ska gälla både i samband med digitala tjänster som en myndighet tillhandahåller åt en annan myndighet och vid en myndighets utkontraktering av it-drift till en annan myndighet. Bestämmelsen är även tillämplig på uppgifter som den mottagande myndigheten får av enskilda och andra myndigheter än beställarmyndigheten för den senare myndighetens räkning.[54]

Av 40 kap. 5 § OSL framgår vidare att sekretess gäller i verksamhet för enbart teknisk bearbetning eller teknisk lagring för någon annans räkning för uppgift om en enskilds personliga eller ekonomiska förhållanden. Bestämmelsen är inte begränsad till att endast

[52] Eget utrymme definieras som ett skyddat förvar som tillhandahålls enligt 2 kap. 10 § första stycket TF endast som led i teknisk bearbetning eller teknisk lagring för annans räkning (eSam, *Juridisk vägledning för verksamhetsutveckling inom e-förvaltning 3.0, s.* 10). Se också prop. 2016/17:198 s. 6 f. och s. 17.
[53] Prop. 2016/17:198 s. 28.
[54] A.a.

gälla när en myndighet tekniskt bearbetar eller tekniskt lagrar åt en annan myndighet (jfr resonemang ovan om för annans räkning).[55]

Att uppgifter omfattas av sekretess utgör sammanfattningsvis inte något hinder mot användning av valideringstjänsten. För det fall en aktör av någon anledning ändå inte vill överföra uppgifter som omfattas av sekretess kan, i stället för den centrala tjänsten, en lokalt installerad version av valideringstjänsten användas.

8.5 Bevarande

8.5.1 Den offentliga arkivsektorn

Den offentliga arkivsektorn utgörs av alla myndigheter och organ som hanterar eller förvarar allmänna handlingar samt av riksdagen, kommunfullmäktige och regionfullmäktige.[56] Den gemensamma nämnaren för den offentliga arkivsektorn är allmänna handlingar. Samtliga arkiv som utgörs av allmänna handlingar omfattas av arkivlagens (1990:782) bestämmelser.

Samtliga myndigheter, dvs. i stat, kommun och region, är arkivbildare. Myndigheterna har en pågående arkivbildning och arkivtillväxt. Till den offentliga arkivsektorns arkivbildare hör även vissa andra organ och sådana juridiska personer där kommuner eller regioner utövar ett rättsligt bestämmande.

Den offentliga arkivsektorn står under översyn och tillsyn av arkivmyndigheter. Det finns en statlig arkivmyndighet, Riksarkivet, och en arkivmyndighet i varje kommun och region. I kommunerna och regionerna hanteras det praktiska arbetet i regel av kommunala myndigheter på uppdrag av arkivmyndigheten. Ofta benämns de förvaltningarna för kommunarkiv (stadsarkiv) eller regionarkiv.

Utöver arkivmyndigheterna finns även Samrådsgruppen för kommunala arkivfrågor (SKA). SKA, vars huvudmän är Riksarkivet och SKR, är ett samverkansorgan för stat, kommuner och landsting inom arkivområdet. SKA utarbetar bl.a. råd om bevarande och gallring inom en rad kommunala områden.[57]

[55] *Säker och kostnadseffektiv it-drift* (SOU 2021:1), s. 268 f.
[56] Se *Härifrån till evigheten. En långsiktig arkivpolitik för förvaltning och kulturarv* (SOU 2019:58), s. 148 ff. för en mer utförlig redogörelse för den offentliga arkivsektorn.
[57] www.samradsgruppen.se/index.php/om-samradsgruppen (hämtad 2021-01-14).

8.5.2 Arkivlagens ändamål

Av 3 § första stycket arkivlagen (1990:782) följer att en myndighets arkiv bildas av de allmänna handlingarna från myndighetens verksamhet och sådana handlingar som avses i 2 kap. 12 § tryckfrihetsförordningen och som myndigheten beslutar ska tas om hand för arkivering. Av tredje stycket samma paragraf framgår att myndigheternas arkiv ska bevaras, hållas ordnade och vårdas så att de tillgodoser

1. rätten att ta del av allmänna handlingar,
2. behovet av information för rättskipningen och förvaltningen, och
3. forskningens behov.

Av punkterna ovan framgår de grundläggande syften som arkivbildningen avser uppfylla. I lagens förarbeten motiveras det i första punkten angivna syftet med att rätten av att ta del av allmänna handlingar reducerats högst väsentligt om sådana handlingar inte bevarades. Motivet till den andra punkten är att det är viktigt för både rättstillämpningen och förvaltningen att det går att ta del av äldre avgöranden så att praxis blir likformig. När det gäller forskningens behov som lyfts fram i tredje punkten avses såväl den professionella forskningen som amatörforskningen. Av lagens förarbeten framgår även att forskningen och kulturen är så intimt sammanknippande att kulturens behov får anses ingå i forskningens behov.[58]

Lagstiftaren understryker i förarbetena att det för att uppnå de ovan angivna syftena inte är tillräckligt att arkivmaterialet bara bevaras. Det ska även – som framgår av början av tredje stycket – vårdas och hållas ordnade med dessa syften för ögonen. Som huvudregel ska arkivmaterial bevaras för all framtid.[59] Handlingen ska även bevaras i ursprungligt skick. Med detta avses att handlingar bevaras så som de var när de kom in till eller upprättades hos myndigheten.[60]

[58] Prop. 1989/90:72 s. 70.
[59] A.a.
[60] Riksarkivet, *Elektroniskt underskrivna handlingar* (Rapport 2006:1), s. 33.

Begreppet gallring

Huvudregeln är att allmänna handlingar ska bevaras. Det som inte bevaras gallras. Gallring får endast göras med stöd av författning eller beslut grundad i lag.

En handling kan gallras helt eller i vissa delar. Vid gallring ska dock enligt 10 § andra stycket arkivlagen alltid beaktas att arkiven utgör en del av kulturarvet och att det arkivmaterial som återstår ska kunna tillgodose de ändamål som anges i 3 § tredje stycket samma lag. Det betyder att vad som ska bevaras kan antingen avse handlingen i sig eller handlingarna tillsammans.

Det finns ingen definition av gallring i arkivlagen. Riksarkivet har dock i ett antal föreskrifter definierat gallring (RA-FS 1991:1, RA-FS 1991:6, 2006:1, RA-FS 2009:1).[61]

I Riksarkivets föreskrifter om elektroniska handlingar definieras gallring som att förstöra allmänna handlingar eller uppgifter i allmänna handlingar, eller vidta andra åtgärder med handlingarna som medför

- förlust av betydelsebärande data,
- förlust av möjliga sammanställningar,
- förlust av sökmöjligheter, eller
- förlust av möjligheter att bedöma handlingars autenticitet.[62]

Definitionen av att gallra tar hänsyn till olika åtgärder som kan påverka de ursprungliga handlingarna. Det är således en vidare tolkning av gallring som anpassats till hanteringen av andra slags handlingar än pappershandlingar.

För att gallring ska vara tillåten krävs det som ovan framgår att det finns stöd för detta i en författning.[63] Riksarkivet har genom arkiv-

[61] Riksarkivets föreskrifter och allmänna råd om arkiv hos statliga myndigheter, ändrade och omtryckta genom: RA-FS 1997:4, ändrade genom: RA-FS 2008:4, RA-FS 2012:1, RA-FS 2018:2, RA-FS 2019:2, Riksarkivets föreskrifter och allmänna råd om gallring av handlingar av tillfällig eller ringa betydelse, ändrade och omtryckta genom: RA-FS 1997:6, ändrade genom: RA-FS 2012:2., Riksarkivets föreskrifter och allmänna råd om handlingar på papper, ändrade genom: RA-FS 2010:2, RA-FS 2012:5, RA-FS 2018:4 och Riksarkivets föreskrifter och allmänna råd om elektroniska handlingar (upptagningar för automatiserad behandling), ändrad genom: RA-FS 2018:7.

[62] 2 kap. 1 § RA-FS 2009:1.

[63] Många bestämmelser om gallring återfinns exempelvis i s.k. registerförfattningar.

förordningen (1991:446) fått bemyndigande att föreskriva och besluta om gallring av allmänna handlingar hos statliga myndigheter. Riksarkivets föreskrifter och beslut om gallring finns publicerade dels i en generell föreskriftsserie (RA-FS) som gäller samtliga statliga myndigheter, dels i en myndighetsspecifik föreskriftsserie (RA-MS). För det fall det saknas författningsstöd för gallring kan myndigheter göra en framställan till Riksarkivet om att de önskar en myndighetsspecifik föreskrift.[64]

Vad avser kommuner och regioner brukar de hänvisa till definition av gallring från Riksarkivet i oförändrat skick eller med vissa justeringar. Kommuner och regioner kan således ha egna definitioner av vad som utgör gallring.[65]

Begreppen bevarande och ursprungligt skick

Som tidigare nämnts är huvudregeln att handlingar ska bevaras i ursprungligt skick. Således är en handling som inte gallras i ursprungligt skick.

Likt gallring definieras inte bevarande i arkivlagen.[66] Det framgår dock indirekt av 5 och 6 §§ arkivlagen att bevarandet är något mer än själva överförandet av handlingarna till arkivlokalen eller e-arkivet. Att bevara innebär att se till att handlingar och uppgifter har tekniska förutsättningar för att kunna bevaras genom t.ex. format, material, metoder och förvaringsmiljö så att de ska kunna läsas, förstås och användas i framtiden.

Begreppet bevara förekommer även i eIDAS-förordningen. I artikel 34 beskrivs vem som får tillhandhålla en kvalificerad tjänst för bevarande av kvalificerade elektroniska underskrifter samt att en sådan tjänst ska använda förfaranden och tekniker som gör det möjligt att förlänga tillförlitligheten för underskrifter utöver perioden för teknisk giltighet. Genom artikel 40 gäller artikel 34 på motsvarande sätt även för stämplar. Av artikel 34 och skäl 61 i förordningens ingress går det att utläsa att begreppet bevarande inom ramen för

[64] Se mer om detta förfarande i Riksarkivets vägledning *Framställningar om myndighetsspecifika föreskrifter (RA-MS)* Version 1.2, 17 september 2019.
[65] SKA, *Vem bestämmer om arkiv i kommunen? – Råd om styrning av den kommunala arkivverksamheten*, oktober 2015, s. 23.
[66] Notera emellertid att begreppet bevarande förekommer i andra svenska författningar och där kan ha en annan innebörd än i arkivlagen, se t.ex. SKA, *Bevara eller gallra, Gallringsråd nr 9: Råd för överförmyndare*, 2020, s. 11.

eIDAS-förordningen är snävare än den svenska definitionen eftersom fokus i förordningen enbart ligger på att säkerställa den rättsliga giltigheten över tid.

8.5.3 Bevarande av elektroniskt undertecknade eller stämplade handlingar

En elektronisk handling är svårare att bevara i oförvanskat skick än en pappershandling. Det krävs också en kontinuerlig förvaltning för att handlingarna ska kunna läsas och användas även i framtiden.[67] Riksarkivet har uttryckt det som att bevarande av digitala objekt i allmänhet handlar om att bevara alla komponenter som använts för att tolka och omvandla kod till det representerade dataobjektet, och tillgång till rätt hårdvara om dataobjektet är maskinberoende. Detta innebär att man kan återställa det digitala objektet i dess ursprungliga skick och mening, vilket förutsätter att komponenternas integritet inte äventyrats.[68]

Bevarande av elektroniskt undertecknade och stämplade handlingar, i fråga om avancerade eller kvalificerade sådana, tillför ytterligare en aspekt i form av bevarandet av giltighet, dvs. att man kan validera inte bara integriteten av innehållet som underskriften avser, utan även vem som undertecknat eller vilken juridisk person som stämplat handlingen.[69] Alltså sådana kontroller som knyter an till underskriftens eller stämpelns juridiska funktioner i form av identifiering och äkthet som beskrivs i avsnitt 4.2.2 och avsnitt 4.3.2. Ett bevarande av en elektronisk underskrift eller stämpel i ursprungligt skick innebär alltså inte att giltigheten har bevarats.[70]

[67] *Härifrån till evigheten. En långsiktig arkivpolitik* (SOU 2019:58), s. 120.
[68] Riksarkivet, *Framställning och bevarande av elektroniska signaturer* (dnr RA 20-2013-1154), 7 oktober 2014, s. 77.
[69] A.a.
[70] Riksarkivet, *Framställning och bevarande av elektroniska signaturer (avsnitt 6)* (dnr RA 20-2013-1154), 29 maj 2015, s. 5.

Tidigare och pågående arbete rörande bevarande av elektroniskt undertecknade handlingar

Ända sedan användningen av elektroniska underskrifter började aktualiseras inom den offentliga förvaltningen har frågan om hur dessa underskrifter ska bevaras hanterats parallellt.[71] Ett viktigt steg i hur frågan ska hanteras togs 2006 då Riksarkivet publicerade rapporten *Elektroniskt underskrivna handlingar*.[72] I rapporten behandlas bl.a. frågor som är av betydelse för bevarande och gallring av elektroniskt undertecknade handlingar inom ramen för myndigheternas e-tjänster.

En viktig fråga som belystes i rapporten är om en elektroniskt undertecknad handling ska ses som en eller flera olika handlingar. Riksarkivet anger i rapporten att en elektroniskt undertecknad handling består av flera delar. Data som representerar texten utgör endast en del av den färdiga handlingen. När texten skrivs under elektroniskt kompletteras den med ett hashvärde som krypteras med undertecknarens privata nyckel och knyts till texten. I funktionellt hänseende kan det krypterade hashvärdet sägas utgöra den elektroniska underskriften genom att den knyter texten till en bestämd utställare. Den elektroniskt undertecknade handlingen består således av en helhet som är definierad till innehåll och struktur. Alla delar behövs för att mottagaren ska kunna ta del av texten och kontrollera att uppgiften om utställare är riktig och att texten inte har förvanskats efter det att handlingen undertecknades. De beskrivna delarna utgör enligt Riksarkivet tillsammans en handling, i enlighet med 2 kap. 3 § TF. Den del av handlingen som utgör underskriften kan visserligen inte presenteras i läsbar form men den kan uppfattas.[73] Det finns emellertid en del uppgifter som behövs för kontroll av en elektroniskt undertecknad handling som kommer in till eller upprättas hos myndigheten och som inte utgör en del av handlingen.[74] Den bedömning som gjordes av Riksarkivet 2006 får än i dag anses vara det vedertagna synsättet.[75] Vi ansluter oss även till denna bedömning.

[71] Se bl.a. *Digitala signaturer – en teknisk och juridisk översikt* (Ds 1998:14), 92 f. och *Formel – Formkrav och elektronisk kommunikation* (Ds 2003:29), s. 28 och Statskontorets rapport *Elektroniska urkunder* (2003:13).
[72] Riksarkivet, *Elektroniskt underskrivna handlingar* (Rapport 2006:1).
[73] A.a. s. 19 ff.
[74] A.a. s. 39. Notera att det även kan finns kontrollmaterial som inte inkommer eller upprättas utan som kräver aktiva åtgärder för att säkra.
[75] Se bl.a. eSam, *Juridisk vägledning för införande av e-legitimering och e-underskrifter 1.1*, juni 2018, s. 53.

I rapporten beskrivs vidare hur flera myndigheter, efter att validering utförts, som bevis på att denna kontroll utförts stämplar handlingen elektroniskt. Stämpeln är ingen garanti för att handlingen ska förbli oförvanskad och bevarad i ursprungligt skick. Den kan däremot användas för att kontrollera om förvanskning har skett efter att den initiala kontrollen gjordes. I rapporten liknas en sådan stämpel med en traditionell ankomststämpel.[76]

När en handling stämplas skapas i praktiken en ny handling där den ursprungliga handlingen ingår tillsammans med andra uppgifter. Här avses uppgifter som hämtats ur den ursprungliga handlingen, från utfärdaren av certifikatet och från myndighetens it-system, t.ex. uppgifter om ingivare, tidpunkt för inkommande, handlingens innehåll i klartext, utfallet av kontrollen, samt handlingen i sitt ursprungliga format.[77]

År 2009 beslutade Riksarkivet om två generella föreskrifter rörande elektroniska handlingar: Riksarkivets föreskrifter och allmänna råd om elektroniska handlingar (RA-FS 2009:1) och Riksarkivets föreskrifter och allmänna råd om tekniska krav för elektroniska handlingar (RA-FS 2009:2). Av 3 kap. 5 § RA-FS 2009:2 framgår att elektroniska handlingar som är elektroniskt undertecknade, och som tillkommer inom ramen för e-tjänster, ska följa vissa tekniska krav.[78]

Inom ramen för Riksarkivets projekt ArkivE publicerades år 2014 respektive 2015 två rapporter om framställning och bevarande av elektroniska underskrifter.[79] Något som lyftes fram i den senare rapporten var att den metod med myndighetsstämpling som presenterades i rapporten från 2006 kan behöva upprepas över tid genom s.k. rekursiv stämpling.[80]

---

[76] Riksarkivet, *Elektroniskt underskrivna handlingar* (Rapport 2006:1), s. 25.
[77] A.a.
[78] IETF RFC 2315 PKCS #7: Cryptographic Message Syntax Version 1.5 eller XML-signatures för strukturerade dokument i XML (Extensible Markup Language). Det kan i sammanhanget nämnas att ETSI år 2012 tog fram en standard för långtidsbevarande (ETSI TS 103 172 V2.1.1 (2012-03). Denna standard bygger på CMS och XML-signature samt PDF-signature. De ovan beskrivna underskriftsformaten från internationella standardiseringsorganisationer är grunden för ETSI:s underskriftsformat. CMS/PKCS#7 är grunden för CaDES, XML-signature är grunden för XaDES och PDF-signature grunden för PaDES.
[79] Riksarkivet, *Framställning och bevarande av elektroniska signaturer* (dnr RA 20-2013-1154), 7 oktober 2014 och Riksarkivet, *Framställning och bevarande av elektroniska signaturer (avsnitt 6)* (dnr RA 20-2013-1154), 29 maj 2015.
[80] Riksarkivet, *Framställning och bevarande av elektroniska signaturer* (dnr RA 20-2013-1154), 7 oktober 2014, s. 79.

För närvarande bedriver Riksarkivet ett arbete benämnt FormatE som ser över de tekniska kraven i RA-FS 2009:2, vilket innefattar standarder för elektroniska underskrifter. SKA har även påbörjat en förstudie för att utforska vilka specifika frågeställningar som är i fokus hos kommuner och regioner avseende att använda och hantera underskrifter i offentliga verksamheter. Förstudien ska sedan ligga till grund för att ta fram lämpliga råd och stöd.[81]

Den grundläggande problematiken vid bevarande av handlingar som försetts med en avancerad eller kvalificerad elektronisk underskrift eller stämpel

Den grundläggande problematiken vid bevarande av elektroniska underskrifter och stämplar av viss nivå utgörs enkelt uttryckt av att en elektronisk underskrift eller stämpel som tillfogas en elektronisk handling har ett ”bäst före-datum”. Efter det att ”bäst-före datumet” utgått kan t.ex. inte en avancerad elektronisk underskrift eller stämpel påvisas vara mer särpräglad än annan digital information. Det krävs därför vad Riksarkivet benämnt som ”yttre legitimitet” för att påvisa att informationen var i ursprungligt skick.[82] Den yttre legitimiteten följer av att den undertecknade handlingens giltighet kontrolleras genom valideringen.

Den begränsade tekniska livslängden för elektroniskt undertecknade eller stämplade handlingar har två orsaker. Den ena orsaken till den begränsade tekniska livslängden är att åtkomst till de spärrlistor som fanns hos certifikatutfärdaren vid tidpunkten för underskriften eller stämplingen inte längre är tillgängliga. Hänvisningar och länkar till certifikatregister, spärrlistor och liknande kan alltså finnas kvar i handlingen och handlingens integritet vara intakt. Men den handling som de hänvisar till kan vara borta.

Den andra orsaken är att ökad processorkraft och matematiska genombrott på sikt komprometterar den kryptering som ligger till grund för underskriften och stämpeln. Antagandet att det med tiden går att knäcka all kryptering har använts som argument mot ett bevarande av elektroniskt undertecknade handlingar. Denna uppskatt-

[81] www.samradsgruppen.se/index.php/component/phocadownload/category/10-konferenser?download=268:inledning-benjamin-yousefi (hämtad 2021-01-14).
[82] Riksarkivet, *Framställning och bevarande av elektroniska signaturer (avsnitt 6)* (dnr RA 20-2013-1154), 29 maj 2015, s. 5 f.

ning utgår från hur rekommendationerna om användning av enskilda algoritmer eller nyckelängder uppdateras.

Gällande vad som krävs för att bevara en elektronisk underskrift eller stämpel är dels fråga om vad som inte får gallras, dels fråga om vad som aktivt måste göras, exempelvis att inhämta spärrlistor eller validera.

Arkivförfattningarna ställer inte krav på att kontroller av inkomna handlingars äkthet ska utföras. Några krav uppställs inte heller på att myndigheter ska inhämta handlingar från andra aktörer för att säkerställa möjligheterna till kontroll på kort och lång sikt. Däremot följer det av arkivförfattningarna att handlingar som faktiskt har kommit in till en myndighet inom ramen för en e-tjänst, t.ex. handlingar som har inhämtats för äkthetskontrollen, bevaras om det inte följer av föreskrifter eller beslut att gallring får ske.[83] Eftersom vissa kontrollfunktioner är en del av handlingen som ska bevaras i ursprungligt skick går det emellertid inte utan författningsstöd för gallring att enbart bevara texten i den undertecknade eller stämplade handlingen. Även efter att den initiala kontrollen har skett ska handlingen därför som huvudregel kunna tillgodose allmänhetens, förvaltningens, rättskipningens och forskningens behov av oförvanskad information.[84]

Utöver den grundläggande problematik som beskrivs ovan finns även vissa svårigheter på mer teknisk detaljnivå kopplat till bevarande av elektroniska underskrifter och stämplar.

8.5.4 Metoder för att bevara elektroniskt undertecknade och stämplade handlingars giltighet

Utredningens förslag: Riksarkivet och Myndigheten för digital förvaltning ska få i uppdrag att utreda förutsättningarna för att använda valideringsintyg som metod för att bevara undertecknade eller stämplade handlingars giltighet. Myndigheterna ska även utreda förutsättningarna för att valideringsintygen skapas inom ramen för den nationella valideringstjänsten.

[83] Riksarkivet, *Elektroniskt underskrivna handlingar* (Rapport 2006:1), s. 32.
[84] A.a. s. 29.

Skälen för utredningens förslag

Ett sätt att hantera den problematik med att bevara giltighet som beskrivs i avsnitt 8.5.3 är ett bestyrkande av kontrollfunktionen. Som framgår av samma avsnitt är att stämpla handlingen och dess valideringsdata med myndighetens elektroniska stämpel en sådan kompletterande åtgärd som en myndighet kan företa i detta syfte. Eftersom dessa stämplar bygger på samma teknologi som den undertecknade eller stämplade handling som stämplas kommer man med denna lösning dock inte helt runt den grundläggande problematiken med tidsbegränsad giltighet.[85] Som ett sätt att komma runt detta har Riksarkivet anfört att s.k. rekursiv tidsstämpling kan användas som ett sätt att bestyrka handlingen. Detta innebär att handlingen innan tidpunkten då kontrollfunktionen upphör att vara giltig, och om handlingen inte ska gallras senast vid den tidpunkten, måste förses med en ny stämpel och att detta resulterar i en kedja som kan följas för att utreda giltigheten av en underskrift eller stämpel. Metoden grundar sig i tekniska specifikationer från ETSI.[86]

DIGG har som lösning på problematiken med att behöva hantera kedjor av certifikat lyft fram användningen av s.k. valideringsintyg.[87] Detta innebär att alla eventuella certifikatskedjor koncentreras till en källa som endast behöver påvisa sin auktoritet, dvs. valideringstjänsten. Av detta följer att endast valideringsdata för valideringsintyget behövs och därigenom kan all valideringsdata för kedjan av certifikat undvikas.

Applicerat på ett förenklat fall med en handling som undertecknats med en avancerad eller kvalificerad elektronisk underskrift blir gången den följande.

- Det krypterade hashvärdet (ursprungliga elektroniska underskriften eller stämpeln) kommer alltid att bevaras och certifikatet för kontroll av utställare av den underskriften eller stämpeln kommer alltid att upphöra.

[85] Riksarkivet, *Framställning och bevarande av elektroniska signaturer (avsnitt 6)* (dnr RA 20-2013-1154), 29 maj 2015, s. 9
[86] Riksarkivet, *Framställning och bevarande av elektroniska signaturer* (dnr RA 20-2013-1154), 7 oktober 2014, s. 79 ff. och Riksarkivet, *Framställning och bevarande av elektroniska signaturer (avsnitt 6)* (dnr RA 20-2013-1154), 29 maj 2015, s. 9.
[87] DIGG, *eID för medarbetare – Förstudierapport inom byggblock Identitet i regeringsuppdraget Att etablera en förvaltningsgemensam infrastruktur för informationsutbyte* (dnr 2019-582), 14 december 2020, s. 24.

- Under den tid den underskriften eller stämpeln kan kontrolleras (dvs. innan dess certifikat upphör) kan dock ett valideringsintyg utfärdas.
- Valideringsintyget, med starkare algoritmer, beräknar hashvärdet av den handlingens underskrift eller stämpel och innehållet som den undertecknade, och krypterar hashvärdet. Valideringsintyget kan omsluta den ursprungliga handlingen.
- Valideringsintyget implementeras med en elektronisk stämpel. Eftersom säkerheten, trots den starkare krypteringen, även för denna stämpel eroderas över tid kan ett nytt valideringsintyg behöva utfärdas för att fortsatt bevara den ursprungliga underskriftens eller stämpelns giltighet.
- Valideringsintyget, med starkare algoritmer, beräknar då hashvärdet av det första valideringsintyget och innehållet som den undertecknade, och krypterar hashvärdet. Det nya valideringsintyget kan antingen innesluta eller ersätta det tidigare valideringsintyget.
- Det sista steget kan repeteras så länge giltigheten av den elektroniska handlingens underskrift eller stämpel ska bevaras.

Valideringsintyg är en metod som genom koncentrationen av certifikatkedjor underlättar skapandet av en härledningsbar kedja av bevis som kan påvisa den ursprungliga giltigheten av en underskrift eller stämpel vars kontrollfunktion inte längre kan valideras som giltig. Metoden bevarar alltså inte eller förlänger livslängden av den ursprungliga kontrollfunktionen, men bestyrker den och alla andra bestyrkanden. Eftersom det inte är en lösning som tagits fram på europeisk nivå går emellertid det inte att säga huruvida det hade accepterats för det fall en svensk myndighet hade lagt fram det som bevismedel i en domstol i en annan medlemsstat eller för den delen en domstol i ett land utanför EU. I det svenska rättssystemet där fri bevisprövning råder torde ett valideringsintyg i relation till Högsta domstolens avgörande i NJA 2017 s. 1105 och den tillämpning som identifierats i förvaltningsrättsliga och straffrättsliga mål inte utgöra något hinder mot att identifiera vem som undertecknat en viss handling (se mer om bevisverkan i avsnitt 4.2.2). Vi ser mot bakgrund av det som anförts att det, innan en myndighet inför ett system med bevarande genom valideringsintyg, bör genomföras en bedömning av

i vilka sammanhang giltigheten av en underskrift eller stämpel kan behöva bevisas och om det exempelvis kan behöva ske utomlands.

Även med beaktande av den risk som ovan anges och som kan vara aktuell för vissa myndigheter kan användandet av valideringsintyg potentiellt anses medföra sådana fördelar för den offentliga förvaltningen i stort att frågan behöver utredas vidare. Vi föreslår därför att Riksarkivet och DIGG får i uppdrag att utreda förutsättningarna för att använda valideringsintyg som metod för att bevara undertecknade och stämplade handlingars giltighet. Myndigheterna ska även utreda förutsättningarna för att valideringsintygen skapas inom ramen för den nationella valideringstjänsten.

8.5.5 Ett ökat stöd från Riksarkivet

Utredningens förslag: Riksarkivet ska få i uppdrag att utreda förutsättningarna för att införa generella bestämmelser och/eller annat stöd avseende bevarande av elektroniskt undertecknade eller stämplade handlingar.

Skälen för utredningens förslag

Som framgår av avsnitt 8.5.3 uppställer bevarande av elektroniska underskrifter och stämplar utmaningar för både arkivbildare och arkivmyndigheter.

Utöver frågan om hur elektroniskt undertecknade eller stämplade handlingars giltighet ska bevaras finns även frågan om giltigheten som sådan måste bevaras. Svaret på denna fråga beror på flera faktorer. Detta kräver en bedömning av typen av underskrift eller stämpel rent tekniskt men frågan om verksamheten måste bevara möjligheten att kunna påvisa giltigheten beror i huvudsak på handlingens funktionella skick, dvs. för vilket syfte handlingen har framställts samt hur den ska användas och hanteras. Detta innefattar bl.a. dess rättsliga sammanhang, behovet av tillförlitlighet och av data eller informationen i helhet. Vad gäller rättsligt sammanhang bör sådant som t.ex. eventuella preskriptionstider beaktas.

Innan framställning av elektroniska underskrifter eller stämplar påbörjas måste bedömning göras avseende vilken typ av underskrift

eller stämpel verksamheten behöver framställa, hur länge underskriften behöver bevaras och vilka åtgärder som måste vidtas för att bevara underskriften för den avsedda tiden.

Av betydelse är att verksamheten förstår och dokumenterat grunden för att gallra kontrollfunktionen, det vill säga att förlora möjligheten att kunna påvisa giltigheten. Anledningen är att det är tekniskt svårt att i efterhand likt andra elektroniska handlingar t.ex. konvertera eller göra andra justeringar för att bevara eller påvisa kontrollfunktionen.

Om en verksamhet framställer avancerade elektroniska underskrifter eller stämplar och inte har stöd för att gallra kontrollfunktionen bör utgångspunkten enligt vår bedömning vara att bevara även möjligheten att påvisa giltigheten om det inte finns uttryckligt stöd för en annan hantering.

För arkivmyndigheterna finns det även andra utmaningar som mer allmänt knyter an till digitaliseringens konsekvenser för arkivsektorn. Arkivutredningen gavs i uppdrag att analysera de ekonomiska konsekvenserna för Riksarkivet och andra arkivmyndigheter av den offentliga förvaltningens övergång till digitala processer. Arkivutredningen genomförde detta arbete i projektform tillsammans med Riksarkivet.[88] Ett urval av andra arkivmyndigheter samt statliga myndigheter fick möjlighet att lämna synpunkter på projektets rapport. I syfte att minska kostnaderna för att ta emot och lagra information föreslogs bl.a. att det i framtiden ska vara möjligt att föreskriva om en ökad gallring av allmänna handlingar. Förutsättningen för det är utvecklade metoder för informationsvärdering och om ökad gallring ska ske måste frågan lyftas till nationell nivå. Det framhölls att det produceras enorma mängder information i den offentliga sektorn och mängden tenderar att öka. Detta innebär dock inte enligt uppgiftslämnarna att mängden information som är värd att bevara ökar proportionerligt. Det är snarare information av tillfällig betydelse som står för merparten av ökningen. En remissinstans menar att arkivmyndigheterna kan bidra till att begränsa kostnadsutvecklingen genom att acceptera att ekonomi behöver vara en princip vid informationsvärdering.[89]

Även om frågan om hur elektroniska underskrifter och stämplar ska bevaras i huvudsak behöver lösas med tekniska medel ser vi före-

[88] *Härifrån till evigheten. En långsiktig arkivpolitik för förvaltning och kulturarv* (SOU 2019:58), s. 521 ff.
[89] A.a. s. 535.

skrifter om bevarande och gallring av dels elektronisk undertecknade eller stämplade handlingar, dels handlingar som behövs för kontroller av underskrifter eller stämplar som ett medel för ett enklare, kostnadseffektivare och mer ändamålsenlig hantering av elektroniskt undertecknade och stämplade handlingar över tid.

Riksarkivet tog i rapporten *Elektroniskt underskrivna handlingar* ställning till frågan om förutsättningar för gallring. I rapporten konstateras att arkivförfattningarna inte reglerar vilka handlingar som ska inhämtas från andra aktörer för att säkerställa möjligheterna till kontroll och att det är oklart vilka rättsliga och andra krav som i framtiden kommer att ställas på inhämtande av kontrollmaterial och eventuell upprepning av den initiala kontrollen[90].

Det slås vidare fast i rapporten att det inte heller går att förutsäga i vilka sammanhang elektroniska underskrifter kommer att användas. Riksarkivet konstaterade att även om förutsättningarna för gallring delvis är desamma för flera av de myndigheter som har infört e-tjänster, saknas tillräckligt underlag för att besluta generella gallringsföreskrifter. Underlaget för rapporten utgjordes av masshanteringen av elektroniskt undertecknade handlingar hos ett antal större myndigheter och Riksarkivet ansåg att det inte då var möjligt att bedöma om resonemangen var tillämpliga i andra sammanhang. Slutsatsen var att så länge som det är oklart i vilka sammanhang elektroniska underskrifter kommer att användas och vilka handlingar som faktiskt kommer att finnas hos myndigheterna, bedöms gallringsfrågan i varje enskilt fall och att eventuell gallring tillsvidare fick regleras i myndighetsspecifika föreskrifter.[91]

Enligt 4 kap. 4 § Riksarkivets föreskrifter och allmänna råd om elektroniska handlingar (RA-FS 2009:1) som tillkom tre år efter rapporten ska myndigheter fortlöpande pröva förutsättningarna för gallring av elektroniska handlingar. eSam, som konstaterar att det inte finns någon RA-FS som specifikt tar upp gallring av elektroniskt undertecknade handlingar, har framfört att en myndighet själv måste utreda förutsättningarna för om och när sådan gallring kan ske.[92]

Ett alternativ för statliga myndigheter som är osäkra på vad som får gallras när det avser elektroniskt undertecknade eller stämplade handlingar är att lämna en framställan till Riksarkivet om myndig-

[90] Riksarkivet, Elektroniskt underskrivna handlingar (Rapport 2006:1), s. 39.
[91] A.a.
[92] eSam, *Juridisk vägledning för införande av e-legitimering och e-underskrifter 1.1*, juni 2018, s. 55.

hetsspecifika gallringsföreskrifter. Om ökad tydlighet kan uppnås genom generella föreskrifter och/eller allmänna råd vore detta dock enligt vår bedömning att föredra eftersom det i längden får anses mindre resurskrävande både för enskilda myndigheter och Riksarkivet. Det skulle även kunna bidra till ett minskat bevarande av handlingar eller delmängder av handlingar som inte behövs för att uppnå syftet med att en elektroniskt undertecknad eller stämplad handling bevaras. Till skillnad från när Riksarkivet senast bedömde denna fråga får vissa av de förutsättningar som då ansågs osäkra, bl.a. i vilka sammanhang elektroniska underskrifter används, ha blivit tydligare. Vi anser därför sammanfattningsvis att Riksarkivet ska få i uppdrag att utreda förutsättningarna för att införa generella bestämmelser och/eller ta fram annat stöd inom området.

Uppdraget borde bl.a. innefatta att utreda vilka handlingar som framställs, används och hanteras hos ett antal utvalda myndigheter i relation till inkomna eller upprättade elektroniskt undertecknade eller stämplade handlingar. Frågan om vad verksamheten behöver bevara, och hur det kan bevaras beror på typen av underskrift eller stämpel och syftet med den, vilket är en fråga om innehållet i handlingen, och ytterst verksamhetens behov och krav. Dessa frågor kan endast besvaras av de enskilda verksamheterna medan den fråga vi anser att Riksarkivet kan förväntas besvara är när underskriften ska bevaras för att uppfylla kraven i 3 § arkivlagen.

Avslutningsvis skulle vi vilja påtala att även om sådana eventuella bestämmelser eller andra stöd ej skulle gälla för gallring inom kommuners och regioners verksamhet skulle det kunna ha vägledande påverkan på det arbete kring bevarande av elektroniskt undertecknade eller stämplade handlingar som bedrivs inom hela den offentliga sektorn.

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

8.6.1 Nuvarande stöd avseende betrodda tjänster

Vårt kartläggningsarbete har visat att behovet inom detta område är stort, framför allt från mindre aktörer i den offentliga förvaltningen (se avsnitt 6.5.6). Det nuvarande stödet från det offentliga avseende betrodda tjänster lämnas huvudsakligen av PTS, DIGG, Kammar-

kollegiet och eSam. Därutöver finns det även stöd som mer generellt gäller digitaliseringsarbete och som har relevans vid införande och användning av betrodda tjänster. Det bör noteras att det av vår kartläggning även har framgått från både tillhandahållare och offentliga aktörer att tillhandahållarna i dagsläget bistår med mycket stöd.

PTS har enligt myndighetens instruktion att, utöver att vara tillsynsmyndighet, även ge stöd och information till myndigheter och enskilda när det gäller betrodda tjänster.[93] PTS har publicerat en vägledning för betrodda tjänster i Sverige enligt eIDAS, som i juni 2020 kom i sin tredje utgåva. Vägledningen innehåller bl.a. en beskrivning av processen för att etablera sig som tillhandahållare av kvalificerade betrodda tjänster, kraven på icke kvalificerade tillhandahållare, rutiner för incidentrapportering och användning av alternativa standarder än de som refereras av EU. Målgruppen för vägledningen är främst tillhandahållare av betrodda tjänster, berörda myndigheter och andra organ.[94]

DIGG har enligt sin myndighetsinstruktion att ansvara för den offentliga förvaltningens tillgång till infrastruktur och tjänster för bl.a. elektroniska underskrifter. DIGG ska även främja användningen av elektroniska underskrifter.[95] DIGG erbjuder i dagsläget visst stöd inom detta område (se mer om detta i avsnitt 8.6.2).

Kammarkollegiet har inom tre ramavtalsområden ställt krav på att elektronisk identifiering och elektroniska underskrifter ska kunna användas.[96] Som stöd vid avrop har myndigheten vidare publicerat en vägledning.[97]

Utöver dessa myndigheter tillhandahåller eSam *Juridisk vägledning för införande av e-legitimering och e-underskrifter*.[98] Vägledningen togs fram av eSam i samarbete med MSB och dåvarande E-legitimationsnämnden. Den senaste versionen av vägledningen är från juni 2018. eSam tillhandahåller fortfarande vägledningen men DIGG avser att ta arbetet vidare.

Vägledningar för kommuner och regioner finns bl.a. i form av SKR:s *Rapport till vägledning vid införandet av e-tjänster* och Sambruks *Praktiska erfarenheter kring e-underskrifter*.

[93] 4 § 14 förordning (2007:951) med instruktion för Post- och telestyrelsen.
[94] PTS, *Vägledning för betrodda tjänster i Sverige enligt eIDAS (Utgåva 3)*, 10 juni 2020, s. 6.
[95] 3 § 1 och 2 förordning (2018:1486) med instruktion för Myndigheten för digital förvaltning.
[96] www.avropa.se/innehall/e-identifiering-och-e-underskrift/ (hämtad 2021-01-14).
[97] Kammarkollegiet, *Vägledning för avrop av tjänster förelektronisk identifiering och elektronisk underskrift från ramavtalsområden inom Programvaror och Tjänster 2019* (Version 2.0), 8 april 2020.
[98] eSam, *Juridisk vägledning för införande av e-legitimering och e-underskrifter 1.1*, juni 2018.

Det finns vidare skriftliga stöd som tagits fram av enskilda myndigheter eller mindre sammanslutningar av myndigheter, exempelvis Boråsregionens *Vägledning elektroniska underskrifter*.

8.6.2 Vilket stöd behövs?

Det stöd som behövs vid införande, förvaltning och vidareutveckling av betrodda tjänster gäller både de betrodda tjänsterna som sådana, som det mer generella stöd som behövs vid all digitalisering inom den offentliga förvaltningen. Nedan presenteras dessa områden. Uppräkningen ska inte ses som uttömmande rörande de behov som mer generellt gäller vid digitalisering, men tjänar till att visa hur många olika frågeställningar som kan behöva besvaras vid införande av en betrodd tjänst eller en e-tjänst där en betrodd tjänst ingår.

De behov av stöd vi identifierat kan delas in i tre olika delområden:

- Vad behövs och vilka bedömningar behöver göras?
- Hur anskaffas en betrodd tjänst?
- Hur införs, förvaltas och vidareutvecklas en betrodd tjänst?

Nedan beskrivs vilka typer av stöd som behövs inom respektive delområde och vilket stöd som finns i dag.

Vad behövs och vilka bedömningar behöver göras?

För att en ändamålsenlig användning av betrodda tjänster inom den offentliga förvaltningen ska uppnås krävs det stöd för att bedöma om en betrodd tjänst är rätt lösning utifrån verksamhetens behov. Detta innefattar stöd i att exempelvis bedöma huruvida en viss bestämmelse uppställer krav om att en underskrift behövs och om kravet i sådana fall även kan tillgodoses med en elektronisk underskrift. Om det inte finns bestämmelser som föranleder att underskrifter krävs finns det ett behov av att bedöma huruvida autentisering och loggning exempelvis kan vara tillräcklig. Dessa frågeställningar belyses i dag i viss utsträckning i eSam:s och SKR:s vägledningar samt Sambruks rapport.[99]

[99] eSam, *Juridisk vägledning för införande av e-legitimering och e-underskrifter 1.1*, juni 2018 s. 28 ff., SKR, *Rapport till vägledning vid införandet av e-tjänster*, oktober 2011 och Sambruk, *Praktiska erfarenheter kring e-underskrifter*, juni 2020.

Ett ställningstagande kring om realisering ska ske genom en e-tjänst, blanketter som skrivs under elektroniskt eller på något annat sätt behöver även göras. DIGG erbjuder visst stöd rörande att ta emot underskrifter (för det fall en aktör väljer en lösning med blanketter) och vissa frågor som ska beaktas vid elektroniskt undertecknande.[100]

Frågor rörande tjänstens utformning ska med hänsyn till kraven på tillgänglighet för personer med funktionsnedsättning också beaktas (se mer om detta i avsnitt 8.1.3).

Inför införandet av betrodd tjänst måste givetvis olika juridiska frågeställningar hanteras, exempelvis om några sekretessfrågor aktualiseras. Vidare är stödet för och hanteringen av personuppgifter ytterligare en central aspekt att beakta. Inom detta område har Integritetsskyddsmyndigheten en rad olika vägledningar.[101] En särskild fråga inom området personuppgifter som även kan behöva beaktas är om andra myndigheter genom en tjänst ges tillgång till uppgifter är frågan om det är att anse som direktåtkomst eller utlämnande på medium för automatiserad behandling och tjänsten i så fall utformas på ett visst sätt för att anses vara det senare.[102]

Även hur personer med skyddade personuppgifter, dvs. som har skyddad folkbokföring, sekretessmarkering och fingerade personuppgifter inom folkbokföringen, ska hanteras måste beaktas. Inom detta område erbjuder Skatteverket en vägledning för hantering inom svensk förvaltning.[103]

Bedömningar avseende informationssäkerhet måste också göras. Samverkansgruppen för informationssäkerhet (SAMFI) består av ett antal myndigheter som alla har ett särskilt ansvar för samhällets informationssäkerhet.[104] SAMFI tillhandahåller bl.a. webbplatsen informationssäkerhet.se där den hjälp som svenska myndigheter kan erbjuda inom området finns samlad. Även eSam:s vägledning inne-

[100] www.digg.se/digital-identitet/e-underskrift/offentlig-aktor (hämtad 2021-01-14).
[101] www.imy.se/vagledningar/ (hämtad 2021-01-14).
[102] Se HFD 2015 ref. 61 och *Juridik som stöd för förvaltningens digitalisering* (SOU 2018:25), s. 84 ff.
[103] https://skatteverket.se/privat/folkbokforing/skyddadepersonuppgifter/hanteringavsekretessmarkeradepersonuppgifter.4.18e1b10334ebe8bc80002541.html (hämtad 2021-01-14).
[104] I SAMFI ingår MSB, PTS, Polismyndigheten, Försvarets radioanstalt, Säkerhetspolisen, Försvarets materielverk /CSEC och Försvarsmakten/Militära underrättelse- och säkerhetstjänsten.

håller ett kapitel om informationssäkerhet.[105] Därtill har Säkerhetspolisen en vägledning om informationssäkerhet inom ramen för säkerhetsskydd.[106]

Myndigheter måste även analysera om tjänsterna kan missbrukas och om de kan utformas för att motverka detta. Ett exempel är det fenomen eSam har lyft fram där företag erbjuder tjänster och uppmanar användaren att legitimera sig mot myndigheters e-tjänster. Den som loggas in i e-tjänsten är däremot inte användaren utan företaget som hämtar information eller utför åtgärder.[107] eSam har skrivit en promemoria om åtgärder som riktar sig mot sådant vilseledande.[108]

Beslut måste även tas rörande hur undertecknade och stämplade handlingar ska hanteras vad avser bl.a. validering och bevarande. Som framgår av avsnitt 8.5.3 är de frågeställningar som finns rörande bevarande något som utreds av både Riksarkivet och SKA. Även om det finns en del äldre material på området saknas det i dag ett erforderligt stöd. Vi ser emellertid att våra förslag i avsnitt 8.5.4 och 8.5.5 kan utgöra grunden för ett mer utvecklat stöd rörande dessa frågor.

Hur anskaffas en betrodd tjänst?

Ytterligare ett område där det finns behov av stöd avser själva anskaffandet. Som framgår ovan finns både ramavtal och vägledning från Kammarkollegiet som omfattar elektroniska underskrifter. Under vår kartläggning har det framkommit att ett stort problem upplevs vara att säkerställa vilka tillhandahållares tjänster som uppfyller eIDAS-förordningens krav vad avser avancerade elektroniska underskrifter. DIGG utför i dagsläget en granskning av fristående underskriftstjänster som utgör ett stöd vid upphandling och som även innefattar att bedöma huruvida tjänsterna uppfyller kraven på att skapa avancerade elektroniska underskrifter.[109] Vi ser att det förslag vi lämnat i avsnitt 8.3 om möjlighet för icke kvalificerade tillhandahållare att föras upp på tillitsförteckningen kommer att ge ett förbättrat stöd för myndigheter i anskaffningsfasen då det blir enklare att identifiera vilka

[105] eSam, *Juridisk vägledning för införande av e-legitimering och e-underskrifter 1.1*, juni 2018 s. 49 ff.
[106] Säkerhetspolisen, *Vägledning i säkerhetsskydd – Informationssäkerhet*, juni 2019.
[107] www.esamverka.se/aktuellt/nyheter/nyheter/2020-05-18-trovardigheten-for-e-legitimation---ar-grunden-for-digitalisering.html (hämtad 2021-01-14).
[108] eSam, *Åtgärder mot att användare vilseleds att logga in någon annan med sin e-legitimation* (dnr/ref: 2018-57), juni 2018.
[109] www.digg.se/digital-identitet/e-underskrift/offentlig-aktor (hämtad 2021-01-14).

tillhandahållare som erbjuder lösningar som uppfyller kraven för skapande av avancerade elektroniska underskrifter och stämplar.

För det fall uppgifter ska behandlas som är säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen konfidentiell eller högre har Säkerhetspolisen en vägledning avseende säkerhetsskyddad upphandling.[110]

Hur införs, förvaltas och vidareutvecklas en betrodd tjänst?

Vad avser införande ser vi att det finns ett behov av praktiska råd rörande både testfasen och driftsättning. Vi ser att det finns ett behov av stöd rörande hur myndigheter ska förvalta och vidareutveckla betrodda tjänster. Dels för att följa utvecklingen vad avser krav och risker och hur dessa kan mötas, dels för att följa upp att de tjänster som används förändras i takt med verksamhetens behov. I dagsläget finns inget sådant stöd från det offentliga i de ovan redovisade delarna.

8.6.3 En utökad roll för Myndigheten för digital förvaltning

Utredningens förslag: Myndigheten för digital förvaltning ska få i uppgift att främja användningen av betrodda tjänster.

Post- och telestyrelsen ska inte längre ha i uppgift att ge stöd och information till myndigheter avseende betrodda tjänster.

Myndigheten för digital förvaltning ska få i uppdrag att ta fram en vägledning för den offentliga förvaltningens användning av betrodda tjänster.

Skälen för utredningens förslag

För att möta det identifierade behovet av ett utökat stöd och en samlad vägledning för den offentliga förvaltningen inom området betrodda tjänster anser vi att den nuvarande ansvarsfördelningen bör ändras och att stödet behöver utökas. Vi anser att detta delvis ska uppnås genom en justering av de uppgifter som PTS respektive DIGG har i dag.

[110] Säkerhetspolisen, *Vägledning i säkerhetsskydd – Säkerhetsskyddad upphandling*, juni 2019.

DIGG har som uppgift att främja användningen av elektroniska underskrifter, men inte övriga betrodda tjänster, medan PTS har i uppgift att ge stöd och information till myndigheter och enskilda när det gäller betrodda tjänster. Det finns således ett visst överlapp mellan myndigheternas uppgifter. DIGG har även pekat på att det inom området betrodda tjänster finns områden som ingen myndighet har eller de facto tar ansvar för.[111] Utifrån våra kontakter med PTS har det framkommit att de framför allt har kontakter med tillhandahållare av betrodda tjänster och att de inte i någon större utsträckning lämnar stöd till enskilda myndigheter. DIGG å sin sida har uppgett att de får många förfrågningar rörande elektroniska underskrifter från myndigheter, men att de saknar tillräckliga resurser för att hantera de frågor som ställs. Utifrån att DIGG har som övergripande uppdrag att samordna och stödja den förvaltningsgemensamma digitaliseringen i syfte att göra den offentliga förvaltningen mer effektiv och ändamålsenlig anser vi det naturligt att även låta DIGG få ansvaret för att ge stöd och information till myndigheter avseende betrodda tjänster. De bör således utöver elektroniska underskrifter även främja användningen av övriga betrodda tjänster. Vi anser vidare att detta kan öka medvetenheten kring, samt användningen av, betrodda tjänster då ingen myndighet i dag har i uppgift att främja användningen av betrodda tjänster som helhet. Vi ser således att den föreslagna uppdelningen täcker in de områden där ingen av dessa myndigheter i dagsläget har ett uttalat ansvar samt löser de gränsdragningsproblem mellan myndigheterna som för närvarande existerar.

Som framgår av avsnitt 8.6.2 är det viktigt att få stöd rörande frågor som kan uppkomma i relation till införande och användning av betrodda tjänster. Vi ser det emellertid som lika angeläget att myndigheter ges tydliga upplysningar om frågor de inte var medvetna att de behöver beakta. Vi ser därför att det, utöver direkt stöd rörande betrodda tjänster, finns ett behov av en samlad, relevant och löpande uppdaterad vägledning som bl.a. innehåller de frågeställningar som bör beaktas. Vägledningen bör även innehålla hänvisningar till sådana ovan redovisade stöd och vägledningar som andra myndigheter erbjuder som har relevans för betrodda tjänster. En sådan vägledning kan även vara till nytta för privata aktörer. DIGG avser att ta över ansvaret för eSam:s *Juridisk vägledning för införande av e-*

[111] DIGG, *Uppdrag om stödjande åtgärder vid nationellt införande av eIDAS-förordningen* (dnr 2019-90), s. 19.

legitimering och e-underskrifter och vi ser det som en god startpunkt för en utökad vägledning som innefattar fler frågeställningar och även andra betrodda tjänster utöver underskrifter. Vi anser därför att DIGG ska ges ett regeringsuppdrag för att uppdatera och vidareutveckla eSam:s vägledning. När vägledningen är framtagen kan förvaltningen av den anses ingå i de ändrade uppgifter vi föreslår i myndighetens instruktion.

8.7 En ökad användning av elektroniska stämplar bör främjas

Utredningens bedömning: Vi anser att en ökad användning av elektroniska stämplar inom den offentliga förvaltningen särskilt bör främjas av Myndigheten för digital förvaltning inom ramen för den nya uppgift avseende betrodda tjänster som utredningen föreslår att myndigheten ska få.

Skälen för utredningens bedömning

Utredningens kartläggningsarbete har visat att användningen av elektroniska stämplar inom den offentliga förvaltningen är relativt begränsat och att förvaltningens fokus vid digitaliseringsarbete verkar framför allt är inriktat på användning av elektroniska underskrifter.

Det finns i svenska författningar endast två hänvisningar till elektroniska stämplar. De aktuella bestämmelserna återfinns i 3 § andra stycket lagen (1969:12) om internationell vägtransport och 8 a § andra stycket lagen (1974:610) om inrikes vägtransport. Av bestämmelserna framgår att en elektronisk fraktsedel antingen ska undertecknas med en avancerad elektronisk underskrift eller förses med en avancerad elektronisk stämpel. Dessa bestämmelser exemplifierar att elektroniska underskrifter och elektroniska stämplar kan ges samma status som utställarverifikation. I avsnitt 4.3.2 redogörs även för att den elektroniska stämpelns juridiska funktioner är desamma som den elektroniska underskriftens. Den avgörande skillnaden mellan underskriften och stämpeln är endast att det är en utställarverifikation från en enskild individ respektive en juridisk person.

Förarbetena till en nyligen genomförd ändring i hyresförhandlingslagen (1978:304) illustrerar väl en av anledningarna som vi ser till att användningen av elektroniska stämplar inte är mer utbredd i dagsläget. PTS hade i sitt remissvar framfört att det utöver att i den då föreslagna lagen öppna upp för att använda avancerade elektroniska underskrifter kan vara av intresse att göra det möjligt att använda avancerade elektroniska stämplar. Den bedömning som gjordes i förarbetena var dock att eftersom berörda parter inte uttalat något behov av en sådan lösning lämnades inte heller något sådant förslag.[112] Det är få aktörer inom den offentliga förvaltningen som uttrycker att de har ett behov av ökad användning av elektroniska stämplar. Samtidigt har det till utredningen exempelvis framförts behov avseende att en elektronisk underskrift ska knytas till en myndighet då det finns många medarbetare där det inte är lämpligt att personnummer exponeras i besluten. En lösning på detta behov hade kunnat vara användning av arbetsgivaren anskaffad e-legitimation där kopplingen till individen är pseudonymiserad.[113] Ett annat alternativ vore dock att använda sig av elektroniska stämplar i stället för elektroniska underskrifter. Som även konstateras i avsnitt 4.2.1 har närmast rutinmässiga krav på undertecknande vid pappersförfaranden i vissa fall synes ha uppställts av myndigheter utan att det funnits krav i lag eller förordning som anger att det behövs.[114] För det fall en myndighet anser att en handling behöver ha en utställarverifikation utan att handlingen har identifierbar koppling till en enskild medarbetare är således en elektronisk stämpel ett bra alternativ.

Som det tidigare återgivna förarbetsuttalandet påvisar ser vi att kunskapsnivån rörande vilka användningsområden som finns för elektroniska stämplar behöver ökas då den elektroniska stämpeln inte har samma användningsområden som många av de stämplar som i dagsläget används inom pappersbaserade processer. Där stämplar endast i vissa fall har en koppling till utställarverifikation. I de fall det rör sig om en utställarverifikation brukar stämpeln därtill ofta kombineras med en underskrift (jfr avsnitt 4.3.1).

---

[112] Prop. 2019/20:8 s. 7.

[113] Pseudonymisering definieras i artikel 4.5 i dataskyddsförordningen som behandling av personuppgifter på ett sätt som innebär att personuppgifterna inte längre kan tillskrivas en specifik registrerad utan att kompletterande uppgifter används, under förutsättning att dessa kompletterande uppgifter förvaras separat och är föremål för tekniska och organisatoriska åtgärder som säkerställer att personuppgifterna inte tillskrivs en identifierad eller identifierbar fysisk person.

[114] *Juridik som stöd för förvaltningens digitalisering* (SOU 2018:25), s. 461.

Mot bakgrund av det ovan redovisade anser vi att en ökad användning av elektroniska stämplar inom den offentliga förvaltningen särskilt bör främjas av DIGG inom ramen för den uppgift vi i avsnitt 8.6.3 föreslår att myndigheten ska få.

8.8 Ökad medverkan i standardiseringsarbete

Utredningens förslag: Regeringen ska ge DIGG och PTS i uppdrag att tillsammans och i samråd med andra berörda aktörer ta fram en handlingsplan för ökad medverkan i det europeiska och internationella standardiseringsarbetet som avser betrodda tjänster.

Skälen för utredningens förslag

Standarder, inklusive tekniska specifikationer, spelar en stor roll inom området betrodda tjänster. Som framgår av avsnitt 5.12.1 fastställs i förordningen diverse krav och vissa genomförandeakter pekar mot standarder eller fastställer referensformat. För ett flertal av kraven i förordningen har kommissionen emellertid valt att ännu inte anta någon genomförandeakt. Det kan dock inte uteslutas att genomförandeakter med sådant innehåll kommer att antas i framtiden. Dessutom kan redan utpekade standarder komma att uppdateras. Standarder kan oavsett om genomförandeakter antagits eller inte få betydelse eftersom vägledningar från tillsynsorgan[115] och ENISA[116] hänvisar till standarder som kan användas för att leva upp till förordningens krav. Även om det inte är ett rättsligt krav att följa dessa vägledningar är det enligt vår bedömning rimligt att anta att de har effekt på tillhandahållarna av betrodda tjänster.

Regeringen beslutade år 2018 om en strategi för standardisering.[117] Regeringen konstaterar i strategin att det finns ett behov av ett aktivt svenskt standardiseringsarbete, där samverkan och samarbete står i centrum samt att det är viktigt att Sverige verkar för att standardisering inte får innovationshämmande och negativa säkerhets-, miljö-

[115] PTS, *Vägledning för betrodda tjänster i Sverige enligt eIDAS (Utgåva 3)*, 10 juni 2020.
[116] ENISA, *Recommendations for QTSPs based on Standards – Technical guidelines on trust services*, 19 december 2017.
[117] Regeringens strategi för standardisering (UD2018/12345/HI).

eller hälsoeffekter.[118] Vidare konstateras att ökad digitalisering och en snabb teknikutveckling leder till ett ökat fokus på standardisering och interoperabilitet.[119] Strategin pekar ut ett antal svenska strategiska prioriteringar ur ett nationellt, europeiskt och internationellt perspektiv, och beskriver hur de ska adresseras genom en aktiv svensk standardiseringspolitik.[120] Vissa prioriteringar avser digital förvaltning.[121]

Det standardiseringsarbete i Europa som avser eller påverkar tillhandahållare av betrodda tjänster genomförs i dag främst av CEN och ETSI. I arbetet med standarderna deltar framför allt europeiska tillhandahållare av betrodda tjänster, deras underleverantörer, fristående experter och experter från olika medlemsstaters myndigheter. Från Sverige deltar bl.a. ett fåtal tillhandahållare av betrodda tjänster och experter. Svenska myndigheter bidrar och deltar i dag endast i begränsad omfattning i arbetet. Den uppfattning vi har fått är att Sveriges påverkan på standardiseringsarbetet kan förbättras, bl.a. genom bättre samordning. Vår bedömning är vidare att det är angeläget att Sverige tar en mer aktiv roll i det relevanta standardiseringsarbetet. Det skulle öka Sveriges möjligheter att påverka arbetet i en riktning som både underlättar förvaltningens användning av betrodda tjänster samt leder till förbättrade möjligheter till export av svenska betrodda tjänster och ökad gränsöverskridande interoperabilitet.

Vi anser att en ökad medverkan från Sverige i standardiseringsarbetet på detta område ligger väl i linje med regeringens ambitioner som kommer till uttryck i standardiseringsstrategin, t.ex. att regeringen ska verka för att främja att standarder tas fram i syfte att främja interoperabilitet och marknadskonkurrens samtidigt som rättssäkerhet upprätthålls.

I standardiseringsstrategin framhåller regeringen också att den, genom myndighetsstyrning, ska betona vikten av ökat deltagande av berörda svenska myndigheter vid framtagandet av harmoniserade standarder. Både DIGG och PTS har i sina instruktioner i uppgift att arbeta med standardisering. DIGG ska enligt 6 § första punkten förordningen (2018:1486) med instruktion för Myndigheten för digital förvaltning delta i och främja nationellt och internationellt standar-

[118] A.a., s. 3.
[119] A.a.
[120] A.a.
[121] A.a. s. 23 f.

diseringsarbete inom sitt verksamhetsområde. PTS ska enligt 7 § tredje punkten förordning (2007:951) med instruktion för Post- och telestyrelsen delta i nationellt och internationellt standardiseringsarbete. Försvarets materielverk (FMV)[122], MSB och Swedac har i sina respektive myndighetsinstruktioner inte uttalade uppgifter avseende att arbeta med standardisering. Myndigheterna arbetar emellertid med, samt bidrar till, standardisering inom ramen för sina ansvarsområden.

Vår bedömning är att det standardiseringsarbete som bedrivs avseende betrodda tjänster kan samordnas i större utsträckning än vad som sker i dag. Vi bedömer också att det finns behov av ett mer strategiskt arbete och att resurser tillsätts i sådan utsträckning att Sverige kan påverka utifrån sina prioriteringar på området. Mot den bakgrunden föreslår vi att regeringen ger DIGG och PTS i uppdrag att ta fram en handlingsplan för hur Sverige ska kunna påverka standardiseringsarbetet i större utsträckning än i dag. Handlingsplanen bör ta sin utgångspunkt i regeringens standardiseringsstrategi. Arbetet med att ta fram handlingsplanen ska ske i samråd med relevanta aktörer på området, särskilt de svenska standardiseringsorganen, andra relevanta myndigheter såsom FMV/CSEC, MSB och Swedac samt branschorganisationer och näringslivet.

8.9 Utformning av författningsbestämmelser rörande underskrifter

8.9.1 Formkrav

Med formkrav avses krav på att ett dokument eller meddelande ska ha en viss form eller tillkomma på visst sätt för att ha en viss rättsverkan. Formkrav kan också föreskriva att en handling ska ha ett visst innehåll. Till formkraven kan också hänföras krav på att en handling ska utföras på visst sätt för att en viss rättsverkan ska inträffa (s.k. procedurkrav).[123]

eSam har omformulerat och komprimerat detta till att 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

[122] Innefattar även CSEC.
[123] *Formel – Formkrav och elektronisk kommunikation* (Ds 2003:29), s. 17.

styrande effekt enligt eSam vanligtvis i att vissa termer eller uttryck betecknar åtgärder som inte kan utföras elektroniskt.[124]

Vad gäller underskrifter kan ett formkrav innebära att en underskrift måste ske genom en namnteckning på papper eller att underskriften måste bevittnas eller exempelvis ske i närvaro av polisman.[125] Även en anvisning om att en elektronisk underskrift ska vara av viss nivå, exempelvis att undertecknade ska ske med en avancerad elektronisk underskrift, utgör ett formkrav.

Av artikel 2.3 i eIDAS-förordningen framgår att förordningen inte påverkar regler i nationell rätt som avser rättsliga eller förfarandemässiga skyldigheter avseende formkrav. I de fall ett nationellt formkrav anses innebära ett krav på t.ex. namnteckning på papper har ett sådant krav alltså företräde framför eIDAS-förordningens reglering om rättslig verkan för elektroniska underskrifter i artikel 25.1.

8.9.2 Teknikneutral reglering

En lagstiftningsteknik som i vissa avseenden kan anses utgöra en motsats till författningar som innehåller formkrav är teknikneutrala regleringar. En teknikneutral reglering kan exempelvis ange att ett beslut ska skrivas under utan att ange att det ska ske genom namnteckning på papper eller med elektronisk underskrift. Innebörden av detta blir att rekvisitet i bestämmelsen om att beslutet ska skrivas under kan utföras med penna på papper, med elektronisk underskrift eller med någon annan framtida teknik för att framställa underskrifter.

Lagstiftaren har länge eftersträvat att utforma författningar på ett teknikneutralt sätt och detta arbete är alltjämt pågående.[126] Hur långt det är möjligt att gå i syfte att uppnå teknikneutralitet är givetvis beroende på vilken koppling som finns eller behöver finnas mellan författningen och specifika tekniska lösningar.[127] Detsamma gäller på EU-nivå där lagstiftningstekniken som kallas nya metoden innebär att detaljerade tekniska krav undviks till förmån för väsentliga krav och hänvisningar till standarder.[128]

[124] eSam, *Juridisk vägledning för införande av e-legitimering och e-underskrifter 1.1*, juni 2018 s. 28.
[125] Se bestämmelserna om upprättande av testamente i 10 kap. ärvdabalken vad avser vittnen och 48 kap. 17 § andra stycket rättegångsbalken vad gäller underskrift i närvaro av polisman.
[126] Se t.ex. prop. 2019/20:189 s. 26.
[127] Se t.ex. prop. 2017/18:299 s. 22 ff.
[128] Regeringskansliet, *Översyn av nya harmoniseringsmetoden för tekniska krav på produkter ("Nya metoden")*, Faktapromemoria 2006/07:FPM66.

Fördelen med ett teknikneutralt förhållningssätt är att det innebär att den tekniska utvecklingen inte behöver leda till regelbundna ändringar och att lagstiftningen därför blir mer flexibel och hållbar över tid. En bestämmelse som tydligt kopplar till en viss teknisk lösning kan även skapa icke önskvärda inlåsningseffekter för den offentliga förvaltningen. Ett tydligt exempel på detta var 5 § i den tidigare gällande förvaltningslagen (1986:223) där det framgick att myndigheterna hade en skyldighet att se till att det var möjligt för enskilda att kontakta dem med hjälp av telefax och elektronisk post och att svar kan lämnas på samma sätt. Det kan i detta sammanhang noteras att motsvarande bestämmelse i den nu gällande förvaltningslagen (2017:900) gavs en teknikneutral utformning.[129]

Digitaliseringsrättsutredningen lyfte i samband med deras kartläggning att bestämmelser visserligen kan sägas vara neutrala i förhållande till vilken teknik som används vid det förfarande som regleras. En sådan till synes teknikneutral reglering kunde dock enligt utredningen ofta innebära att traditionella förfaranden och processer som innefattar pappershantering utgör utgångspunkten för de handlingsdirektiv som författningen anger. Detta gäller bl.a. om det rör sig om att regleringen styr att viss information under ett visst skede ska överföras från en aktör till en annan, exempelvis genom att ange en process bestående av anmälan respektive ansökan eller att på annat sätt ange handlingsdirektiv om att information i ett visst skede ska överföras.[130]

Digitaliseringsrättsutredningen ansåg vidare att informationshantering med digitala medel väcker frågor även rörande dessa typer av bestämmelser, eftersom den digitala tekniken möjliggör en helt annan typ av hantering av information än vad som var möjligt när processerna reglerades. Enligt deras bedömning kan en teknikneutral reglering nu och i framtiden inte utgå från att papper är informationsbäraren och att postgång används för förmedling av information. Även de gällande författningar som kan framstå som teknikneutrala kan därför behöva förändras med anledning av digitaliseringen.[131]

Digitaliseringsrättsutredningen ansåg att det fanns många fördelar med teknikneutrala regleringar men framhöll att den största nackdelen med en teknikmässigt fristående författning var svårig-

[129] Prop. 2016/17:180 s. 170.
[130] *Juridik som stöd för förvaltningens digitalisering* (SOU 2018:25), s. 126.
[131] A.a.

heterna för tillämparen som ska applicera de neutrala reglerna på en många gånger komplex teknisk verklighet. Utredningen anförde vidare att en alltigenom teknikneutral reglering riskerade att försvåra dess förutsebarhet, till nackdel såväl för tillämpande myndigheter som för enskilda.[132] Vi delar denna bild och skulle även vilja lägga till ytterligare en aspekt. I många fall är den författningstekniska uppbyggnaden sådan att en bestämmelse på lagnivå är teknikneutral och att eventuella detaljregleringar rörande specifika tekniska lösningar som kompletterar bestämmelsen återfinns i förordning eller föreskrift. De val som görs avseende vilken teknisk lösning som ska användas eller vilken säkerhetsmässig nivå dessa lösningar ska hålla sker således ofta på förordnings- eller föreskriftsnivå. Detta lyfter en mer principiell fråga om på vilken nivå sådana beslut ska fattas. I synnerhet när det kan anses ha stor påverkan på Sveriges informationssäkerhet. Vi återkommer till denna fråga nedan under avsnitt 8.9.5.

8.9.3 Tidigare utredningsarbete avseende elektroniska underskrifters användning och rättsverkan

Frågan om elektroniska underskrifters rättsverkan och hur formkrav som hindrar användning av elektroniska underskrifter ska undanröjas har varit aktuell i över tjugo år. Olika bedömningar har även funnits och finns än i dag avseende hur signaturdirektivets respektive eIDAS-förordningens bestämmelser påverkar nationell rätt i detta avseende. Se avsnitt 5.9 för mer om dessa bestämmelser och utredningens bedömning rörande denna fråga.

IT-utredningen

IT-utredningen tillsattes 1994 med uppgift att bl.a. utreda användningen av elektroniska dokument inom förvaltningen och näringslivet. I syfte att underlätta användningen av elektroniska underskrifter inom den offentliga förvaltningen föreslog utredningen att när formkrav som medför att elektronisk dokumenthantering inte kan användas – t.ex. att handlingar ska vara egenhändigt undertecknade – en bestämmelse om att regeringen fick föreskriva att digitala dokument eller, när det kan anses tillräckligt, elektroniska handlingar utan elek-

[132] A.a. s. 127.

tronisk underskrift eller stämpel får användas.[133] Utredningens förslag i denna del genomfördes aldrig.

Regeringskansliets beredningsgrupp för digitala signaturer

Regeringskansliets beredningsgrupp för digitala signaturer tog 1998 fram departementspromemorian *Digitala signaturer – en teknisk och juridisk översikt* (Ds 1998:14). Promemorian var avsedd att utgöra underlag för Regeringskansliets fortsatta arbete på en svensk politik inom området som då benämndes digitala signaturer. Gruppen tog ställning till huruvida en elektronisk underskrift – om den uppfyller en viss säkerhetsnivå – generellt ska ges samma rättsverkan som en egenhändig namnteckning. Även om gruppen fann att det fanns fördelar med en sådan lagstiftningsmetod i form av att alla de lagar och föreskrifter som innehåller krav på underskrift kan på en gång fås att omfattas av användning av elektroniska underskrifter genom en lagregel om jämställande med underskrift. Gruppen konkluderade dock att det vid denna tid, då tekniken inte hade prövats i större skala kunde leda till oanade konsekvenser. Gruppens slutsats var mot bakgrund av bl.a. de olika skälen bakom formkraven i olika författningar att en generellt verkande reglering innebärande att elektroniska underskrifter godtas i stället för egenhändiga namnteckningar över hela rättsområdet inte skulle vara möjlig.[134] Majoriteten av remissinstanserna delade denna bedömning. Vissa ansåg dock att frågan avfärdades alltför lättvindigt och ansåg det nödvändigt med en generell likställighet genom lagstiftning.[135]

Genomförandet av signaturdirektivet

I november 1999 antogs signaturdirektivet (se mer om direktivet i avsnitt 5.3). I departementspromemorian *Elektroniska signaturer* (Ds 1999:73) lämnades förslag till hur direktivet skulle genomföras i svensk rätt. I promemorian lyftes återigen frågan om förutsättningarna för att införa en generell regel i svensk lagstiftning som likställer vissa typer av elektroniska underskrifter med egenhändiga namn-

[133] *Elektronisk dokumenthantering* (SOU 1996:40), s. 97 f.
[134] *Digitala signaturer – en teknisk och juridisk översikt* (Ds 1998:14), s. 183 ff.
[135] *Elektroniska signaturer* (Ds 1999:73), s. 102.

underskrifter. Slutsatsen i promemorian var att man knappast kan undgå det omfattande arbetet med att göra en inventering av befintliga författningar och överväga i varje enskilt fall om en ändring är motiverad. När behovet är klarlagt kan man dock på ett enkelt sätt genomföra nödvändiga förändringar, även om regeln ges i lag.[136] I lagens förarbeten anfördes att utgångspunkten bör vara att det inte bör finnas otidsenliga formkrav som på ett onödigt sätt hindrar elektronisk kommunikation. Mot bakgrund av den ovan nämnda behandlingen i promemorian av frågan om en generell regel var slutsatsen i lagens förarbeten att en sådan typ av regel inte torde vara möjlig.[137]

FORMEL-gruppen

Regeringen beslutade år 2002 att Regeringskansliet departementsvis skulle se över gällande formkrav i lagar och förordningar och överväga behovet av förändringar i syfte att undanröja onödiga hinder för elektronisk kommunikation och elektronisk dokument- och ärendehantering. För att samordna arbetet inrättades inom Regeringskansliet en arbetsgrupp vilken antog namnet FORMEL-gruppen. I arbetsgruppen företräddes departementen av chefstjänstemän eller chefer för rättssekretariaten.[138]

FORMEL-gruppen avlämnade sin rapport *Formel – Formkrav och elektronisk kommunikation* år 2003. Gruppens genomgång av gällande rätt med formkrav omfattade sammantaget omkring 2 000 författningsställen. Genomgången visade att formkrav kunde betecknas på många olika sätt. FORMEL-gruppen framhöll att sådana krav kan hindra digital kommunikation eller dokumentation genom att uttryckligen utesluta digitala rutiner eller genom att det råder osäkerhet om hur kraven ska tillämpas på digitala rutiner. Det framkom också att formkravens innebörd inte sällan var oklar och att även likalydande formkrav kunde ha olika innebörd. Det visade sig även att formkraven kunde ha olika syften och bevekelsegrunder. Ofta var det dessutom svårt att reda ut vilket syfte som låg bakom enskilda formkrav.[139] Bland de formkrav som enligt FORMEL-gruppens analys och bedömningar hindrade elektroniska rutiner återfanns bl.a. krav

[136] A.a.
[137] Prop. 1999/2000:117 s. 58.
[138] *Formel – Formkrav och elektronisk kommunikation* (Ds 2003:29), s. 15 f.
[139] A.a. s. 10.

på underskrift, namnteckning och undertecknande. Det fanns andra typer av begrepp som inte alls borde uppfattas som formkrav, t.ex. anmälan, ansökan och underrättelse. Det fanns också exempel på begrepp eller krav som normalt inte borde hindra elektroniska rutiner, t.ex. handling respektive beslut, eller krav på skriftlighet eller att uppgifter ska lämnas enligt ett visst formulär.[140]

Frågan om en generell reglering lyftes även på nytt i samband med FORMEL-gruppens arbete. Gruppen fann att den ena extrempunkten utgjordes av att ändra varje bestämmelse som innehåller formkrav för att tydliggöra att elektroniska rutiner kan användas och vilka krav dessa måste uppfylla. Det motsatta angreppssättet skulle enligt FORMEL-gruppen innebära att man införde en generell bestämmelse som skulle föreskriva att samtliga formkrav av en viss typ, t.ex. namnunderskrift, skulle anses uppfyllda med vissa elektroniska rutiner, t.ex. elektronisk underskrift. Det senare exemplifierades med en numera upphävd finsk lagbestämmelse som innehöll en föreskrift om att alla formkrav av en viss typ får fullgöras med en viss typ av elektroniska rutiner vid all kommunikation med förvaltningen. Man kunde enligt FORMEL-gruppen också tänka sig en regel som vore än mer vidsyftande än den finska, nämligen en som inte är begränsad till förvaltningen utan omfattar all kommunikation och dokumentation i samhället. Mellan de båda extrempunkterna fann gruppen olika möjliga varianter. Man kunde exempelvis tänka sig regler med generell verkan inom ett begränsat område, t.ex. en viss myndighet eller en viss typ av ärenden. En generell regel som jämställer elektroniska underskrifter med vissa traditionella formkrav hade dock avvisats redan innan gruppen inledde sitt arbete. Eftersom detta ställningstagande inte hade föregåtts av någon generell översyn av formkrav fann gruppen emellertid sig föranledd att än en gång ta ställning till denna fråga. Sammantaget var det enligt FORMEL-gruppen dock inte lämpligt att införa en regel som generellt föreskriver att exempelvis krav på underskrift får fullgöras på visst sätt med elektroniska rutiner. Gruppen ansåg inte heller att det var lämpligt att införa en regel som föreskrev detta för förvaltningen. Däremot uteslöt de inte att det kunde finnas skäl att på vissa områden införa regler som föreskrev att formkrav kunde fullgöras på visst sätt eller att samtliga kommunikationer skulle ha viss form. Avslutnings-

[140] A.a. s. 95 ff. Se även RÅ 2009 ref. 70 vad gäller bedömning av om ett krav på att ett förfarande skulle utföras ”skriftligen” var ett hinder för att använda e-post.

vis påpekade gruppen att valet av regleringstekniskt angreppssätt också hängde samman med vilken ansats som valdes i processuellt hänseende. Nya formkrav, som skulle tillåta elektroniska rutiner, måste därmed enligt gruppen utformas utifrån förutsättningarna på varje enskilt område. Gruppen föreslog alltså inga generella standardlösningar för hur formkrav borde anpassas. FORMEL-gruppen noterade också två tänkbara lösningar när det gäller förhållandet mellan traditionella formkrav och elektronisk kommunikation eller dokumentation. Det finska exemplet ovan bygger på att de traditionella formkraven i annan lagstiftning finns kvar, men anses uppfyllda på ett visst nytt sätt. Det andra alternativet angavs vara att föreskriva nya formkrav som hänför sig enbart till den elektroniska miljön och föreskriva särskilda elektroniska formkrav. Då är det alltså inte fråga om att fullgöra traditionella formkrav med nya medel, utan att ett krav på t.ex. elektronisk underskrift är ett alternativt formkrav. Båda förhållningssätten ansågs förenliga med strävan efter teknikneutralitet.[141]

Digitaliseringsrättsutredningen

Närmare femton år efter FORMEL-gruppens arbete fördjupade sig även Digitaliseringsrättsutredningen i dessa frågor. Utredningen hade dock mot bakgrund av brist på tid och resurser inte möjlighet att på nytt göra en genomgång av förekomsten av formkrav som hindrar digitala rutiner i alla gällande författningar.[142] Genom utredningens omfattande kartläggning av den offentliga förvaltningens behov identifierades dock att det, i linje med vad FORMEL-gruppen tidigare fann, på flera rättsområden fortfarande förelåg behov av att ändra författningar som innehåller formkrav för att förvaltningen helt ska kunna ersätta pappersförfaranden med digitala förfaranden. Begrepp i lagstiftningen som underskrift, undertecknande och namnteckning kom alltjämt i ljuset när myndigheter undersökte möjligheter att t.ex. anordna digitala tjänster för att inleda ärenden. Utredningens bedömning i denna del var bl.a. att det i det fortsatta arbetet var angeläget att vidta åtgärder för att anpassa gällande rätt med krav på underskrift, undertecknande eller namnteckning till digitala förfar-

[141] A.a. s. 45.
[142] *Juridik som stöd för förvaltningens digitalisering* (SOU 2018:25), s. 453.

anden. De olika formuleringarna bedömdes enligt utredningen knappast avsedda att ha olika innebörd även om det noterades att begreppet undertecknad i ett par författningar getts en teknikneutral betydelse. Någon generell slutsats innebärande att begreppet undertecknad numera skulle ha en annan innebörd än tidigare lät sig enligt utredningen dock inte göras endast med ledning av ett fåtal bestämmelser. Innebörden av formkravet bör i stället lämpligen bedömas för varje enskild bestämmelse med beaktande av den rättsliga miljö som aktuell bestämmelse finns i och hur kravet tidigare har bedömts.[143]

Digitaliseringsrättsutredningen berörde även frågan om en generell reglering. De såg det som särskilt angeläget att undersöka om de skulle kunna nå fram till en generell författningsändring i syfte att åstadkomma en förvaltningsgemensam reglering där digitala förfaranden för underskrifter så långt som möjligt likställs med pappersförfaranden. En sådan generell reglering på formkravsområdet vore särskilt önskvärd mot bakgrund av att samma begrepp ges olika innebörd i olika författningar. Sådana olikheter försvårade enligt utredningen samverkan i en digital förvaltning, där utrymmet för att tolkning och tillämpning av rättsregler ska kunna skilja sig åt mellan myndigheter eller verksamheter är mer begränsat än i den analoga miljön. Utredningen noterade att frågan bedömts två gånger tidigare och att en sådan generell bestämmelse inte då bedömts vara lämplig. Mot bakgrund av tidsramarna för utredningen och svårigheter med att göra välavvägda bedömningar om hur ett eventuellt generellt författningskrav skulle kunna utformas lämnade utredningen emellertid inget sådant förslag.[144]

8.9.4 Formkrav avseende elektroniska underskrifter

I svenska författningar finns det flera bestämmelser där det uttryckligen framgår att handlingar som ska vara undertecknade antingen ska eller får undertecknas med elektronisk underskrift. I de fall där det anges att en handling ska undertecknas elektroniskt gäller det endast när en handling upprättats eller överförs elektroniskt.[145]

Det förekommer för närvarande ingen svensk författning där det uppställs krav om att en underskrift ska ske med en kvalificerad elek-

[143] A.a. s. 464.
[144] A.a. s. 465.
[145] Se t.ex. 8 a § lagen (1974:610) om inrikes vägtransport.

tronisk underskrift. Hänvisningar till elektroniska underskrifter utformas i dagsläget på tre olika sätt. En vanligt förekommande lösning är att det i lag föreskrivs att underskriften ska vara en sådan avancerad elektronisk underskrift som avses i artikel 3 i eIDAS-förordningen.[146] Det förekommer även att hänvisningar görs till sådan elektronisk underskrift som avses i artikel 3 i eIDAS-förordningen utan att det anges att underskriften ska vara avancerad eller kvalificerad.[147] Till sist finns även exempel där det anges att en underskrift ska eller får undertecknas med elektronisk underskrift utan att hänvisning görs till eIDAS-förordningen.[148] När det gäller de två senare varianterna förekommer ibland att det delegerats till behörig myndighet att fastställa kraven på elektronisk underskrift.[149]

De krav vi har identifierat avser enkel eller avancerad elektronisk underskrift. Ett exempel där endast enkel underskrift krävs är 48 kap. 17 § andra stycket rättegångsbalken där detta kombineras med ett procedurkrav om att godkännande av strafföreläggande för ordningsbot lämnas i närvaro av polisman.

8.9.5 Teknikneutralitet som utgångspunkt

Utredningens bedömning: I syfte att uppnå en mer enhetlig och långsiktigt utformad lagstiftning bör bestämmelser som tillåter användning av elektroniska underskrifter som huvudregel vara teknikneutralt utformade. Angivande av vilken nivå av elektronisk underskrift som krävs bör endast anges i lag om det bedöms nödvändigt för att säkerställa en tillräckligt hög nivå av informationssäkerhet.

Teknikneutrala bestämmelser bör även utformas så att de också möjliggör användning av elektroniska stämplar när det är lämpligt.

[146] Se t.ex. 1 kap. 13 § aktiebolagslagen (2005:551).
[147] Se t.ex. 5 kap. 4 § andra stycket lagen (2010:921) om mark- och miljödomstolar.
[148] Se t.ex. 4 kap. 8 § tredje stycket fastighetsbildningslagen (1970:988).
[149] Se t.ex. 5 kap. 8 § förordningen (2018:759) om ekonomiska föreningar och Bolagsverkets föreskrifter om elektronisk ansökan och anmälan för vissa företag m.m. (BOLFS 2008:1).

Skälen för utredningens bedömning

Formkrav i författning som hindrar eller försvårar användning av elektroniska underskrifter förekommer fortfarande. Av vad som framkommit i samband med vår kartläggning av den offentliga förvaltningens behov har det emellertid inte framgått att detta i dagsläget skulle vara ett stort problem som hindrar användningen av elektroniska underskrifter för de aktörer vi haft kontakt med. Flera lagstiftningsärenden som undanröjer sådana hinder har även på senare år genomförts. Det kan även noteras att en begränsad typ av generell bestämmelse i linje med de som presenteras i avsnitt 8.9.3 sedan den 1 januari 2021 återfinns i 33 kap. 1 a § rättegångsbalken. Av bestämmelsen följer att en ansökan som enligt en bestämmelse i rättegångsbalken ska vara egenhändigt undertecknad får skrivas under med en sådan avancerad elektronisk underskrift i artikel 3 i eIDAS-förordningen. Nyligen tillsattes även en utredning vars uppgift är att vid behov föreslå de ändringar av bestämmelsen i regeringsformen om underskrift av regeringsbeslut som krävs för att göra bestämmelsen teknikneutral.[150]

De kvarstående hinder vi identifierat återfinns i bestämmelser som berör kommunernas verksamhet. Sambruk har i rapporten *Praktiska erfarenheter kring e-underskrifter* en sammanställning där flera exempel på hindrande eller potentiellt hindrande bestämmelser framgår.[151] I vissa fall finns hindren i myndighetsföreskrifter där angivande av att betygshandlingar ska skrivas under kombineras med krav om att underskriften ska ges ett namnförtydligande.[152]

Ett annat exempel från sammanställningen är kravet i 1 kap. 4 § föräldrabalken om att underskrifter ska bevittnas i samband med en faderskapsbekräftelse. Utredningen om faderskap och föräldraskap har föreslagit att det under vissa omständigheter ska vara möjligt att bekräfta faderskap elektroniskt.[153] I skrivande stund har regeringen inte gått vidare med utredningens förslag i denna del. Det kan i sammanhanget noteras att det i Storbritannien införts en lösning där

[150] Dir. 2020:55.
[151] Sambruk, *Praktiska erfarenheter kring e-underskrifter*, juni 2020 s. 17 ff.
[152] 14 § Skolverkets föreskrifter om utformningen av slutbetyg i grundskolan, grundsärskolan och specialskolan (SKOLFS 2011:57) och 18 § Skolverkets föreskrifter om utformningen av terminsbetyg i grundskolan, grundsärskolan, specialskolan och sameskolan (SKOLFS 2014:50).
[153] *Nya regler om faderskap och föräldraskap* (SOU 2018:68), s. 182 ff.

bevittnande av underskrifter kan ske elektroniskt. Undertecknaren och vittnet måste emellertid vara på samma ställe rent fysiskt.[154]

Vi anser att det är viktigt för digitaliseringen av den offentliga förvaltningen att arbetet med att identifiera och undanröja kvarvarande formkrav som hindrar användning av elektroniska underskrifter fortgår.

Under vår kartläggning har det dock varit tydligt att osäkerhet kring om användning av elektroniska underskrifter är tillåten upplevs som ett större hinder än bestämmelser som tydligt hindrar sådan hantering. I viss utsträckning kan domstolsavgöranden undanröja sådana oklarheter även om det inte kan anses vanligt att sådana tolkningsfrågor blir föremål för domstolsprövning.[155]

Ett mer heltäckande sätt att undanröja osäkerhet vore att införa en sådan generell reglering som tidigare föreslagits och som beskrivs i avsnitt 8.9.3. Vi anser emellertid att en generell bestämmelse innebärande att elektroniska underskrifter godtas i stället för namnteckningar kräver en mer omfattande genomgång och analys av befintliga bestämmelser än som ryms inom ramen för detta delbetänkande.

Ett ökat stöd, i enlighet med det som föreslås i avsnitt 8.6, vid bedömningar av om en bestämmelse tillåter användning av elektroniska underskrifter kommer till viss mån kunna minska den osäkerhet som råder. Ett sätt att, i vart fall på längre sikt, motverka denna osäkerhet är även enligt vår bedömning att förändra den systematik med vilken bestämmelser om användning av underskrifter och elektroniska underskrifter utformas.

I Sverige har oftast, om än inte helt enhetligt så ändå systematiskt, den i avsnitt 8.9.4 redovisade lagstiftningstekniken använts som innefattar att ändra varje bestämmelse som innehåller formkrav på så sätt att det tydliggörs att elektroniska rutiner för underskrift kan användas. Regeringen har tidigare uppmärksammat detta och konstaterat att det inte finns någon enhetlig lagteknisk lösning för hur ett formkrav för elektronisk underskrift bör se ut och att en lämplighetsbedömning i stället får göras för varje enskild bestämmelse där formkravet behöver anpassas.[156] Vi anser att detta sätt att utforma bestämmelser som uttryckligen tillåter att elektroniska underskrifter får användas

[154] www.gov.uk/government/news/hm-land-registry-to-accept-electronic-signatures (hämtad 2021-01-14).
[155] Se t.ex. Kammarrätten i Göteborgs dom den 24 september 2014 i mål nr 3459-14 avseende justering av kommunala protokoll med en elektronisk underskrift.
[156] Prop. 2017/18:126 s. 22 f.

är problematisk och ett resultat av att något samlat grepp kring frågan egentligen inte tagits sedan FORMEL-gruppens arbete. Vi ser även att FORMEL-gruppens slutsatser än i dag är mycket tongivande när det kommer till att utforma bestämmelser om underskrifter. Som tidigare nämnts var en av FORMEL-gruppens slutsatser att om en formföreskrift i lag, förordning eller myndighetsföreskrift anger att en handling ska vara försedd med underskrift, namnteckning, undertecknande eller liknande, kan detta krav inte uppfyllas med elektroniska rutiner.[157] Denna bedömning grundas i den omfattande genomgång av författningsbestämmelser gruppen utförde under 2002 och 2003. I vissa fall har detta synsätt frångåtts och begreppet undertecknad har på senare år fått en teknikneutral innebörd i ett par författningar.[158] Detta är ett tydligt avsteg från vad som uttalats i tidigare förarbeten.[159] Kravet kan enligt dessa författningar alltså uppfyllas både genom undertecknande på papper eller med elektroniska medel. I andra författningar har dock i liket med FORMEL-gruppens bedömning samma begrepp, även under senare tid, bedömts endast kunna uppfyllas genom namnteckning med penna på papper.[160] Regeringen har vidare förhållandevis nyligen uttalat att någon generell slutsats inte kan dras om att begreppet undertecknad skulle ha en annan innebörd än vid FORMEL-gruppens inventering. En enskild bedömning av formkravets innebörd får i stället enligt regeringen göras för varje bestämmelse där det förekommer. Bedömningen får enligt regeringen göras mot bakgrund av samtliga relevanta omständigheter såsom bestämmelsens rättsliga miljö och hur kravet tidigare har bedömts.[161]

eSam har, även om man noterar att begreppen används teknikneutralt i skatteförfarandelagen, i sin vägledning uttalat att FORMEL-gruppens bedömning alltjämt torde utgöra ”gällande rätt”.[162]

Även om FORMEL-gruppens bedömning enligt vår uppfattning bör vara vägledande för bestämmelser som de granskat och som fortfarande är gällande anser vi att man i lagstiftningssammanhang inte längre bör koppla samman begreppen underskrift och undertecknande med en namnteckning med penna på papper. Det finns som

[157] *Formel – Formkrav och elektronisk kommunikation* (Ds 2003:29), s. 87 f.
[158] Prop. 2010/11:165 s. 346 och prop. 2016/17:142 s. 41 och 61.
[159] Se bl.a. prop. 2001/02:142, s. 70.
[160] Se t.ex. prop. 2011/12:126 och prop. 2013/14:236.
[161] Prop. 2017/18:126 s. 22.
[162] eSam, *Juridisk vägledning för införande av e-legitimering och e-underskrifter 1.1*, juni 2018 s. 28.

tidigare nämnts exempel på när detta har frångåtts och vi anser att om begreppen underskrift eller undertecknande används i nya författningsbestämmelser bör de alltid anses vara teknikneutrala. Vi bedömer även att tekniken med att uttryckligen ange att en elektronisk underskrift kan användas kan ge upphov till mycket av den upplevda osäkerheten eftersom det då kan ifrågasättas om bestämmelser utan sådant klargörande tillåter en sådan användning.

En hänvisning till eIDAS-förordningens definitioner innebär att lagstiftaren tagit ställning till vilken nivå som krävs för en elektronisk underskrift i det aktuella sammanhanget. Att ange vilken nivå som en underskrift ska ha kan vara ett nödvändigt styrmedel för att exempelvis säkerställa en tillräcklig säkerhetsnivå. Om det till följd av informationssäkerhetsaspekter är nödvändigt att i lag säkerställa att en viss nivå av elektronisk underskrift ska användas bör detta göras. Det finns dock anledning att ifrågasätta om sådana hänvisningar som huvudregel bör ske på lagnivå. I flera befintliga bestämmelser har även dessa hänvisningar genom bemyndiganden delegerats till regeringen eller en myndighet att besluta om. Den typ av hänvisning till viss teknik som det rör sig om brukar även vanligtvis framgå längre ner i normhierarkin än i lag.

En följd av en ordning med i huvudsak teknikneutrala bestämmelser är att det inte i lag behöver anges att elektroniska underskrifter får användas. Detta hade medfört flera av de i avsnitt 8.9.2 uppräknande fördelarna eftersom explicita hänvisningar till en viss teknik eller hur den tekniken benämns åldras snabbt mot bakgrund av den snabba utvecklingen inom digitaliseringens område. Inom området elektroniska underskrifter är detta extra tydligt då det exempelvis redan skett ett skifte av begrepp från digitala signaturer till elektroniska signaturer och därefter till elektroniska underskrifter. I många bestämmelser finns som tidigare nämnts även hänvisningar till eIDAS-förordningen, dessa hänvisningar är s.k. statiska hänvisningar.[163] Detta innebär att det anges vilken lydelse av förordningen som hänvisningen görs till. Om det därefter sker ändringar i förordningen som påverkar hänvisningen måste bestämmelsen i sin tur ändras.

Vi anser sammanfattningsvis att huvudregeln vid utformningen av nya författningar som tillåter användning av elektroniska under-

[163] Se t.ex. 45 kap. 4 § rättegångsbalken, 11 § skuldsaneringslagen (2016:675), 111 kap. 5 § socialförsäkringsbalken, 2 kap. 7 § årsredovisningslagen (1995:1554) och 9 kap. 3 § lagen (2007:1091) om offentlig upphandling.

skrifter bör vara att om en bestämmelse inte uttryckligen anger att det krävs en egenhändig namnteckning ska ett krav om underskrift kunna utföras elektroniskt. Detta är även i linje med FORMEL-gruppens bedömning om hur anpassning av hindrade formkrav bör ske. FORMEL-gruppen fann att man bör eftersträva

- långsiktighet och teknikneutralitet, t.ex. genom att undvika onödig teknisk terminologi, och
- reglering på låg nivå, dvs. man bör inte ge överdrivet detaljerade föreskrifter i lag eller förordning när andra styrmedel är mer ändamålsenliga.[164]

Det går med all rätt att påpeka att en sådan huvudregel som här föreslås kan bidra till att det vid tillämpning blir ännu otydligare vad som gäller och i förlängningen ger upphov till mer osäkerhet. Som konstateras ovan används begreppen underskrift och undertecknande dock redan i dag både som teknikbundna och teknikneutrala. I brist på en lagstiftningsinsats där alla berörda bestämmelser samtidigt ändras så att de blir enhetliga ser vi en succesiv förändring som bättre än att fortsätta lagstifta på de olika sätt som nu förekommer.

Som framgår av avsnitt 8.9.2 finns det även flera nackdelar med teknikneutrala bestämmelser som behöver tas i beaktande. Vi anser dock inte att dessa nackdelar är skäl för att inte utforma författningar på ett teknikneutralt sätt. Vi delar emellertid Digitaliseringsrättsutredningens slutsats att det ställer högre krav på förarbeten att dels ge konkret rättsligt stöd till vägledning för tillämparen, dels tillvarata enskildas intressen av bl.a. transparens och förutsebarhet.[165]

Även om det inte kan anses nära förestående vill vi även lyfta att det inom en inte alltför avlägsen framtid kan bli aktuellt att helt utmönstra pappersbaserade processer ur den offentliga förvaltningen. En lagteknisk konstruktion där bestämmelsen på lagnivå är teknik- och processneutral och där formerna för hur undertecknandet ska ske regleras i förordning eller myndighetsföreskrifter hade underlättat en sådan framtida förändring. I detta sammanhang vill vi även framföra att det finns anledning att i större utsträckning även överväga teknikneutrala bestämmelser som inte endast avgränsar sig till underskrifter. Som framgår av avsnitt 8.7 ser vi att det finns stor

[164] *Formel – Formkrav och elektronisk kommunikation* (Ds 2003:29), s. 45 f.
[165] *Juridik som stöd för förvaltningens digitalisering* (SOU 2018:25), s. 127.

potential för en ökad användning av elektroniska stämplar. Det kan emellertid innebära ett behov av att författningsbestämmelser antingen medger eller genom dess utformning inte hindrar användning av stämplar. Teknikneutrala bestämmelser bör därför enligt vår mening utformas så att de också möjliggör användning av elektroniska stämplar när det är lämpligt.

Avslutningsvis ser vi det även som positivt att det nyligen genomförts ändringar i rättegångsbalken där underskriftskrav tagits bort vad gäller en åklagares stämningsansökan och en stämning som utfärdats av åklagare. Vad gäller stämningsansökan togs även ett krav bort på att underskrift inte krävs om ansökan kan överföras på ett sätt som uppfyller vissa säkerhetskrav.[166] Även om det inte kunde behandlas inom ramen för det lagstiftningsärendet lyftes även i den aktuella propositionen att det kan finnas skäl att återkomma till frågan om att undanta vissa ingivare till domstol, t.ex. myndighetsföreträdare, från ett krav på undertecknande.[167] Vi anser att det borde finnas förutsättningar för liknande förenklingar även för annan kommunikation inom förvaltningen än den som sker mellan myndigheter och domstolar. Vi skulle därför vilja betona vikten av att det i lagstiftningsärenden tas ställning till om underskriftskrav över huvud taget kan anses berättigade när den aktuella handlingen ska skickas med säkra kommunikationssätt inom den offentliga förvaltningen.

[166] Prop. 2019/20:189 s. 27 ff.
[167] A.a. s. 32.

9 Risker

9.1 Informations- och cybersäkerhet

En ökad användning av betrodda tjänster inom den offentliga förvaltningen medför stora möjligheter och nyttor, men också risker. Den ökade användningen innebär att de betrodda tjänsterna blir ett mer intressant mål för brottslighet och andra antagonister inklusive sofistikerade antagonister som kan vilja komma åt enskilda personer eller samhället i stort. De mest kvalificerade antagonistiska hoten utgörs i första hand av angrepp utförda av statliga eller statsunderstödda aktörer. Effekterna av ett sådant angrepp kan få lika stora konsekvenser för samhällsviktiga funktioner och kritiska it-system som ett konventionellt väpnat angrepp.[1]

Den ökade användningen av e-tjänster och beroendet av digitaliseringen innebär att de risker som finns behöver mötas av samhället och av den verksamhet som förlitar sig på dessa tjänster. För 15 år sedan var e-legitimationer och e-tjänster ett komplement till det vanliga pappersflödet. Då gick det även att gå tillbaka till ett pappersbaserat sätt att arbeta. Det förefaller inte alltid vara fallet i dag då det digitala är det normala och kanske enda alternativet.

Som ett steg i att hantera de risker som digitaliseringen medför tog regeringen under 2017 fram en nationell strategi för samhällets informations- och cybersäkerhet.[2] Med informations- och cybersäkerhet avses i strategin en uppsättning säkerhetsåtgärder för bevarande av konfidentialitet, riktighet och tillgänglighet hos information. Med konfidentialitet avses att obehöriga inte ska kunna ta del av informationen. Med riktighet menas att informationen inte förändras, manipuleras eller förstörs på ett obehörigt sätt. Med tillgänglighet menas här att behöriga ska kunna ha tillgång till informationen på

[1] Prop. 2020/21:30 s. 151.
[2] *Nationell strategi för samhällets informations- och cybersäkerhet*, Skr. 2016/17:213.

det sätt och vid den tidpunkt som tjänsterna erbjuder. För informationssäkerhet som avser digital information används i strategin även begreppet cybersäkerhet.[3] Detta begrepp är vanligt förekommande i en internationell kontext. Inom ramen för detta delbetänkande kommer vi dock endast att använda oss av begreppet informationssäkerhet.

9.2 Förutsättningar för säkra betrodda tjänster

Det krävs en komplex kedja av teknik, processer och kunskap för att betrodda tjänster ska ge det skydd som avsetts. De betrodda tjänsterna använder krypteringsalgoritmer och hashalgoritmer. De krypteringsalgoritmer som används för betrodda tjänster i Europa och Sverige är framför allt RSA[4] och eliptiska kurvor (ECDSA).[5] Den hashalgoritm som används är främst SHA-2.[6] I en mindre utsträckning används även blockkedjeteknik.

För att kryptolösningar ska vara tillräckligt säkra finns det sju viktiga faktorer som beskrivs i avsnitten nedan tillsammans med de risker som brister inom respektive område kan medföra. Dessa faktorer som beskrivs i avsnitt 9.2.1–9.2.7 är en vidarebearbetning, med utgångspunkt för betrodda tjänster, av de faktorer som utredningen NISU 2014 lyfte fram i sitt förslag till nationell strategi och åtgärdsplan för säkra kryptografiska funktioner.[7]

Utöver riskerna med kryptolösningar beskrivs i avsnitt 9.2.8–9.2.9 ett antal andra risker som tillhandahållandet och användandet av betrodda tjänster för med sig.

9.2.1 Säkra kryptografiska algoritmer

Säkra kryptografiska algoritmer innebär att de matematiska algoritmer som ligger till grund för skyddet inte innehåller svagheter som kan utnyttjas av en angripare. Om en krypteringsalgoritms styrka innehåller svagheter kan – i värsta fall – samtliga säkerhetsfunktioner

[3] A.a. s. 4.
[4] Förkortningen består av begynnelsebokstäverna i upphovsmännens efternamn (Rivest, Shamir och Adleman).
[5] Eliptic Curve Digital Signature Algorithm.
[6] Secure Hash Algortihm 2.
[7] *Informations- och cybersäkerhet i Sverige – Strategi och åtgärder för säker information i staten* (SOU 2015:23) s. 303.

som baseras på denna algoritm slås ut i det ögonblick detta blir allmänt känt. Det skulle inte gå att skilja en korrekt transaktion från en förfalskad. Det skulle t.ex. innebära att, för de tjänster som baseras på algoritmen, samtliga e-legitimationer skulle gå att förfalska och all datatrafik gå att avlyssna eller förfalska. Inloggningar är inte längre säkra. All information som någonsin krypterats med en kompromitterad algoritm måste betraktas som röjd. Detta kan leda till extremt omfattande informationsförluster och en sådan incident vore även direkt samhällsfarlig. Tidigare har flera väl etablerade kryptoalgoritmer fasats ut då brister i dessa har blivit kända. Detta gäller i samband med elektroniska underskrifter och stämplar inte bara krypteringsalgoritmer utan även hashalgoritmer. Ett exempel på detta är att det i hashalgoritmen SHA-1 upptäcktes att olika informationsmängder kunde ge samma hashvärde efter ett mindre antal matematiska operationer än vad algoritmen ursprungligen var avsedd för[8]. När sårbarheten upptäcktes började användningen av algoritmen fasas ut. Utfasningen skedde främst vid användning för elektroniska underskrifter och stämplar där skyddet behöver bevaras länge, medan det inte sågs som lika problematiskt för skydd av kortlivad information där algoritmen används för att skydda transaktioner eller sessioner. Bakgrunden till utfasningen är att efter upptäckt av en sårbarhet brukar attacker utvecklas, förfinas och förbättras så att en algoritms styrka eroderar än mer.

9.2.2 Säkra standarder

Ytterligare en förutsättning för tillräckligt säkra betrodda tjänster är att de matematiska algoritmerna översatts till säkra standarder. Om en standard skulle innehålla brister kan det få liknande konsekvenser som i avsnittet ovan, till dess att standarden åtgärdats och samtliga system uppdaterats. Även denna typ av incident kan bli direkt samhällsfarlig, eftersom den kan komma att omfatta många produkter och system samtidigt och det kan också ta lång tid innan nödvändiga uppdateringar genomförts. Historiskt har flera sådana brister upptäckts. När RSA först användes för kryptering visade det sig exempelvis ha inneboende sårbarheter som medförde att om en text kryp-

[8] Rijmen, Vincent och Oswald, Elisabeth, *Update on SHA-1,* Cryptology ePrint Archive: Report 2005/010, 20 januari 2005.

terades rakt av utan att använda tillägg av slumpmässiga tecken i början, mitten eller slutet av informationen, s.k. ”padding”, kunde den krypterade informationen räknas ut med hjälp av ett antal andra krypterade meddelanden som använder samma publika nyckel.[9] RSA används därför alltid tillsammans med sådana slumpmässiga tecken.

9.2.3 Säkra it-produkter

Säkra it-produkter förutsätter att produktutvecklarna implementerat valda standarder korrekt och att produkterna i övrigt är fria från sårbarheter som skulle kunna utnyttjas av en angripare. Om kryptostandarden är felaktigt implementerad i en produkt på ett sådant sätt att det finns brister, kan samtliga system där en sådan produkt finns installerad drabbas. Beroende på den enskilda produktens spridning och användningsområde kan sådana incidenter drabba berörda användare och även bli samhällsfarliga.

Exempel på incidenter till följd av fel i säkra it-produkter är den s.k. ROCA-sårbarheten som det redogörs för i avsnitt 9.3.2.

9.2.4 Säkra systemarkitekturer

Med säkra systemarkitekturer avses att it-produkterna kombinerats på ett sådant sätt att det önskade skyddet uppnås. Att etablera säkra system som består av olika komponenter (it-produkter) är en komplicerad uppgift som kräver särskild kompetens. Om ett system inte har rätt arkitektur kan det leda till brister vilka i sin tur kan leda till mer eller mindre allvarliga incidenter för det berörda systemet. På nationell nivå är det rimligt att anta att det finns många system med bristfällig arkitektur (eller implementation, se avsnitt 9.2.5). Om det finns många sådana system leder det till en aggregering av risk och att viktiga samhällsfunktioner inte har it-system som är robusta nog.

[9] Hastad, J., *N Using RSA with Low Exponent in a Public Key Network*, Williams H.C. (eds) Advances in Cryptology – CRYPTO’85 Proceedings, CRYPTO 1985, Lecture Notes in Computer Science, vol 218, Springer, Berlin, Heidelberg, 1986.

9.2.5 Säkra systemimplementationer

Med säkra systemimplementationer avses att systemintegratörer skapar system där krypteringsfunktionerna används korrekt, upplevs tillräckligt användaranpassade och inte innehåller konfigurationsmisstag eller andra sårbarheter som kan utnyttjas av en angripare. Om en systemintegratör gör misstag då ett visst system etableras kan den berörda verksamheten drabbas av mer eller mindre allvarliga incidenter. En sådan incident kan vara allvarlig för det berörda systemet.

9.2.6 Säker nyckelhantering

Med säker nyckelhantering avses att de krypteringsnycklar som används i förekommande fall har genererats, distribuerats, använts och destrueras på ett säkert sätt, dvs. att nycklarna inte i något led i kedjan kan användas av någon obehörig. Om nyckelhanteringen inte är säker kan samtlig information som skyddats med de berörda nycklarna vara komprometterad. Om en nyckel röjts är all information som krypterats med denna nyckel att betrakta som komprometterad. Eftersom nycklar i många tillämpningar inte byts ut regelbundet kan detta innebära mycket stora informationsförluster. Beroende på den information som skyddats kan nyckelincidenter vara mycket allvarliga. Det beror även på vilken nivå det sker, om det är en certifikatutfärdares nyckel som röjs berörs alla certifikat som utfärdats i den infrastrukturen medan om en persons nyckel röjs berörs endast de underskrifter eller stämplar som nyckeln använts till.

9.2.7 Utbildade användare

Användare måste förstå hur de använder systemen korrekt, vara medvetna om riskerna med felaktig användning samt omedelbart anmäla förlorade nycklar och andra relevanta incidenter. Om användarna inte är utbildade kan det leda till nyckelincidenter och/eller att obehöriga får tillgång till systemen, vilket kan få följdverkningar. Användarna behöver även vara medvetna om att det kan finnas bedragare

som försöker få dem att logga in bedragaren snarare än sig själv i olika system och tjänster.[10]

9.2.8 Validering med stöd av förteckningar som tillhandahålls av privata aktörer

I samband med kartläggningsarbetet har vi träffat flera aktörer som hänvisar till att de vill använda elektroniska underskriftstjänster som inte ger något varningsmeddelande för de interna eller externa parter som förlitar sig på underskrifterna. Flera programvaror som används av offentlig förvaltning använder tillitsförteckningar som privata företag tillhandahåller (se mer om dessa förteckningar i avsnitt 5.12.2), t.ex. Adobe Acrobat som utöver EU:s medlemsstaters tillitsförteckningar även kan validera andra tillhandahållare som finns i Adobes egen förteckning. Även olika webbläsare och operativsystem använder tillitsförteckningar som privata företag tillhandahåller. Det gör det svårt för användare att veta om t.ex. en elektronisk underskrift har skapats av en betrodd tjänst som finns med i någon av EU:s medlemsstaters tillitsförteckningar eller inte. Flertalet av dessa programvaror har transparanta processer för hur utfärdare läggs till i tillitsförteckningarna men det innebär samtidigt att användare av dessa förteckningar automatiskt litar på ett antal utfärdare utan att ha någon egentlig egen kontroll över vilken säkerhet de erbjuder.

9.2.9 Övriga risker

Ett säkert tillhandahållande av betrodda tjänster är beroende av ett systematiskt och riskbaserat informationssäkerhetsarbete som ständigt förbättras. I det systematiska informationssäkerhetsarbetet ingår bl.a. ändamålsenliga arbetssätt för riskhantering, införande av säkerhetsåtgärder, uppföljning, incidenthantering och kontinuitetsplanering. Dessa arbetssätt är avgörande för att tillhandahållare av betrodda tjänster ska kunna identifiera, införa och upprätthålla tillräck-

[10] Se t.ex. Allmänna reklamationsnämndens referat 2019-11253 för en exemplifiering av hur ett sådant bedrägeri kan gå till. Utöver exemplet som rör en situation där någon efter ett telefonsamtal blivit lurad att ge bedragaren tillgång till en e-tjänst finns även webbtjänster eller mobilapplikationer där en person loggar in själv, men där den verkliga inloggningen sker mot en annan bakomliggande e-tjänst eller bastjänst som den som loggar in inte ser. Se mer om det senare förfarandet i eSam, *Åtgärder mot att användare vilseleds att logga in någon annan med sin e-legitimation* (dnr/ref: 2018-57), juni 2018.

liga tekniska och organisatoriska säkerhetsåtgärder, som vid brister kan påverka säkerheten och förtroendet för tillhandahållaren och dess tjänster. Här följer exempel på sådana säkerhetsåtgärder och risker.

Om tillhandahållaren utfärdar certifikat behöver denne ha en tillförlitlig identifiering av personen som certifikatet utfärdas till. Även med tillförlitliga identifieringslösningar finns det risker för att grundidentiteten är falsk och vid indirekta identifieringsmetoder finns risken att det är någon annan som använder identiteten. Ett certifikat kan användas mot många olika förlitande parter och om fel person kan använda det kan konsekvenserna bli allvarliga.

En tillhandahållare behöver ha personal med rätt kompetens, uppdragstagare och underleverantörer som är tillförlitliga och kompetenta på området och som arbetar efter överenskomna och ändamålsenliga arbetssätt. Det behöver även finnas personal med rätt kompetens att rekrytera. Något som givetvis försvåras av den brist på personer med it-kompetens som för närvarande finns.[11] Tillhandahållare behöver arbeta efter ändamålsenliga processer för att tillhandahålla tjänsten. Om inte finns risken för att en enskild anställd av misstag eller av illvilja kan påverka tjänsten. För känsligare processer brukar minst två anställda gemensamt behöva genomföra åtgärden tillsammans, t.ex. användandet av certifikatutfärdarens privata nyckel för att utfärda certifikat.

Tillhandahållaren behöver vidare vidta ett antal tekniska åtgärder, t.ex. använda tillförlitliga system och produkter som säkerställer tillgång endast till behöriga.

Förlitande parter behöver också ha processer för att kontrollera äktheten i t.ex. en elektronisk underskrift och säkerställa integriteten i den information som undertecknats. Det finns även risker i format som används, t.ex. XML och PDF, avseende förändringar som kan ske av information som inte omfattas av den elektroniska underskriften. Det har även funnits sårbarheter i formaten för underskrifter som sådana som medfört att förändringar av undertecknad information har gjorts utan att det visat fel i samband med validering av underskriften.[12]

[11] IT & Telekomföretagens rapport *IT-kompetensbristen*, 17 december 2020. Hämtad från www.almega.se/app/uploads/sites/2/2020/12/ittelekomforetagen-it-kompetensbristen-2020-online-version.pdf (hämtad 2021-01-25).
[12] T.ex. den s.k. Shadow-attacken mot PDF-dokument: https://news.rub.de/english/press-releases/2020-07-22-it-security-content-signed-pdf-documents-can-be-changed-unnoticed (hämtad 2021-01-29).

9.3 Kända säkerhetsincidenter och dess konsekvenser

9.3.1 DigiNotar

DigiNotar var en utfärdare av certifikat, bl.a. kvalificerade certifikat, som var verksam i Nederländerna. De sålde certifikat, inklusive certifikat för autentisering av webbplatser på den globala marknaden, men även certifierade kvalificerade certifikat i Nederländerna. Den 19 juli 2011 upptäckte DigiNotar att de blivit utsatta för intrång, inklusive att falska certifikat utfärdats utan DigiNotars vetskap. Dessa certifikat spärrades och DigiNotar tog in hjälp för att utreda intrånget. I slutet av juli trodde de att de klarat av intrånget men den 28 augusti 2011 publicerade någon ett falskt certifikat som pekade på Googles domän som utfärdats av DigiNotar. Detta certifikat hade använts i veckor för s.k."man in the middle"-attacker som påverkat ca 300 000 användare, främst i Iran. Trafik som skulle till olika underdomäner till Google, t.ex. Gmail skickades till andra sidor där exempelvis personers inloggningsuppgifter kan ha fångats upp.[13]

Utredningen visade att ett första intrång skedde i DigiNotars nät den 17 juni 2011. Nätverket var segmenterat och det säkra nätsegmentet som innehöll de servrar som utfärdade certifikaten var inte direkt åtkomliga via internet. Genom att tunnla sig genom andra komprometterade system i DigiNotars nätverk lyckades angriparen komma åt det säkra nätsegmentet den 1 juli 2011. Första försöket att skapa ett falskt certifikat skedde den 2 juli och angriparen lyckades skapa ett första certifikat den 10 juli.

DigiNotar hade åtta servrar som användes för att utfärda certifikat och alla åtta var komprometterade. Behandlingshistoriken och loggarna fanns på samma servrar och dessa hade manipulerats. Det gjorde att det var svårt att se vad angriparen hade gjort. Angriparen hade under intrången använt flera proxyservrar för att gömma sig. Enligt företaget som genomförde utredningen fanns dock flera spår som pekade på en angripare från Iran. Syftet med intrånget föreföll vara att använda falska certifikat för att spionera på ett stort antal användare i Iran.

Företaget fann inga bevis för att angriparen utfärdade några kvalificerade certifikat, men i loggarna fanns två serienummer till certifikat som inte kunde kopplas till tidigare utfärdade certifikat. Med beak-

[13] Hoogstraaten, Hans, *Black Tulip Report of the investigation into the DigiNotar Certificate Authority breach*, 10.13140/2.1.2456.7364, 2012.

tande av att loggarna manipulerats är ingen helt säker på om några kvalificerade certifikat utfärdades av angriparen eller ej.

Intrånget fick till följd att förtroendet från kunderna och den nederländska tillsynsmyndigheten, Dutch Independent Post and Telecommunications Authority (OPTA) var förbrukat. OPTA beslutade den 7 september 2011 att dra tillbaka DigiNotars status som kvalificerad tillhandahållare och gav DigiNotar två dagar på sig att reagera. OPTA drog tillbaka statusen den 14 september 2011 och beslutade att DigiNotar skulle informera sina kunder och spärra alla utfärdade certifikat. Anledningen var bl.a. att de bröt mot ett antal regler men främst att intrånget i servern som utfärdar kvalificerade certifikat gjorde att tillförlitligheten till utfärdade certifikat inte längre kunde garanteras. DigiNotar fick spärra samtliga utfärdade certifikat och bolaget gick sedermera i konkurs.[14]

Den nederländska staten använde DigiNotars certifikat i stor utsträckning, men då framför allt för autentisering av webbservrar. Det innebar att de behövde byta ut dessa certifikat. I Nederländerna användes främst DigiNotars kvalificerade certifikat av två grupper, notarius publicus och utmätningsmän för förändringar avseende ägarskap till fastigheter och fast egendom.

För de enskilda personer som köpt och använt DigiNotars kvalificerade certifikat blev dessa värdelösa när de spärrades och de behövde hitta en annan tillhandahållare.[15]

9.3.2 ROCA-sårbarheten

Forskare från Masaryks universitet i Tjeckien upptäckte under år 2017 en sårbarhet i den anordning som används för att skapa kryptografiska nyckelpar i ett stort antal utfärdade elektroniska id-kort inom EU.[16] På det elektroniska id-kortet genereras och lagras nyckelparet och det elektroniska id-kortet utgör en anordning för skapande av kvalificerade elektroniska underskrifter. Akronymen ROCA står för

[14] Enligt presentation av den dåvarande nederländska tillsynsmyndigheten OPTA på FESA-möte i Warszawa den 8 november 2011.
[15] A.a.
[16] Nemec, M. m.fl., *The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli*, ACM SIGSAC Conference on Computer and Communications Security, 2017, s. 1631 ff.
Hämtad från https://crocs.fi.muni.cz/_media/public/papers/nemec_roca_ccs17_preprint.pdf (hämtad 2021-01-14).

”Return Of Coppersmith’s Attack” och Coppersmith är benämningen på en metod för att attackera kryptografiska lösningar.

De tjeckiska forskarna fann att algoritmen som användes för att skapa certifikaten för de elektroniska id-korten genererade för lite variation i sina svar, dvs. slumptalsgenereringen för nyckelparen. Det gick därför att med datorkraft förfalska avancerade och även kvalificerade elektroniska underskrifter där dessa sårbara elektroniska id-kort hade använts.

Flera medlemsstater i EU har därför behövt utfärda nya elektroniska id-kort och personer som ingår avtal baserade på elektroniska underskrifter genererade via dessa sårbara elektroniska id-kort löper en risk att underskrifterna är förfalskade[17].

Det finns flera länder i EU som har utfärdat elektroniska id-kort med den här sårbarheten. Det gäller exempelvis elektroniska id-kort utfärdade i Estland, Spanien, Slovakien, Österrike och Tyskland.[18] Sårbarheten påverkar även som nämnts alla de som har slutit avtal med någon som har undertecknat avtalet med hjälp av ett sårbart elektroniskt id-kort. Detta medför att problemet med sårbarheten drabbar hela EU.

Sårbarheten i de elektroniska id-korten kan endast åtgärdas genom att byta ut algoritmen i certifikaten, dvs. i nyckelparet. Om det inte från kortets utfärdandedatum redan är förberett för att ett kort ska kunna hantera ytterligare algoritmer är det inte möjligt att lägga till i efterhand. Det är en del av säkerheten för elektroniska identiteter som är överförda till något föremål som exempelvis ett chip eller ett smartkort att algoritmer inte kan förändras efter chippets eller kortets utfärdande.

Flera länder har spärrat ett stort antal nationella elektroniska id-kort och bytt ut dessa, bl.a. Estland och Spanien. Utfärdarna av certifikaten som innehåller sårbarheten kan även spärra dessa på en lista. Detta har dock ingen retroaktiv verkan på de underskrifter som har skapats under tiden som certifikatet var giltigt och de underskrifterna är fortsatt sårbara.

En person som vill veta om den kan förlita sig på en underskrift skapat av ett elektroniskt id-kort kan låta validera underskriften. Det

[17] EU Joinup, Estonia, Spain and Slovakia tackle smart card vulnerabilities: https://joinup.ec.europa.eu/collection/egovernment/news/fake-esignatures (hämtad 2021-01-14).
[18] Republic of Estonia, Information System Authority, *ROCA Vulnerability and eID: Lessons Learned.* Hämtad från: www.ria.ee/sites/default/files/content-editors/kuberturve/roca-vulnerability-and-eid-lessons-learned.pdf (hämtad 2021-01-14).

betyder att personen elektroniskt, via en betrodd tjänst som utför validering, kontrollerar om den elektroniska underskriften är giltig. Det finns dock ingen skyldighet för en valideringstjänst att pröva om en elektronisk underskrift är baserad på ett elektroniskt id-kort som är drabbad av en sårbarhet.

Sårbara kort har använts för att skapa kvalificerade elektroniska underskrifter i Europa. Det är svårt att som förlitande part se om en elektronisk underskrift omfattats av sårbarheten eller inte. Om en underskrift gör det innebär det att den undertecknade informationsmängden till ganska liten kostnad och arbetsinsats kan förändras utan att det upptäcks.

9.4 Risker kopplade till samhällets beroende av betrodda tjänster

Digitaliseringen innebär ett ökat beroende av betrodda tjänster. Det gör även att konsekvenserna om de betrodda tjänsterna fallerar blir mer omfattande i dagsläget än tidigare. En incident som påverkar tillgängligheten kan vara besvärlig och på lång sikt allvarlig eftersom ingen kan använda tjänsterna. Tillgängligheten kan t.ex. påverkas av en överbelastningsattack där någon angriper systemet genom att skicka så mycket trafik till en resurs att den blir otillgänglig. En sådan attack skedde exempelvis mot BankID under våren 2020.[19]

Incidenter som påverkar riktighet och konfidentialitet är dock normalt sätt betydligt värre. Om en enskild person avslöjar sin privata nyckel eller PIN-kod som skyddar den privata nyckeln är det allvarligt för den och alla som förlitar sig på underskrifter som denne skapar. Incidenter likt DigiNotar, där det misstänks att någon kommer åt en utfärdares privata nyckel är betydligt värre och drabbar alla som har eller förlitar sig på certifikat som utfärdaren utfärdat. Riktighetsincidenter kan också medföra ett tappat förtroende för de betrodda tjänster som omfattas av incidenten. Om en väl spridd implementation eller en krypteringsalgoritm drabbas kan hela samhället påverkas.

Det finns även risker med att användare av betrodda tjänster luras att använda dessa åt någon annan. Betrodda tjänster, då främst elek-

[19] Dagens Nyheters rapportering om att Bank-ID utsatts för en attack: www.dn.se/ekonomi/bank-id-utsatt-for-attack-svart-att-veta-vem-som-ar-angriparen/ (hämtad 2021-01-14).

troniska underskrifter och stämplar, används i olika sammanhang i transaktioner som kan röra stora värden. Det finns därför incitament för kriminella att använda dessa kanaler. Om sådana bedrägerier blir omfattande, riskerar hela förtroendet för betrodda tjänster, eller åtminstone de utsatta betrodda tjänsterna, att erodera.

När samhället i större utsträckning förlitar sig på betrodda tjänster kan omfattande incidenter få förödande konsekvenser för den enskilda verksamheten och för samhället i stort. Risken är ytterst att förtroendet hos allmänheten för offentlig förvaltning allvarligt kan skadas beroende på vad tjänsterna används till och hur en eventuell incident hanteras. Om incidenter motsvarande DigiNotar eller ROCA-sårbarheten skulle inträffa och få en betydande påverkan på Sverige skulle det sannolikt inverka på såväl ledning som operativ teknisk hantering och kriskommunikation med allmänhet, media och drabbade aktörer. Resurser för den typen av insatser behöver säkras och övas på för att dimensionera organisationerna som ansvarar för den betrodda tjänsten och tillhörande infrastruktur. Det förutsätter att tekniska experter snabbt kan förklara vad som är problemet för både ledning, som ska fatta svåra beslut om eventuell nedstängning med alla störningar det kan innebära, och kommunikatörer som ska förklara vad som hänt för allmänhet, media och andra drabbade organisationer. Detta kräver kontinuitetsplanering, i förväg uppbyggd samverkan och gemensamma forum samt övning.

9.5 Hantering av risker

eIDAS-förordningen och andra regelverk är tillsammans med de lagstadgade kontrollerna och tillsynen till för att tillhandahållare ska uppfylla de säkerhetskrav som krävs för att tillhandahålla betrodda tjänster. Det finns dock ett antal omfattande incidenter, däribland de som beskrivs ovan, som har inträffat trots regelverket och som pekar på risker som behöver hanteras. Riskerna kan behöva hanteras på såväl nationell nivå som av respektive verksamhet som förlitar sig på tjänsterna.

Varje verksamhet ansvarar för att använda de betrodda tjänster som är anpassade efter deras behov av säkerhet och de risker den verksamheten är utsatt för. Det gör att vissa betrodda tjänster kanske

enbart kan användas där fel inte kan leda till omfattande konsekvenser medan andra verksamheter eller verksamhetsdelar har andra krav.

Enskilda statliga myndigheter ska i enlighet med MSB:s föreskrifter om informationssäkerhet för statliga myndigheter bl.a. arbeta utifrån de risker och behov som myndigheten identifierar, men även identifiera och hantera behovet av kontinuitet för behandling av information. I detta ingår risker kopplade till användningen av betrodda tjänster.[20] Myndigheter kan därför behöva säkerställa att det finns alternativa metoder och arbetssätt om betrodda tjänster i de normala flödena inte kan användas och utföra övningar för att testa att en sådan kontinuitetsplan fungerar. Myndigheter behöver även i dessa sammanhang analysera risken för att de tjänster som de erbjuder utsätts för brottslig verksamhet. Det finns för närvarande ingen möjlighet till tillsyn och därmed extern kontroll och granskning av efterlevnaden av bestämmelserna i föreskrifterna. Detta riskerar att minska tilliten till att reglerna följs.

Det finns även andra åtgärder som en enskild tillhandahållare av betrodda tjänster, en enskild organisation eller samhället i stort kan göra för att minska riskerna. Det kan t.ex. vara att

- inte bara förlita sig på enbart en tillhandahållare,
- inte enbart använda och vara beroende av endast en krypteringsalgoritm,
- planera för vad som behöver göras om en omfattande incident skulle inträffa, och
- som enskild organisation planera för hur man hanterar en situation där de betrodda tjänster som används i verksamheten är otillgängliga respektive kompromitterade, t.ex. genom kontinuitetsplaner och övningar.

[20] Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS 2020:6).

10 Konsekvenser

10.1 Nollalternativet

Ett nollalternativ innefattar en bedömning av vad som händer om de av utredningen föreslagna åtgärderna inte genomförs. Både Utredningen om effektiv styrning av nationella digitala tjänster och Digitaliseringsrättsutredningen konstaterade att den digitala utvecklingen har begränsningar vad gäller förutsebarhet.[1] Vi delar denna bedömning. Det är av denna anledning svårt att bedöma påverkan av ett nollalternativ på längre sikt. På kort sikt bedömer vi att det finns en risk att den offentliga förvaltningen går miste om samordningsvinster. Det senare kan bl.a. vara att en avsaknad av ett reformerat och utökat stöd leder till att många myndigheter, likt i dag, på var sitt håll eller i sammanslutningar utreder likartade frågeställningar. En avsaknad av en nationell valideringstjänst kan även leda till ökade kostnader för den offentliga förvaltningen om varje myndighet behöver anskaffa eller utveckla en lösning för validering. De svårigheter som i dag finns rörande validering kommer även att kvarstå.

Ett nollalternativ kan även innebära att digitaliseringen av den offentliga förvaltningen inte sker i lika snabb takt då exempelvis en avsaknad av en tillitsförteckning med icke kvalificerade tillhandahållare och deras tjänster kan bidra till fortsatta svårigheter att validera elektroniska underskrifter och stämplar. Därtill kommer det vara fortsatt osäkerhet kring om en betrodd tjänst som har skapat en underskrift, eller tillhandahållaren av tjänsten, lever upp till de krav som ställs i eIDAS-förordningen. Även avsaknaden av det ovan nämnda utökade och reformerade stödet kan påverka digitaliseringstakten.

Att inte genomföra de förslag som avser att underlätta bevarande av elektroniska underskrifter och stämplar samt att undanröja den

[1] *reboot – omstart för den digitala förvaltningen* (SOU 2017:114), s. 433 och *Juridik som stöd för förvaltningens digitalisering* (SOU 2018:25), s. 521.

osäkerhet som finns om hur bevarandet ska ske kan även påverka hur snabbt digitaliseringen av vissa processer sker. Det kan även leda till en ökad risk för att bevarande och gallring inte sker i enlighet med det arkivrättsliga regelverket.

10.2 Konsekvenser för kommuner och regioner

10.2.1 Konsekvenser för den kommunala självstyrelsen

I 14 kap. 3 § regeringsformen anges att en inskränkning i den kommunala självstyrelsen inte bör gå utöver vad som är nödvändigt med hänsyn till de ändamål som föranlett den. En lagstiftning som ställer upp krav för en kommunal verksamhet minskar generellt sett kommunernas möjligheter att själva göra prioriteringar i sin verksamhet.

Vi bedömer att förslagen i detta delbetänkande inte får några konsekvenser för den kommunala självstyrelsen.

10.2.2 Kommunala finansieringsprincipen

Kommunala finansieringsprincipen innebär att om staten inför nya eller ändrade föreskrifter som ändrar skyldigheter för kommunerna och regionerna kan detta påverka dessas kostnader. För att hantera sådana konsekvenser har i samförstånd mellan staten, kommunerna och regionerna en finansieringsordning utvecklats, den s.k. kommunala finansieringsprincipen. Principen och dess tillämpning är inte lagfäst, men har godkänts av riksdagen.[2]

Den kommunala finansieringsprincipen omfattar enbart statligt beslutade åtgärder som tar sikte på verksamheter. Principen innebär att staten inte bör införa nya obligatoriska uppgifter för kommuner och regioner, göra tidigare frivilliga uppgifter obligatoriska, ändra ambitionsnivån på befintliga uppgifter eller göra regeländringar som påverkar kommuners möjligheter att ta ut avgifter utan medföljande finansiering, t.ex. i form av höjda statsbidrag. En förändring som leder till sänkta kostnader för kommunerna och regionerna ska på motsvarande sätt innebära minskade bidrag.

Vi bedömer att förslagen i detta delbetänkande inte leder till några kommunalekonomiska konsekvenser som enligt den kommunala

[2] Prop. 1993/94:150 bil. 7 avsnitt 2.5.1, bet. 1993/94:FiU19, rskr. 1993/94:442.

finansieringsprincipen ska kompenseras genom anslag på statens budget. Även om förslagen kan leda till besparingar för enskilda kommuner och regioner bedömer vi inte heller att detta utgör grund för minskade bidrag.

10.3 Konsekvenser för brottsligheten och det brottsförebyggande arbetet

Av skäl 2 i eIDAS-förordningens ingress framgår att förordningen syftar till att öka förtroendet för elektroniska transaktioner på den inre marknaden, genom att tillhandahålla en gemensam grund för ett säkert elektroniskt samspel mellan medborgare, företag och myndigheter. Användning av betrodda tjänster kan öka säkerheten exempelvis för granskning av egenhändiga namnteckningar jämfört med elektroniska underskrifter. En äkthetskontroll av en namnteckning kräver tidigare kännedom om namnteckningens utformning och är därtill resurskrävande (se mer om detta i avsnitt 4.2.2). Med en elektronisk underskrift ges både enklare och bättre förutsättningar för att koppla en underskrift till en specifik individ. Den elektroniska underskriften har därtill en stark koppling till innehållet som skrivits under. Denna ökade säkerhet kan bl.a. försvåra förfalskning av handlingar och underskrifter som kan ske som ett led i olika typer av brottslighet, bl.a. välfärdsbrottslighet.[3]

Teknik kan emellertid även användas som medel för att utföra brottsliga handlingar. Flera av de tjänster som finns på marknaden för att skapa elektroniska underskrifter använder e-legitimation för autentisering av den användare som ska skriva under. ID-kortsutredningen konstaterade att de risker som är förknippade med en elektronisk identifiering primärt uppstår vid identifieringen i samband med att en person skaffar e-legitimationen.[4] Detta är emellertid, enligt vår uppfattning, framför allt något som alltså har koppling till användning av e-legitimation och inte användning av betrodda tjänster, även om sådan användning av e-legitimationer givetvis kan leda till att det exempelvis skapas elektroniska underskrifter som används i brottsliga syften. Ingen av utredningens förslag bedöms öka riskerna för identitetsrelaterad brottslighet.

[3] Jfr *Kvalificerad välfärdsbrottslighet – förebygga, förhindra, upptäcka och beivra* (SOU 2017:37), s. 354 ff.
[4] *Ett säkert statligt ID-kort – med e-legitimation* (SOU 2019:14), s. 317.

Utredningens förslag bedöms vidare stödja det brottsförebyggande arbetet genom att det ökade stödet till den offentliga förvaltningen avseende betrodda tjänster kommer medvetandegöra om risker för missbruk och hur tjänster kan utformas för att motverka sådant missbruk.

En ökad användning av betrodda tjänster, där de faktorer som framgår av kapitel 9 beaktas, kan även leda till ökad informationssäkerhet och således även på detta sätt ha brottsförebyggande effekt.

10.4 Konsekvenser för sysselsättningen

Vi bedömer att förslagen inte får några direkta konsekvenser för sysselsättningen.

10.5 Konsekvenser för offentlig service i olika delar av landet

Förslagen i detta delbetänkande avser att leda till, i de fall där behov finns, en ökad användning av betrodda tjänster. Detta kan öka tillgången till digital offentlig service på distans i hela landet.

10.6 Konsekvenser för små företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt i förhållande till större företags samt konsekvenser för företag i stort

Av 15 § i kommittéförordningen (1998:1474) följer att konsekvenserna av förslagen för små företag särskilt ska anges om de har betydelse för denna grupp. Utredningen ska enligt direktiven även särskilt ange konsekvenser för företag i form av kostnader och ökade administrativa bördor. Nedan presenteras konsekvenserna för små företag. Det som anges om kostnader och administrativ börda kan även appliceras på medelstora och stora företag. Givetvis med den skillnaden att kostnader och administrativa bördor får anses vara mindre betungande för dessa företag.

Flera av de företag som tillhandahåller tjänster för skapande av avancerade elektroniska underskrifter är små. Dessa företag har i stort

sett varit utestängda från att sälja sina tjänster till svenska myndigheter i och med de ramavtal som tecknats och den lösning som primärt används i form av en fristående underskriftstjänst.

Förslaget om att icke kvalificerade tillhandahållare får föras upp på tillitsförteckningen kommer, för de företag som önskar vara med, troligen innebära en viss administrativ börda samt kostnad för att inkomma med ansökan och möta de krav som kommer ställas. Därutöver kommer en årlig avgift behöva erläggas. Årsavgiften kommer dock sannolikt att vara relativt låg då den begränsas av 11 § förordningen (2016:602) om finansiering av Post- och telestyrelsens verksamhet som anger att avgiften som mest får vara 25 000 kronor per år per tillhandahållare av betrodda tjänster.

Att finnas i tillitsförteckningen kommer sannolikt att vara attraktivt eftersom det troligen kommer uppställas som ett krav från de flesta aktörer i offentlig förvaltning vid anskaffning av betrodda tjänster. Därtill kan det även ses som en kvalitetsstämpel bland potentiella kunder i den privata sektorn.

Den sammanvägda bedömningen är att det kommer att vara förenat med vissa begränsade kostnader och en viss administrativ börda att finnas i tillitsförteckningen, men att det kommer att underlätta marknadsinträde och öppna upp möjligheten för den som är uppförd på förteckningen att utöka sin kundkrets.

Utöver tillhandahållare av betrodda tjänster berörs också andra företag av vårt förslag om nationell valideringstjänst, eftersom vi föreslår att även privata utförare inom främst utbildnings-, vård- och omsorgssektorerna ska kunna använda tjänsten för validering av elektroniska underskrifter och stämplar. För dessa företag innebär tillgång till tjänsten enligt vår bedömning ökade möjligheter att kunna validera sådana underskrifter och stämplar, något som kan bidra till ökad effektivisering. Det är enligt vår uppfattning svårt att bedöma exakt hur många företag som omfattas av denna möjlighet. Vi kan emellertid konstatera att det enligt Friskolornas riksförbund fanns närmare 4 000 fristående förskolor och skolor i Sverige år 2019[5] och att det enligt Vårdföretagarna fanns närmare 15 400 vårdföretag år 2018.[6] Av vårdföretagen hade strax under 90 procent färre än 10 anställda.

[5] Friskolornas riksförbund, *Fakta om friskolor december 2019*, s. 1.
[6] Vårdföretagarna, *Privat Vårdfakta 2020*, s. 17.

10.7 Konsekvenser för jämställdheten mellan män och kvinnor

Andelen kvinnor i åldersgruppen 16–85 år som använder mobilt BankID eller BankID med kortläsare vid legitimering på internet är 81 procent. Motsvarande andel män är 80 procent.[7] Andelen kvinnor i åldersgruppen 16–85 år som lämnat uppgifter elektroniskt genom användning av myndigheters webbplatser eller mobila applikationer är 65 procent. För männen är andelen 68 procent.[8] Detta talar för att kvinnor och män har likartade förutsättningar för att använda betrodda tjänster. Förslagen bedöms därför inte få några konsekvenser för jämställdheten mellan män och kvinnor.

10.8 Konsekvenser för att nå de integrationspolitiska målen

Vi bedömer att förslagen inte får några negativa konsekvenser för att nå de integrationspolitiska målen.

10.9 Närmare om konsekvenserna för enskilda förslag

10.9.1 Beskrivning av den svenska marknaden för betrodda tjänster

Utredningen har under hösten 2020 låtit göra en begränsad marknadsundersökning och PTS har under samma period låtit göra en undersökning av vilka tillhandahållare av betrodda tjänster som finns på den svenska marknaden. Den sammantagna bilden utifrån dessa undersökningar visar att den svenska marknaden består av ca 70–80 tillhandahållare av betrodda tjänster. Av dessa är två kvalificerade, och resterande icke kvalificerade, tillhandahållare av betrodda tjänster. Dessa tillhandahållare erbjuder olika betrodda tjänster men flera, ca 45 aktörer erbjuder tjänster med koppling till elektroniska underskrifter. Flera av dessa tillhandahållare erbjuder även möjlighet att validera de underskrifter som levereras inom ramen för deras under-

[7] Statistiska centralbyrån, Statistikdatabasen, Legitimering vid användning av internet efter legitimeringssätt, år 2018.
[8] Statistiska centralbyrån, Statistikdatabasen, Användning av myndigheters webbsidor eller appar utifrån användningsområde Skickat in ifyllda blanketter, år 2020.

skriftstjänst. Några av dessa aktörer är, utöver den svenska marknaden, även aktiva på den nordiska, europeiska eller internationella marknaden.

Storleken på de företag som tillhandahåller betrodda tjänster på den svenska marknaden varierar kraftigt och innefattar allt från verksamhet med koppling till de stora bankkoncernerna eller stora itbolag till mellanstora bolag och fåmansföretag.

Det finns ett fåtal aktörer som har stora volymer inom offentlig förvaltning och som granskats via DIGG:s specifikation för fristående underskriftstjänst. Det finns vidare några underskriftstjänster som används i stor utsträckning av offentlig förvaltning medan andra tillhandahållare främst levererar tjänster till näringslivet.

För närvarande finns det endast ett fåtal tillhandahållare som erbjuder generella valideringstjänster, dvs. sådana där andra än egna utfärdade underskrifter och stämplar valideras.

10.9.2 En utökad tillitsförteckning

Det kommer inte vara förenat med tvång för icke kvalificerade tillhandahållare eller betrodda tjänster att finnas med i tillitsförteckningen. Att föras upp på förteckningen är således frivilligt. Det kommer även vara förknippat med vissa administrativa bördor och kostnader (se mer om detta i avsnitt 10.6). Att finnas i tillitsförteckningen bedöms dock vara ett sätt att som tillhandahållare visa att vissa krav uppfylls. Vidare bedöms möjligheten för validering av tillhandahållarens avancerade elektroniska underskrifter och stämplar via den nationella valideringstjänsten eller andra valideringstjänster som använder tillitsförteckningen sannolikt ha en positiv inverkan på viljan att finnas med i förteckningen.

Som anges i avsnitt 10.6 kan tillitsförteckningen vidare antas leda till att den offentliga förvaltningen kommer att ställa krav på att tillhandahållare finns med i förteckningen och det kan komma att ses som en kvalitetsgaranti även av privat sektor. Motsatsvis kan detta innebära att tillhandahållare som inte finns med i förteckningen kan få svårare att sälja sina tjänster.

När icke kvalificerade tillhandahållare av betrodda tjänster som tillhandahåller avancerade elektroniska underskrifter och stämplar får föras upp på förteckningen kan möjligen intresset för att etablera

sig som kvalificerad tillhandahållare minska. Behovskartläggningen under utredningsarbetet pekar emellertid på att det endast finns ett begränsat behov av kvalificerade betrodda tjänster och att dessa behov framför allt är kopplade till gränsöverskridande användning. Förekomsten av icke kvalificerade tillhandahållare i den svenska tillitsförteckningen kombinerat med en nationell valideringstjänst möjliggör även gränsöverskridande användning av dessa tillhandahållares tjänster i de fall där det mottagande landet accepterar avancerade elektroniska underskrifter och stämplar från icke kvalificerade tillhandahållare av betrodda tjänster.

Konsekvenser för PTS

Förslaget om en tillitsförteckning innebär ytterligare uppgifter för PTS. Det innebär dels att förfaranden och föreskrifter behöver tas fram och vidmakthållas, dels att kontrollverksamheten kommer att utökas. Det är svårt att bedöma hur många aktörer som kommer vara intresserade av att vara med i tillitsförteckningen. Utredningen bedömer dock att det kommer anses vara fördelaktigt för flertalet tillhandahållare av betrodda tjänster. Bedömningen är därför att ca 10–20 aktörer kommer att vilja vara med i förteckningen under var och ett av de första två åren.

PTS arbete med tillsyn av betrodda tjänster har tidigare finansierats via anslag till DIGG. I budgetpropositionen för 2021 har tilldelningen av anslaget ändrats så att PTS får detta anslag direkt. PTS anslag har således ökats med 3 000 000 kronor från och med 2021 för myndighetens tillsyn över betrodda tjänster. Finansieringen sker genom att anslaget för DIGG minskas med motsvarande belopp. Anslaget föreslås minska med 480 000 kronor 2021 till följd av en generell besparing och beräknas fr.o.m. 2022 minskas igen med samma belopp.[9]

PTS disponerar även över avgifter som myndigheten tar ut av operatörer inom verksamheterna för elektronisk kommunikation, post och betrodda tjänster. Beräknade intäkter som myndigheten får disponera är 292 375 000 kronor för 2021.[10]

[9] Prop. 2020/21:1 Utgiftsområde 22 s. 110 och 117.
[10] A.a. s. 111.

Avgiftsuttaget för betrodda tjänster 2019 uppgick dock endast till 25 000 kronor och det budgeterade avgiftsuttaget för 2021 uppgår till 75 000 kronor.[11]

De kvalificerade tillhandahållarna kräver mer omfattande kontroller än vad icke kvalificerade gör men är samtidigt betydligt färre. När icke kvalificerade tillhandahållare förs upp på förteckningen kan även volymen av tillsyn förväntas öka i och med den ökade insynen i verksamheterna, men även eftersom aktörerna blir mer medvetna om skyldigheten att rapportera incidenter. Resursbehovet uppskattas därför behöva fördubblas till totalt 6 000 000 kronor per år för att långsiktigt hantera tillitsförteckningen och då främst för handläggning av ansökningar från, och kontroller av, tillhandahållare av avancerade elektroniska underskrifter och stämplar. För att etablera föreskrifter och anmälningsprocesser kan resursbehovet potentiellt vara större än så under det första året.

Tabell 10.1 Kostnader för PTS utökade roll avseende icke kvalificerade tillhandahållare och tjänster

Aktivitet	Timmar år 1	Timmar per år
Ta fram och underhålla regelverk för ansökningsförfarande	2 000	500
Kontroll av ansökningar	2 000	2 000
Förnyad kontroll		1 000
Utökad tillsyn		500
Total kostnad per år	**3 000 000 kr**	**3 000 000 kr**

Schablonen uppskattad enligt modellen 50 000 kr/månad i 12 månader, lönekostnadspåslag 54 % och overhead 50 % vilket ger en lönekostnad på 722 kr/timme avrundat till 750 kr.

En delmängd av kostnadsökningen kan avgiftsfinansieras. Avgiften bör dock vara mindre än för kvalificerade tillhandahållare av betrodda tjänster varför beräkningen baserar sig på spannet 10 000–20 000 kronor per år. Avgiften för kvalificerade tillhandahållare av betrodda tjänster är för närvarande 25 000 kronor per år och kan inte höjas utan att ändringar görs i 11 § förordningen om finansiering av Post- och telestyrelsens verksamhet. Avgiften kan inte finansiera hela verksam-

[11] Post- och telestyrelsen, *Rapport: Årsredovisning 2019* (PTS-ER-2020:1) s. 60 f. och Regeringsbeslut 2020-12-17 *Regleringsbrev för budgetåret 2021 avseende Post- och telestyrelsen* (I2020/03355, I2020/03296(delvis) och I2020/00597).

hetsområdet, men kan bidra med viss kostnadstäckning. Sammantaget gör det att avgifter bedöms kunna bidra med i storleksordningen 200 000–400 000 kronor det första året och 400 000–800 000 kronor per år de kommande åren.

Den ökade kostnaden för PTS kommer, utöver eventuell avgiftsfinansiering, behöva finansieras genom ökade anslag via reformutrymmet.

Konsekvenser för domstolarna

Beslut om att inte föra upp eller avföra en icke kvalificerad tillhandahållare eller betrodd tjänst från tillitsförteckningen kan enligt utredningens förslag överklagas till allmän förvaltningsdomstol. Som framgår av avsnitt 10.9.1 finns det i dagsläget ett 70-tal icke kvalificerade tillhandahållare av betrodda tjänster. Vi har ovan gjort bedömningen att 10–20 av dessa tillhandahållare kan antas vara intresserade av att föras upp på förteckningen under var och ett av de första två åren. Rätten att överklaga dessa beslut bör mot denna bakgrund inte generera någon större mängd mål för domstolarna. Förslaget bedöms därför inte få några konsekvenser för de allmänna förvaltningsdomstolarna som måste finansieras i särskild ordning.

Förslaget är förenligt med EU-rätten

Bedömningen att det ur ett EU-rättsligt perspektiv är möjligt för medlemsstaterna att välja att föra upp icke kvalificerade tillhandahållare av betrodda tjänster samt icke kvalificerade betrodda tjänster på sina tillitsförteckningar framgår av kapitel 7 samt avsnitt 8.3.2.

Vilka förutsättningar tillhandahållarna och de betrodda tjänsterna måste leva upp till för att få föras upp på den svenska tillitsförteckningen föreslår vi ska fastställas genom myndighetsföreskrifter. Det är, som påpekas i avsnitt 8.3.5, viktigt att de kriterier och krav som fastställs i sådana föreskrifter beaktar den fria rörligheten.

Vi bedömer att våra förslag inte behöver anmälas till kommissionen enligt de procedurer som fastställs i Europaparlamentets och rådets direktiv (EU) 2015/1535 av den 9 september 2015 om ett informationsförfarande beträffande tekniska föreskrifter och beträffande föreskrifter för informationssamhällets tjänster, eller i tjänstedirektivet.

Framtida myndighetsföreskrifter kan emellertid omfattas av krav på anmälan, något som PTS måste beakta i det fortsatta arbetet med sina föreskrifter på området.

10.9.3 En nationell valideringstjänst

Det finns endast ett fåtal tillhandahållare av valideringstjänster på den svenska marknaden. De flesta valideringstjänster tillhandahålls som en helhet av tillhandahållare av underskriftstjänster där valideringstjänsten är en del av leveransen som då bara validerar underskrifter som skapas med den egna tjänsten. Den av utredningen beställda marknadsundersökningen har identifierat ett fåtal generella valideringstjänster och dessa utgår antingen utifrån EU:s tillitsförteckning eller en kombination av förteckningen och en lista över egna betrodda utfärdare av underskrifter och stämplar. Dessa tjänster har i regel en prenumerations- eller transaktionsbaserad prismodell med månadsavgifter och rörliga avgifter. Vår bedömning är att marknaden för generella valideringstjänster kommer att påverkas om förslaget avseende en nationell valideringstjänst genomförs. Det har hittills varit en begränsad efterfrågan på, och ett begränsat utbud av, generella valideringstjänster. Det beror troligen på att det vanligaste är, som ovan anges, att valideringstjänster levereras tillsammans med underskriftstjänster och att valideringstjänsten då är begränsad till samma tillhandahållares underskrifter eller att den görs i egen regi, t.ex. baserat på EU-kommissionens programvara som finns tillgänglig som öppen källkod (DSS). Det innebär att den offentliga förvaltningen troligtvis inte kommer ha något behov av de generella valideringstjänster som finns på marknaden. Den nationella valideringstjänsten kommer att konkurrera med andra valideringstjänster och valideringslösningar.

Vår kartläggning visar att behoven hos aktörerna i den offentliga förvaltningen i dagsläget inte tillgodoses fullt ut av marknaden. Många aktörer uppger att de upplever utmaningar kopplat till validering. Den påverkan på marknaden som den nationella valideringstjänsten innebär anser vi vara motiverad utifrån de behov som finns inom förvaltningen. Ett offentligt åtagande på detta område är således påkallat.

Kostnadsberäkningen för en nationell valideringstjänst liksom alternativkostnaden baserar sig på att en valideringstjänst upprättas

med hjälp av programvara som finns tillgänglig som öppen källkod, antingen DSS eller den som utvecklats inom ramen för ett nyligen genomfört projekt om valideringstjänster och valideringsintyg som finansierats av Vinnova.[12]

DIGG har försett utredningen med en uppskattning av kostnaderna för att etablera en nationell valideringstjänst. Denna uppskattning har utgjort grunden för denna beräkning. Uppskattningen pekar på att det är en utvecklings- och etableringskostnad år 1 på ca 2 miljoner kronor och därefter kostnader på ca 8 miljoner kronor per år.[13]

Vi anser också att det finns anledning att ställa omfattande säkerhetskrav på en nationell valideringstjänst och har därför räknat med ökade kostnader med anledning av detta. Kostnaderna hänför sig till initial och återkommande säkerhetsgranskningar, penetrationstester och redundant drift av tjänsten. Kostnadsuppskattningarna baserar sig på ett timpris för säkerhetsgranskningar och penetrationstester om 1 500 kronor per timme. Priset är uppskattat utifrån ramavtal och annan offentlig information om kostnader för penetrationstest och säkerhetsgranskning. Säkerhetsgranskning och penetrationstest bedöms under utvecklings- och etableringsskedet ta en arbetsmånad var för två personer, dvs. ca 300 timmar. Efterkommande år bedöms det finnas ett fortsatt, om än något mindre, behov i samband med förändringar som nya versioner av tjänsten eller andra mer omfattande förändringar. Uppskattningen är att behoven av säkerhetsgranskning år ett omfattar 200 timmar och därefter 100 timmar per år. På motsvarande sätt bedöms penetrationstesterna omfatta 100 timmar år ett och därefter 100 timmar per år. Valideringstjänsten behöver ha en hög nivå av tillgänglighet och tillkommande kostnader är för omfattande redundans och överkoppling.

Lokaldrift eller egen valideringstjänst

Utredningen har låtit ett konsultbolag räkna på kostnaden för att införa en valideringstjänst. Beräkningen har utgått från att kommissionens ramverk för validering som finns som öppen källkod (DSS)

[12] www.vinnova.se/p/arkiveringsbara-digitala-underskrifter/ (hämtad 2021-01-18).

[13] I kostnaderna ingår omarbetning av tillitsförteckning, krav och specifikation inklusive internationellstandardisering, utveckling och anskaffning, kompletteringar och anpassning för att stödja standarder och API:er, öppen källkodspublicering, upprätta valideringspolicy som omfattar de flesta i den offentliga förvaltningens behov, teknisk drift och förvaltning, information till förlitande parter och teknisk support till förlitande parter.

implementeras. Konsultbolaget har intervjuat två större aktörer verksamma på marknaden om kostnaden för att realisera en valideringstjänst baserad på DSS för myndigheterna. Siffrorna grundar sig på de uppgifter som de fått från dessa aktörer. Siffrorna är behäftade med osäkerhet gällande framför allt hur komplex en anskaffande myndighets it-miljö är och hur omfattande säkerhetskrav myndigheten ställer. Det kan utöver dessa kostnader även finnas en begränsad etableringskostnad för tjänsten som sådan. De uppskattade kostnaderna kan ändå ge en fingervisning om vad realisering av en valideringstjänst lokalt kan kosta per statlig myndighet, kommun eller region.

Tabell 10.2 Kostnad per myndighet för egen valideringstjänst

Aktivitet	Uppskattad min kostnad	Uppskattad max kostnad
Etablering av valideringstjänst	72 000	900 000
Projektledning och utbildning	36 000	450 000
Underhållskostnader	300 000	1 200 000
Totalkostnad per myndighet för valideringstjänst	**408 000**	**2 550 000**

Konsekvenser för DIGG

Etablering och drift av den nationella valideringstjänsten skulle innebära nya uppgifter för DIGG. DIGG:s kostnader för detta bör finansieras genom tillskott av anslag via reformutrymmet. För det fall avgifter för bruk av valideringstjänsten tas ut bör dessa även användas för att delfinansiera kostnaden.

Förslaget är förenligt med EU-rätten

Av artikel 2 i kommissionens genomförandebeslut 2015/1506 framgår att andra format av elektroniska underskrifter, än de som beslutet i övrigt pekar på, ska erkännas, under förutsättning att den medlemsstat där tillhandahållaren av betrodda tjänster som användes av undertecknaren är etablerad, erbjuder andra medlemsstater möjligheter till validering av underskrift som är lämpad, när så är möjligt, för automatiserad behandling. Sådan validering kan ske genom en sådan valideringstjänst som vi föreslår. Eftersom tjänsten enligt vårt förslag ska validera elektroniska underskrifter och stämplar som har skapats av

betrodda tjänster som finns med i den svenska eller andra medlemsstaters tillitsförteckningar kan det få positiv inverkan på möjligheterna att utöva den fria rörligheten. Att som medlemsstat tillhandahålla en valideringstjänst av det slag vi föreslår är förenligt med eIDAS-förordningen samt primärrätten. Det är emellertid viktigt att DIGG, som föreslås få föreskriftsrätt avseende tjänsten, bl.a. beaktar den fria rörligheten. Det gäller även vid utformandet av tjänsten som sådan.

Vi bedömer att våra förslag avseende tjänsten inte är föremål för anmälan enligt de procedurer som fastställs i direktiv (EU) 2015/1535 eller i tjänstedirektivet. Eventuella framtida myndighetsföreskrifter kan emellertid, beroende på innehåll, behöva anmälas till kommissionen. Det är således något DIGG måste beakta i det fortsatta arbetet.

10.9.4 Regeringsuppdrag om att utreda förutsättningarna för att använda valideringsintyg som metod för att bevara undertecknade eller stämplade handlingars giltighet

Konsekvenser för Riksarkivet

Utredningen föreslår att regeringen ger Riksarkivet ett uppdrag att tillsammans med DIGG utreda förutsättningarna för att använda valideringsintyg som metod för att bevara undertecknade och stämplade handlingars giltighet Detta uppdrag bedöms falla inom ramen för Riksarkivets uppgifter enligt 5 § förordningen (2009:1593) med instruktion för Riksarkivet och ska därmed finansieras inom myndighetens befintliga ram.

Konsekvenser för DIGG

För DIGG:s del bedöms detta förslag kunna finansieras inom ramen för det ökade anslag som föreslås i avsnitt 10.9.3.

10.9.5 Regeringsuppdrag om att utreda förutsättningarna för att införa generella bestämmelser och/eller annat stöd avseende bevarande av elektroniskt undertecknade eller stämplade handlingar

Konsekvenser för Riksarkivet

Utredningen föreslår att regeringen ger Riksarkivet ett uppdrag om att utreda förutsättningarna för att införa generella bestämmelser och/eller annat stöd avseende gallring av elektroniskt undertecknade eller stämplade handlingar. Detta uppdrag bedöms falla inom ramen för Riksarkivets uppgifter enligt 5 § förordningen med instruktion för Riksarkivet och ska därmed finansieras inom myndighetens befintliga ram.

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

Konsekvenser för PTS

I avsnitt 10.9.2 redogörs för PTS nuvarande finansiering för verksamhetsområdet betrodda tjänster. Vårt förslag i denna del är att PTS uppgift att lämna stöd inom området betrodda tjänster ska begränsas i jämförelse med vad som i nuläget framgår av myndighetens instruktion. Vi förutser dock inga budgetära konsekvenser för PTS utifrån den förändring vi föreslår avseende stöd till myndigheter. Detta med anledning av att PTS i nuläget inte i någon större utsträckning lämnar stöd till myndigheter. En neddragning av medel eller utväxling är därför inte aktuell. Därutöver föreslår vi utökade uppgifter för myndigheten avseende tillitsförteckningen vilket kommer föranleda behov av en anslagsökning inom området betrodda tjänster (se mer om detta i avsnitt 10.9.2).

Konsekvenser för DIGG

Förslaget om ändring av DIGG:s uppgifter innebär ett utökat ansvar för myndigheten inom området betrodda tjänster. Det stöd som DIGG föreslås lämna avser både tekniska och juridiska frågor. DIGG:s anslag ökades med 5 000 000 kronor från och med 2021 för att finan-

siera att myndigheten ska ge ett rättsligt stöd till den offentliga förvaltningen.[14] Detta förslag, i den del det avser rättsligt stöd, bedöms kunna finansieras inom ramen för det ökade anslaget och därmed finansieras inom myndighetens befintliga ram. För det stöd som avser de tekniska aspekterna rörande betrodda tjänster bedöms myndighetens anslag, genom tillskott via reformutrymmet, däremot behöva ökas med motsvarande två årsarbetskrafter eller 3 000 000 kronor.

Den ovan angivna finansieringen bedöms även täcka kostnaderna för förslaget om att DIGG ska få i uppdrag att ta fram en vägledning för den offentliga förvaltningens användning av betrodda tjänster.

10.9.7 Ökad medverkan i standardiseringsarbete

PTS och DIGG har inskrivet i sina respektive instruktioner att de ska delta i nationellt och internationellt standardiseringsarbete (se avsnitt 8.8). Eftersom det föreslagna regeringsuppdraget bedöms falla inom ramen för myndigheternas nuvarande uppgifter ska det finansieras inom respektive myndighets befintliga ram.

[14] Prop. 2020/21:1 Utgiftsområde 22 s. 117.

11 Ikraftträdande

11.1 Ikraftträdande av ändringar i lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering

Utredningens förslag: Lagändringarna ska träda i kraft den 1 januari 2022.

Skälen för utredningens förslag

Vi bedömer att det är angeläget att de ändringar vi föreslår träder i kraft så snart som möjligt till stöd för den offentliga förvaltningens digitalisering och dess användning av betrodda tjänster.

Med hänsyn till den tid som kan beräknas gå åt för remissförfarande, fortsatt beredning inom Regeringskansliet och riksdagsbehandling samt utveckling av nödvändiga it-system vid berörda myndigheter bör de lagbestämmelser utredningen föreslår tidigast kunna träda i kraft den 1 januari 2022. Förslagen är inte av den arten att de kräver några särskilda övergångsregler.

11.2 Ikraftträdande av förordningsändringar

Utredningens förslag: Förordningsändringarna ska träda i kraft den 1 januari 2022.

Skälen för utredningens förslag

Vi bedömer det angeläget att även de föreslagna förordningsändringarna träder i kraft så snart som möjligt.

Med hänsyn till den tid som kan beräknas gå åt för remissförfarande och fortsatt beredning inom Regeringskansliet bör de ändringar utredningen föreslår i förordning (2016:576) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering tidigast kunna träda i kraft den 1 januari 2022. Förslagen är inte av den arten att de kräver några särskilda övergångsregler.

Vad avser föreslagna ändringar i förordningen (2007:951) med instruktion för Post- och telestyrelsen och förordningen (2018:1486) med instruktion för Myndigheten för digital förvaltning föranleder dessa sådana budgetära konsekvenser för DIGG att den tid som kan beräknas gå åt för remissförfarande och fortsatt beredning inom Regeringskansliet medför att sådan finansiering som tidigast kan beaktas inom ramen för budgetpropositionen för 2022. De aktuella förordningsändringarna kan därför som tidigast träda i kraft den 1 januari 2022. Förslagen är inte av den arten att de kräver några särskilda övergångsregler.

12 Författningskommentar

12.1 Förslaget till lag om ändring i lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering

Tillitsförteckning

7 §

Paragrafen, som är ny, behandlas i avsnitt 8.3 och innebär att det i lag införs en bestämmelse om den förteckning som avses i artikel 22 i eIDAS-förordningen.

Enligt *första stycket* ska tillsynsmyndigheten i enlighet med artikel 22 i eIDAS-förordningen upprätta, underhålla och offentliggöra en förteckning över kvalificerade tillhandahållare av betrodda tjänster och de kvalificerade betrodda tjänster som dessa aktörer tillhandahåller. Det anges vidare att förteckningen ska benämnas tillitsförteckning. Denna term förekommer inte i eIDAS-förordningen. Stycket motsvarar i stort nuvarande 5 § förordningen (2016:576) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering, som i sin tur bygger på artikel 22 i eIDAS-förordningen. Eftersom bestämmelsen nu tas med i lag anges till skillnad från ovan nämnda paragraf i förordningen att det i stället för Post- och telestyrelsen är tillsynsmyndigheten som ska tillhandahålla tillitsförteckningen. Av 4 § i förordningen med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering följer att Post- och telestyrelsen är tillsynsmyndighet. Någon förändring avseende vilken myndighet som ska ansvara för förteckningen är således inte avsedd.

I *andra stycket* anges vilka tillhandahållare och tjänster som, utöver de som framgår av första stycket, får föras upp på tillitsförteckningen.

Av *andra stycket första punkten* följer att även icke kvalificerade betrodda tjänster som tillhandahålls av kvalificerade tillhandahållare får föras upp på tillitsförteckningen. I enlighet med bestämmelserna i eIDAS-förordningen kan endast kvalificerade tillhandahållare av betrodda tjänster tillhandahålla kvalificerade betrodda tjänster. Sådana tjänster förs upp på förteckningen med stöd av bestämmelserna i eIDAS-förordningen.

På tillitsförteckningen får enligt *andra stycket andra punkten* även icke kvalificerade tillhandahållare av betrodda tjänster och betrodda tjänster som de tillhandahåller föras upp.

8 §

Paragrafen, som är ny, behandlas i avsnitt 8.3 och beskriver förfarandet för icke kvalificerade tillhandahållare som vill föras upp på tillitsförteckningen och de kriterier och tekniska krav som behöver vara uppfyllda.

Enligt *första stycket* fattas beslut om att föra upp sådana tillhandahållare eller tjänster som avses i 7 § andra stycket på tillitsförteckningen av tillsynsmyndigheten.

Genom *andra stycket* delegeras till regeringen eller den myndighet som regeringen bestämmer möjligheten att meddela kompletterande föreskrifter.

Föreskrifterna får enligt *andra stycket första punkten* avse kriterier och tekniska krav som icke kvalificerade tillhandahållare av betrodda tjänster ska uppfylla för att föras upp på tillitsförteckningen. Sådana tillhandahållare omfattas redan av vissa krav avseende säkerhet och incidentrapportering genom artikel 19 i eIDAS-förordningen. Med kriterier avses sådant som tillhandahållaren som sådan behöver uppfylla i exempelvis rättsligt, organisatoriskt, finansiellt eller säkerhetsmässigt hänseende. Med tekniska krav avses t.ex. krav på de it-system som tillhandahållaren använder.

Av *andra stycket andra punkten* följer att föreskrifter får meddelas om vilka typer av icke kvalificerade betrodda tjänster som får föras upp på tillitsförteckningen samt kriterier och tekniska krav för dessa.

Med ansökningsförfarandet i *andra stycket tredje punkten* avses sådant som har koppling till den ansökan som en tillhandahållare måste lämna in till tillsynsmyndigheten för att föras upp, eller för att

föra upp en betrodd tjänst, på tillitsförteckningen. I föreskrifterna kan exempelvis anges hur en sådan ansökan ska lämnas in till myndigheten och vad den ska innehålla.

Enligt *tredje stycket* får tillsynsmyndigheten avföra en icke kvalificerad tillhandahållare av betrodda tjänster eller en icke kvalificerad betrodd tjänst från tillitsförteckningen om de inte längre lever upp till de kriterier eller tekniska krav som har meddelats med stöd av andra stycket. Vad gäller kvalificerade tillhandahållare och kvalificerade betrodda tjänster regleras detta i artikel 20.3 i eIDAS-förordningen. Enligt artikeln kan tillsynsmyndigheten återkalla statusen som kvalificerad för tillhandahållare eller för betrodda tjänster. Medlemsstatens tillitsförteckning ska då uppdateras. Den nu föreslagna bestämmelsen kompletterar artikel 20.3 i eIDAS-förordningen och gör det möjligt för tillsynsmyndigheten att avföra icke kvalificerade tillhandahållare och icke kvalificerade betrodda tjänster från förteckningen. Tillsynsmyndigheten har även andra sanktionsmöjligheter att tillgripa med stöd av 6 § i form av förelägganden och förbud. Möjligheten att avföra en icke kvalificerad tillhandahållare eller en icke kvalificerad betrodd tjänst från tillitsförteckningen är avsedd för de fall då sanktioner enligt 6 § inte medfört rättelse eller där bristerna är så pass allvarliga att det krävs skyndsamma åtgärder från tillsynsmyndighetens sida för att undvika skada.

En icke kvalificerad tillhandahållare av betrodda tjänster kan med stöd av *fjärde stycket* själv begära att den eller de betrodda tjänster den tillhandahåller ska avföras från tillitsförteckningen. Detsamma gäller för en kvalificerad tillhandahållare av betrodda tjänster som vill att en icke kvalificerad betrodd tjänst som denne tillhandahåller ska avföras från förteckningen. En sådan begäran lämnas till tillsynsmyndigheten. Vad som gäller för avförande från tillitsförteckningen för kvalificerade tillhandahållare eller kvalificerade betrodda tjänster regleras i eIDAS-förordningen och den nu föreslagna bestämmelsen påverkar inte detta förfarande.

Enligt *femte stycket* får tillsynsmyndigheten bestämma att ett beslut enligt tredje stycket att avföra en icke kvalificerad tillhandahållare eller betrodd tjänst från tillitsförteckningen ska gälla omedelbart. Bestämmelsen är avsedd för situationer när det krävs skyndsamma åtgärder för att undvika skada genom att en tillhandahållare eller betrodd tjänst som inte längre uppfyller kriterierna eller de tekniska

kraven i andra stycket kvarstår i förteckningen till dess att beslutet vunnit laga kraft.

Nationell valideringstjänst

9 §

Paragrafen, som är ny, behandlas i avsnitt 8.4 och anger att det ska finnas en tjänst för validering av elektroniska underskrifter och stämplar.

Enligt *första stycket* ska den myndighet som regeringen bestämmer tillhandahålla en tjänst som validerar elektroniska underskrifter och elektroniska stämplar. Tjänsten ska benämnas nationell valideringstjänst.

Av *andra stycket* följer att den nationella valideringstjänsten enligt *första punkten* får användas av offentliga aktörer och enligt *andra punkten* av enskilda som validerar elektroniska underskrifter och elektroniska stämplar som skapats av offentliga aktörer. Offentlig aktör definieras i 10 §.

Enligt *tredje stycket* får regeringen eller den myndighet regeringen bestämmer meddela föreskrifter om den nationella valideringstjänstens funktionalitet, tekniska specifikationer samt villkor och avgifter för användning av tjänsten. Genom sådana föreskrifter kan det exempelvis preciseras under vilka förutsättningar validering kan ske, hur en offentlig aktör kan ansluta mot tjänsten och hur tjänsten får användas.

10 §

Paragrafen, som är ny, behandlas i avsnitt 8.4.3 och redogör för de rättssubjekt som anses vara offentliga aktörer. Motsvarande bestämmelser finns i 4 och 5 §§ lagen (2018:1937) om tillgänglighet till digital offentlig service. Paragrafen är avsedd att ha samma innebörd som nämnda bestämmelser i den lagen, se prop. 2017/18:299 s. 30 ff. och 86 ff.

11 §

Paragrafen, som är ny, behandlas i avsnitt 8.4.6 och anger att den myndighet som regeringen enligt 9 § första stycket bestämmer ska tillhandahålla den nationella valideringstjänsten får i denna tjänst behandla personuppgifter. Sådan behandling får ske om det är nödvändigt för att enligt *första punkten* validera en elektronisk underskrift eller elektronisk stämpel eller enligt *andra punkten* säkerställa att villkor som har meddelats med stöd av lagen efterlevs.

Kommittédirektiv 2020:27

Ökad och standardiserad användning av betrodda tjänster i den offentliga förvaltningen

Beslut vid regeringssammanträde den 12 mars 2020

Sammanfattning

En särskild utredare ska utreda förutsättningarna för ökad och standardiserad användning av betrodda tjänster i den offentliga förvaltningen. Syftet med utredningen är att höja säkerheten och stärka tilliten när betrodda tjänster används.

I utredarens uppdrag ingår att

- kartlägga och analysera den offentliga förvaltningens behov av åtgärder för ökad och standardiserad användning av betrodda tjänster,
- lämna förslag på sådana åtgärder, särskilt när det gäller att
  - tydliggöra när avancerade respektive kvalificerade elektroniska underskrifter bör användas i den offentliga förvaltningen,
  - kunna validera och bevara elektroniska underskrifter, och
  - kunna använda e-legitimation i tjänsten, och
- lämna nödvändiga författningsförslag.

Uppdraget ska redovisas senast den 30 december 2020.

Betrodda tjänster

Betrodda tjänster är sådana tjänster som används för att skapa, kontrollera, validera och bevara elektroniska underskrifter, elektroniska stämplar, elektroniska tidsstämplingar och certifikat samt för att autentisera webbplatser och säkra elektroniska leveranser. Sådana tjänster utgör samhällskritisk infrastruktur som är en förutsättning för fortsatt utveckling av digital service till privatpersoner och företag. De är också centrala för att förverkliga EU:s strategi om en digital inre marknad med fri rörlighet av varor och tjänster. För att kunna verka i en digital miljö är en säker identifiering av helt avgörande betydelse vid t.ex. informationsutbyte eller underskrift av handlingar. Säkra betrodda tjänster är också en förutsättning för en fungerande verksamhet hos många offentliga arbetsgivare.

Betrodda tjänster regleras av Europaparlamentets och rådets 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, den s.k. eIDAS-förordningen. Syftet med förordningen är att öka förtroendet för elektroniska transaktioner på den inre marknaden genom att tillhandahålla en gemensam grund för ett säkert elektroniskt samspel mellan privatpersoner, företag och den offentliga förvaltningen. Avsikten är att därigenom öka effektiviteten hos offentliga och privata digitala tjänster, affärsverksamhet och e-handel i unionen.

Förordningen reglerar vad betrodda tjänster är och vilka tekniska och juridiska förutsättningar som gäller för dem. Betrodda tjänster kan under vissa förutsättningar anses vara kvalificerade eller icke-kvalificerade. Kvalificerade betrodda tjänster är giltiga inom hela EES-området. Post- och telestyrelsen (PTS) publicerar teknisk och juridisk information för kvalificerade betrodda tjänster på den svenska förteckningen över kvalificerade tillhandahållare av betrodda tjänster (trusted list). eIDASförordningen är för närvarande föremål för översyn. Resultatet av översynen ska publiceras av Europeiska kommissionen senast den 1 juli 2020.

Kompletterande bestämmelser till förordningen finns i lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering och förordningen (2016:576) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering.

Utredningen om effektiv styrning av nationella digitala tjänster lämnar i betänkandet reboot – omstart för den digitala förvaltningen (SOU 2017:114) förslag på flera åtgärder för ökad styrning av området för elektronisk identifiering och betrodda tjänster.

Regeringen beslutade den 31 oktober 2019 att tillsätta en utredning som ska föreslå de anpassningar och kompletterande författningsbestämmelser som Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten) ger anledning till. Utredaren ska också överväga om det finns anledning att införa ytterligare krav för att skydda verksamhet som är av betydelse för Sveriges säkerhet, som krav på certifiering och godkännande av vissa produkter, tjänster och processer (dir. 2019:73). Uppdraget ska redovisas i den del som avser anpassningar med anledning av EU-förordningen senast den 1 juni 2020. I den del som avser regler till skydd för Sveriges säkerhet ska uppdraget redovisas senast den 1 mars 2021.

Behovet av åtgärder för ökad och standardiserad användning av betrodda tjänster

Förordningen anger vissa krav som betrodda tjänster måste uppfylla. Principen är att en tjänst som är godkänd inom en medlemsstat automatiskt ska vara godkänd i alla medlemsstater. Däremot har genomförandeakter för gemensamma standarder inte antagits. Det finns inte heller regler och riktlinjer för gemensamma standarder på nationell nivå. En konsekvens av detta är att det i praktiken är mycket svårt att utan avancerade it-stöd kunna avgöra om ett elektroniskt undertecknat dokument går att lita på.

Ökad och standardiserad användning av elektroniska underskrifter som går att lita på och som är enkla att använda är grundläggande i ett alltmer digitaliserat samhälle. I svenska digitala tjänster används främst underskrifter som i förordningen benämns avancerade elektroniska underskrifter. I kommissionens genomförandebeslut (EU) 2015/1506 av den 8 september 2015 om fastställande av specifikationer rörande format för avancerade elektroniska underskrifter och avancerade elektroniska stämplar i enlighet med artiklarna 27.5 och 37.5 i Europaparlamentets och rådets förordning (EU) nr 910/2014

om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden beskrivs vilka format och metoder som måste erkännas av medlemsstaterna. Det som i eIDASförordningen benämns kvalificerade elektroniska underskrifter används endast i begränsad omfattning i Sverige och marknaden för betrodda tjänster har inte utvecklats på det sätt som förutsågs vid förordningens tillkomst. Svensk lagstiftning ställer inte heller krav på användning av kvalificerade elektroniska underskrifter, utan förekommande krav tar sikte på avancerade elektroniska underskrifter. 2017 års ID-kortsutredning föreslår att det ska införas ett nytt statligt identitetskort med en e-legitimation som ska kunna användas för att skapa just avancerade elektroniska underskrifter. Frågan om den statliga e-legitimationen ska kunna användas även för att skapa kvalificerade elektroniska underskrifter lämnas till stor del öppen, se betänkandet Ett säkert statligt ID-kort – med e-legitimation (SOU 2019:14).

Från flera håll i den offentliga förvaltningen har det kommit rapporter om problem kopplade till elektroniska underskrifter. Både juridiska oklarheter och tekniska svårigheter återkommer i beskrivningarna av de utmaningar som finns. Det gäller särskilt validering och bevarande av dokument som skrivits under elektroniskt. Svårigheterna består bl.a. i att kunna godta olika format och underskrifter. Flera myndigheter använder i dag digitala tjänster där hela förfarandet hanteras i ett flöde. Det innebär att tjänsten hämtar information om användaren och dennes behörighet baserat på information från den elektroniska identifieringen som gjordes i samband med inloggningen. Behörigheten kontrolleras sedan direkt när t.ex. en handling skrivs under elektroniskt. Flödet blir då låst till ett enda sätt att hantera elektronisk identifiering och underskrift. Detta gör det svårt att utveckla tjänster som godtar andra elektroniska underskrifter än de som är kopplade till den elektroniska identifieringen. Det gäller särskilt vid gränsöverskridande användning av digitala tjänster. Ett sätt att hantera detta är att använda en fristående underskriftstjänst som utfärdar ett engångscertifikat för underskrift utifrån den använda e-legitimationen. Ett sådant förfarande kan också användas för en utländsk elektronisk underskrift. I digitala tjänster som tar emot elektroniskt underskrivna blanketter blir flödet enklare, eftersom underskriften då är helt separerad från den digitala tjänstens medel för elektronisk identifiering. Här uppstår i stället krav på mottagaren att kunna validera den elektroniska underskriften.

En digital tjänst kan känna igen elektroniska underskrifter som baseras på kvalificerade certifikat. Sådana underskrifter kontrolleras mot uppgifterna i den svenska förteckningen över kvalificerade tillhandahållare av betrodda tjänster. När det gäller avancerade elektroniska underskrifter finns det inte samma detaljreglering som för kvalificerade elektroniska underskrifter. Avancerade elektroniska underskrifter omfattas exempelvis inte av någon anmälningsplikt och det finns inte heller någon motsvarande förteckning. Det innebär bland annat att det saknas möjlighet att validera avancerade elektroniska underskrifter. Det gör det svårt för mottagaren att avgöra om och hur en avancerad underskrift från en okänd tillhandahållare lever upp till kraven på en avancerad elektronisk underskrift. Mot bakgrund av detta föreslås i betänkandet reboot – omstart för den digitala förvaltningen att regeringen ska tillsätta en utredning som ser över behovet av svensk reglering av betrodda tjänster som inte är kvalificerade.

Ett hinder som ofta lyfts fram när det gäller digitaliseringen av offentlig sektor är avsaknaden av standardiserade e-legitimationer för användning vid tjänsteutövning. De elektroniska intyg som i dag skickas mellan parterna vid elektronisk identifiering innehåller uppgifter om användarens identitet, bl.a. personnumret. Däremot saknas vanligen information om vilken organisation användaren företräder och vilken behörighet denne har. Utredningen om effektiv styrning av nationella digitala tjänster beskriver att det för att effektivisera informationsutbytet mellan myndigheter har utvecklats en praxis som innebär att myndigheter litar på varandra, s.k. organisationstillit. Det räcker då att kontrollera att den andra parten företräder den myndighet som uppges. Utredningen konstaterar dock att frågan om behörigheter är komplex och att behörigheter kan bedömas utifrån olika perspektiv. Myndigheten för digital förvaltning lyfter fram behovet av att utveckla tjänster för hantering av behörigheter som en prioriterad åtgärd för att åstadkomma effektivt och säkert informationsutbyte inom den offentliga förvaltningen. Sveriges Kommuner och Regioner påpekar behovet av att staten tar ett övergripande ansvar för en gemensam sektorsövergripande infrastruktur för e-legitimering i tjänsten och att uppdraget för Myndigheten för digital förvaltning måste förtydligas i denna del (SKR:s styrelses ställningstagande Digital identitetshantering, 2019).

För att Sverige ska leva upp till sina förpliktelser enligt EU-rätten krävs även enligt bland annat Europaparlamentets och rådets direktiv 2006/123/EG av den 12 december 2006 om tjänster på den inre marknaden med tillhörande beslut samt Europaparlamentets och rådets förordning (EU) 2018/1724 av den 2 oktober 2018 om inrättande av en gemensam digital ingång för tillhandahållande av information, förfaranden samt hjälp- och problemlösningstjänster och om ändring av förordning (EU) nr 1024/2012 att Sverige i vissa fall gör det möjligt för personer från andra EU-länder att identifiera sig för att ansöka om tillstånd m.m.

Flera medlemsstater arbetar med att vidareutveckla betrodda tjänster för att hantera behörigheter. Det saknas bland annat standarder för utbyte av information om behörigheter vid gränsöverskridande informationsutbyte. Sådana standarder ska användas även nationellt och för att möjliggöra en sådan utveckling även i Sverige finns det behov av att utreda och lämna förslag på åtgärder som främjar en ökad användning av eIDASförordningens betrodda tjänster för att möta förvaltningens behov. Det behövs ett enhetligt sätt att hantera e-legitimationer i tjänsten, och förordningen bedöms utgöra en långsiktig och hållbar bas för den fortsatta utvecklingen på området. Standarder är en viktig grund för att skapa långsiktigt hållbara och återanvändbara lösningar.

Mot denna bakgrund ska utredaren utreda förutsättningarna för ökad och standardiserad användning av betrodda tjänster i den offentliga förvaltningen. Syftet med utredningen är att höja säkerheten och stärka tilliten när betrodda tjänster används.

I uppdraget ingår att

- kartlägga och analysera den offentliga förvaltningens behov av åtgärder för ökad och standardiserad användning av betrodda tjänster,
- lämna förslag på sådana åtgärder, särskilt när det gäller att
  - tydliggöra när avancerade respektive kvalificerade elektroniska underskrifter bör användas i den offentliga förvaltningen,
  - kunna validera och bevara elektroniska underskrifter, och
  - kunna använda e-legitimation i tjänsten, och
- lämna nödvändiga författningsförslag.

Internationell utblick

Utredaren ska undersöka och översiktligt redovisa hur de frågor som uppdraget omfattar hanteras i andra länder som är jämförbara med Sverige, exempelvis de nordiska länderna.

Konsekvensbeskrivningar

Utredaren ska analysera de samhällsekonomiska effekterna i utredningsarbetets alla delar, från problembeskrivning och syfte till analys av alternativ och motiv till förslag samt bedöma förslagens konsekvenser i enlighet med kommittéförordningen (1998:1474) och förordningen om konsekvensutredning vid regelgivning (2007:1244). Om förslagen kan förväntas leda till kostnadsökningar för det allmänna, ska utredaren föreslå hur dessa ska finansieras. Om förslagen innebär en inskränkning av den kommunala självstyrelsen, ska en proportionalitetsprövning göras enligt 14 kap. 3 § regeringsformen. De särskilda avvägningar som underbygger förslagen ska redovisas särskilt. Utredaren ska också särskilt ange konsekvenser för företag i form av kostnader och ökade administrativa bördor. Utredaren ska också analysera risker med identitetsrelaterad brottslighet och redovisa konsekvenser för brottsbekämpning och brottsförebyggande arbete.

Kontakter och redovisning av uppdraget

Utredaren ska hålla sig informerad om och beakta relevant arbete som bedrivs inom Regeringskansliet, utredningsväsendet, t.ex. utredningen Cybersäkerhet – genomförande av cybersäkerhetsakten och vissa åtgärder till skydd för säkerhetskänslig verksamhet (Fö 2019:01), och EU. Utredaren ska särskilt beakta det arbete som bedrivs hos Myndigheten för digital förvaltning. Vidare ska utredaren inhämta övriga behövliga upplysningar från berörda myndigheter och organisationer.

Uppdraget ska redovisas senast den 30 december 2020.

(Infrastrukturdepartementet)

Kommittédirektiv 2020:135

Tilläggsdirektiv till Utredningen om betrodda tjänster (I 2020:01)

Beslut vid regeringssammanträde den 17 december 2020

Förlängd tid för uppdraget

Regeringen beslutade den 12 mars 2020 kommittédirektiv till en särskild utredare att utreda förutsättningarna för en ökad och standardiserad användning av betrodda tjänster i den offentliga förvaltningen i syfte att höja säkerheten och stärka tilliten när betrodda tjänster används (dir. 2020:27). I uppdraget ingår en kartläggning och analys av den offentliga förvaltningens behov av åtgärder för ökad och standardiserad användning av betrodda tjänster och att lämna förslag på sådana åtgärder. Utredaren ska även lämna nödvändiga författningsförslag. I utredarens uppdrag betonas särskilt följande delområden: tydliggörande av när avancerade respektive kvalificerade elektroniska underskrifter bör användas i den offentliga förvaltningen, validering och bevaring av elektroniska underskrifter samt användning av e-legitimation i tjänsten. Utredningen har tagit namnet Utredningen om betrodda tjänster. Uppdraget skulle enligt direktiven slutredovisas senast den 30 december 2020.

Utredningstiden förlängs. Uppdraget ska, med undantag för den delredovisning som ska lämnas den 15 februari 2021, i stället slutredovisas senast den 30 juni 2021.

Redovisning av uppdraget

Den del av uppdraget som avser åtgärder för ökad och standardiserad användning av betrodda tjänster enligt punktuppställningen nedan ska redovisas senast den 15 februari 2021.

I delredovisningen ska följande ingå:

- kartläggning och analys av den offentliga förvaltningens behov avåtgärder för ökad och standardiserad användning av betrodda tjänster,
- förslag på sådana åtgärder och nödvändiga författningsförslag, särskilt när det gäller att
  - tydliggöra när avancerade respektive kvalificerade elektroniska underskrifter bör användas i den offentliga förvaltningen, och
  - validera och bevara elektroniska underskrifter.

Resterande delar av uppdraget som framgår av dir. 2020:27 ska slutredovisas den 30 juni 2021.

(Infrastrukturdepartementet)

EUROPAPARLAMENTETS OCH RÅDETS 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

EUROPAPARLAMENTET OCH EUROPEISKA UNIONENS RÅD HAR ANTAGIT DENNA FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artikel 114,

med beaktande av Europeiska kommissionens förslag,

efter översändande av utkastet till lagstiftningsakt till de nationella parlamenten,

med beaktande av Europeiska ekonomiska och sociala kommitténs yttrande [1],

i enlighet med det ordinarie lagstiftningsförfarandet [2], och

av följande skäl:

(1) Att bygga upp förtroendet för nätmiljön är avgörande för den ekonomiska och sociala utvecklingen. Bristande förtroende, särskilt på grund av upplevd brist på rättssäkerhet, gör att konsumenter, företag och offentliga myndigheter tvekar att utföra transaktioner på elektronisk väg och att använda nya tjänster.

(2) Syftet med denna förordning är att öka förtroendet för elektroniska transaktioner på den inre marknaden genom att tillhandahålla en gemensam grund för ett säkert elektroniskt samspel mellan medborgare, företag och offentliga myndigheter, och därigenom öka effektiviteten hos offentliga och privata nättjänster, elektronisk affärsverksamhet och e-handel i unionen.

(3) Europaparlamentet och rådets direktiv 1999/93/EG [3] gällde elektroniska underskrifter utan att skapa ett heltäckande, gräns- och sektorsöverskridande regelverk för säkra, pålitliga och lättanvända elektroniska transaktioner. Genom denna förordning stärks och utvidgas det direktivets regelverk.

(4) I kommissionens meddelande av den 26 augusti 2010 med titeln *En digital agenda för Europa* utpekades fragmenteringen av den digitala marknaden, bristen på interoperabilitet och den ökande it-brottsligheten som viktiga hinder för en positiv spiral för den digitala ekonomin. I sin rapport om EU-medborgarskapet 2010 med titeln *Att undanröja hindren för EU-medborgarnas möjligheter att utöva sina rättigheter* betonade kommissionen ytterligare vikten av att undanröja de största hindren för att unionsmedborgarna ska kunna utnyttja fördelarna med en digital inre marknad och gränsöverskridande digitala tjänster.

(5) I sina slutsatser av den 4 februari 2011 och den 23 oktober 2011 uppmanade Europeiska rådet kommissionen att se till att en digital inre marknad skapas senast 2015, att göra snabba framsteg på centrala områden inom den digitala ekonomin och att främja en fullständigt integrerad digital inre marknad genom att underlätta gränsöverskridande användning av nättjänster, med särskild fokus på att underlätta säker elektronisk identifiering och autentisering.

[1] EUT C 351, 15.11.2012, s. 73.
[2] Europaparlamentets ståndpunkt av den 3 april 2014 (ännu ej offentliggjord i EUT) och rådets beslut av den 23 juli 2014.
[3] Europaparlamentets och rådets direktiv 1999/93/EG av den 13 december 1999 om ett gemenskapsramverk för elektroniska signaturer (EGT L 13, 19.1.2000, s. 12).

(6) I sina slutsatser av den 27 maj 2011 uppmanade rådet kommissionen att bidra till den digitala marknaden genom att skapa lämpliga förhållanden för ömsesidigt gränsöverskridande erkännande av grundläggande funktioner såsom elektronisk identifiering, elektroniska dokument, elektroniska underskrifter och elektroniska leveranstjänster samt för interoperabla e-förvaltningstjänster i hela EU.

(7) Europaparlamentet betonade, i sin resolution av den 21 september 2010 om fullbordandet av den inre marknaden för e-handel ([1]), betydelsen av säkerhet i elektroniska tjänster, särskilt i elektroniska underskrifter, och behovet av att skapa en infrastruktur för kryptering med öppen nyckel (PKI) i hela Europa samt uppmanade kommissionen att inrätta en europeisk nätverkssport för valideringsmyndigheter för att garantera gränsöverskridande interoperabilitet för elektroniska underskrifter och öka säkerheten i samband med transaktioner som görs via internet.

(8) Enligt Europaparlamentets och rådets direktiv 2006/123/EG ([2]) ska medlemsstaterna inrätta ”gemensamma kontaktpunkter” för att se till att alla förfaranden och formaliteter som är nödvändiga för tillträde till en tjänsteverksamhet och för att utöva den kan fullgöras enkelt, på distans och på elektronisk väg, via den lämpliga gemensamma kontaktpunkten och med behöriga myndigheter. Många nättjänster som är tillgängliga via gemensamma kontaktpunkter kräver elektronisk identifiering, autentisering och underskrift.

(9) I de flesta fall kan medborgare inte använda sin elektroniska identifiering för att autentisera sig i en annan medlemsstat därför att de nationella systemen för elektronisk identifiering i deras land inte är erkända i andra medlemsstater. Detta elektroniska hinder utestänger tillhandahållare av tjänster från möjligheten att fullt ut utnyttja fördelarna med den inre marknaden. Ömsesidigt erkända medel för elektronisk identifiering kommer att underlätta tillhandahållandet av en rad olika tjänster över gränserna på den inre marknaden och ge företagen möjlighet att verka över gränserna utan att stöta på en mängd hinder i sina kontakter med myndigheter.

(10) Genom Europaparlamentets och rådets direktiv 2011/24/EU ([3]) inrättades ett nätverk av nationella myndigheter som är ansvariga för e-hälsa. I syfte att öka säkerheten och kontinuiteten i gränsöverskridande hälso- och sjukvård ska nätverket utarbeta riktlinjer om tillgång till elektroniska hälso- och sjukvårdsuppgifter samt tjänster, inklusive genom att stödja ”gemensamma åtgärder för identifiering och autentisering för att underlätta överförbara uppgifter i gränsöverskridande hälso- och sjukvård”. Ömsesidigt erkännande av elektronisk identifiering och autentisering är en förutsättning för att gränsöverskridande sjukvård ska kunna bli verklighet för Europas befolkning. Om personer reser för att söka vård måste deras sjukjournaler vara tillgängliga i behandlingslandet. Detta förutsätter robusta, säkra och tillförlitliga ramar för elektronisk identifiering.

(11) Denna förordning bör tillämpas i full överensstämmelse med de principer om skydd av personuppgifter som föreskrivs i Europaparlamentets och rådets direktiv 95/46/EG ([4]). Vad gäller principen om ömsesidigt erkännande som fastställs genom denna förordning bör autentisering för en nättjänst endast avse behandling av den identifieringsinformation som är adekvat, relevant och som inte går utöver vad som är nödvändigt för att få tillgång till den aktuella nättjänsten. Därtill bör kraven i direktiv 95/46/EG om sekretess och säkerhet vid behandling följas av tillhandahållaren av betrodda tjänster och tillsynsorgan.

(12) Ett av målen för denna förordning är att undanröja befintliga hinder för den gränsöverskridande användningen av medel för elektronisk identifiering som används i medlemsstaterna för autentisering för åtminstone offentliga tjänster. Denna förordning syftar inte till att ingripa i fråga om elektroniska identitetshanteringssystem och tillhörande infrastrukturer som inrättats i medlemsstaterna. Syftet med denna förordning är att se till att säker elektronisk identifiering och autentisering för åtkomst till gränsöverskridande nättjänster som erbjuds av medlemsstaterna är möjlig.

([1]) EUT C 50 E, 21.2.2012, s. 1.
([2]) Europaparlamentets och rådets direktiv 2006/123/EG av den 12 december 2006 om tjänster på den inre marknaden (EUT L 376, 27.12.2006, s. 36).
([3]) Europaparlamentets och rådets direktiv 2011/24/EU av den 9 mars 2011 om tillämpningen av patienträttigheter vid gränsöverskridande hälso- och sjukvård (EUT L 88, 4.4.2011, s. 45).
([4]) Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (EGT L 281, 23.11.1995, s. 31).

(13) Medlemsstaterna bör även fortsättningsvis ha rätt att för elektronisk identifiering använda eller införa medel för åtkomst till nättjänster. De bör även ha möjlighet att själva bestämma om de vill engagera den privata sektorn i tillhandahållandet av dessa medel. Medlemsstaterna bör inte vara skyldiga att anmäla sina system för elektronisk identifiering till kommissionen. Det ankommer på medlemsstaterna att välja om de till kommissionen vill anmäla alla, några eller inga av de elektroniska identifieringssystem som används på nationell nivå för att få åtkomst till åtminstone offentliga nättjänster eller särskilda nättjänster.

(14) I förordningen bör vissa villkor fastställas rörande vilka medel för elektronisk identifiering som måste erkännas och hur systemen för elektronisk identifiering bör anmälas. Dessa villkor bör hjälpa medlemsstaterna att bygga upp det förtroende som krävs för varandras system för elektronisk identifiering samt att ömsesidigt erkänna medel för elektronisk identifiering som ingår i deras anmälda system. Principen om ömsesidigt erkännande bör gälla om den anmälande medlemsstatens system för elektronisk identifiering uppfyller villkoren för anmälan och om anmälan har offentliggjorts i *Europeiska unionens officiella tidning*. Principen om ömsesidigt erkännande bör dock endast avse autentisering för en nättjänst. Åtkomsten till dessa nättjänster och deras slutliga leverans till den sökande bör vara nära kopplad till rätten att ta emot sådana tjänster enligt villkoren i nationell lagstiftning.

(15) Skyldigheten att erkänna medel för elektronisk identifiering bör enbart avse medel vars identifieringstillitsnivå motsvarar en nivå som är lika hög eller högre än den nivå som krävs för den aktuella nättjänsten. Den skyldigheten bör dessutom endast tillämpas när det offentliga organet i fråga använder tillitsnivån väsentlig eller hög i samband med åtkomst till den nättjänsten. Medlemsstaterna bör ha rätt att, i enlighet med unionsrätten, erkänna medel för elektronisk identifiering med lägre identifieringstillitsnivåer.

(16) Tillitsnivåerna bör återge graden av tillit till ett medel för elektronisk identifiering vid fastställande av en persons identitet och skapa visshet om att den person som gör anspråk på en viss identitet faktiskt är den person som har tilldelats denna identitet. Tillitsnivån beror på den grad av tillit detta medel för elektronisk identifiering ger i fråga om en persons påstådda eller styrkta identitet med beaktande av olika processer (t.ex. styrkande och kontroll av identitet, och autentisering), förvaltningsverksamhet (t.ex. den enhet som utfärdar medel för elektronisk identifiering och förfaranden för att utfärda sådana medel) och de tekniska kontroller som tillämpas. Det finns olika tekniska definitioner och beskrivningar av tillitsnivåer tack vare unionsfinansierade storskaliga pilotprojekt, standardiseringsarbete och internationell verksamhet. Det storskaliga pilotprojektet Stork och ISO 29115 avser, bland annat, nivåerna 2, 3 och 4, som bör tas under noggrant övervägande vid fastställandet av minsta tekniska krav, standarder och förfaranden för tillitsnivåerna låg, väsentlig och hög enligt denna förordning, samtidigt som en konsekvent tillämpning av denna förordning säkerställs med särskilt hänseende på tillitsnivån hög i samband med styrkande av identitet för utfärdande av kvalificerade certifikat. De fastställda kraven ska vara teknikneutrala. Det ska vara möjligt att uppnå de nödvändiga tekniska kraven med hjälp av olika tekniklösningar.

(17) Medlemsstaterna bör uppmana den privata sektorn att frivilligt använda medel för elektronisk identifiering inom ramen för ett anmält system för identifieringsändamål när detta behövs för nättjänster eller elektroniska transaktioner. Genom möjligheten att använda sådana medel för elektronisk identifiering kan den privata sektorn förlita sig på elektronisk identifiering och autentisering som redan i stor utsträckning används i många medlemsstater för åtminstone offentliga tjänster, samtidigt som det blir lättare för företag och medborgare att få åtkomst till sina gränsöverskridande nättjänster. För att göra det lättare för den privata sektorn att använda sådana gränsöverskridande medel för elektronisk identifiering bör den autentiseringsmöjlighet som tillhandahålls av en medlemsstat vara tillgänglig för de förlitande parter i den privata sektorn som är etablerade utanför denna medlemsstats territorium på samma villkor som för de förlitande parter i den privata sektorn som är etablerade i denna medlemsstat. Med hänsyn till förlitande parter i den privata sektorn får den anmälande medlemsstaten fastställa villkor för åtkomst till medlen för autentisering. Sådana villkor för åtkomst kan innehålla uppgift om huruvida medlen för autentisering för det anmälda systemet för närvarande är tillgängliga för förlitande parter i den privata sektorn.

(18) I denna förordning bör det föreskrivas skadeståndsansvar för den anmälande medlemsstaten, den part som utfärdar medlet för elektronisk identifiering och den part som handhar autentiseringsförfarandet vid underlåtenhet att uppfylla relevanta skyldigheter enligt denna förordning. Denna förordning bör dock tillämpas i enlighet med nationella bestämmelser om skadeståndsansvar. Den ska därför inte påverka tillämpningen av dessa nationella bestämmelser om t.ex. definition av skada eller relevanta tillämpliga förfaranderegler, inbegripet regler om bevisbörda.

(19) Säkerheten i system för elektronisk identifiering är avgörande för ett tillförlitligt gränsöverskridande ömsesidigt erkännande av medel för elektronisk identifiering. Mot denna bakgrund bör medlemsstaterna samarbeta med avseende på säkerheten och interoperabiliteten i systemen för elektronisk identifiering på unionsnivå. När system för elektronisk identifiering kräver att förlitande parter på nationell nivå använder särskild maskinvara eller programvara förutsätter den gränsöverskridande interoperabiliteten att dessa medlemsstater inte inför sådana krav och därtill hörande kostnader för förlitande parter som är etablerade utanför deras territorium. I så fall bör lämpliga lösningar diskuteras och utvecklas inom interoperabilitetsramverkets räckvidd. Tekniska krav som har sin grund i de inneboende specifikationerna för nationella medel för elektronisk identifiering som sannolikt berör innehavarna av sådana elektroniska medel (t.ex. smartkort) är däremot oundvikliga.

(20) Medlemsstaternas samarbete bör underlätta den tekniska interoperabiliteten för de anmälda systemen för elektronisk identifiering i syfte att främja en hög nivå av förtroende och en säkerhetsnivå som är anpassad till risknivån. Ett utbyte av information och bästa praxis mellan medlemsstaterna med sikte på ömsesidigt erkännande bör bidra till detta samarbete.

(21) Genom denna förordning bör även ett allmänt regelverk för användningen av betrodda tjänster upprättas. Någon allmän skyldighet att använda dem eller att installera en accesspunkt för alla befintliga betrodda tjänster bör dock inte skapas. I synnerhet bör den inte gälla tillhandahållande av tjänster som endast används inom slutna system mellan en avgränsad uppsättning deltagare, och som inte påverkar tredje man. Exempelvis system som inrättats i företag eller offentlig förvaltning för hantering av interna förfaranden där betrodda tjänster används bör inte omfattas av kraven i denna förordning. Endast betrodda tjänster som tillhandahålls för allmänheten och som påverkar tredje man bör uppfylla de krav som fastställs i denna förordning. Denna förordning bör inte heller gälla frågor som avser ingående eller giltighet av avtal eller andra rättsliga förpliktelser om nationell rätt eller unionsrätten föreskriver vissa formkrav. Den bör inte heller inverka på nationella formkrav avseende offentliga register, i synnerhet inte kommersiella register eller fastighetsregister.

(22) För att bidra till deras allmänna gränsöverskridande användning bör det vara möjligt att använda betrodda tjänster som bevis vid rättsliga förfaranden i alla medlemsstater. Rättsverkan av betrodda tjänster ska definieras i nationell rätt, om inte annat föreskrivs i denna förordning.

(23) I den mån denna förordning medför en skyldighet att erkänna en betrodd tjänst, får en sådan betrodd tjänst ogillas endast om skyldighetens adressat av tekniska skäl bortom adressatens direkta kontroll är oförmögen att läsa eller kontrollera den. Denna skyldighet bör dock inte i sig medföra att ett offentligt organ är tvunget att anskaffa den maskinvara och programvara som krävs för teknisk läsbarhet för alla befintliga betrodda tjänster.

(24) Medlemsstaterna får behålla eller införa nationella bestämmelser, i överensstämmelse med unionsrätten, avseende betrodda tjänster så länge dessa tjänster inte har harmoniserats fullständigt genom denna förordning. Betrodda tjänster som överensstämmer med denna förordning bör dock omfattas av fri rörlighet på den inre marknaden.

(25) Utöver de tjänster som ingår i den fasta förteckning över betrodda tjänster som avses i denna förordning bör medlemsstaterna ha frihet att fastställa andra typer av betrodda tjänster för erkännande på nationell nivå som kvalificerade betrodda tjänster.

(26) På grund av den snabba tekniska utvecklingen bör denna förordning omfatta en strategi som är öppen för innovation.

(27) Denna förordning bör vara teknikneutral. Den rättsliga verkan som den medför bör vara möjlig att uppnå med alla typer av tekniska medel, förutsatt att kraven i denna förordning är uppfyllda.

(28) För att framför allt öka små och medelstora företags samt konsumenternas förtroende för den inre marknaden och för att främja användningen av betrodda tjänster och produkter, bör begreppen kvalificerade betrodda tjänster och kvalificerad tillhandahållare av betrodda tjänster införas i syfte att ange krav och skyldigheter som säkerställer hög grad av säkerhet oavsett vilken typ av kvalificerad betrodd tjänst eller produkt som används eller tillhandahålls.

(29) I linje med de skyldigheter som följer av Förenta nationernas konvention om rättigheter för personer med funktionsnedsättning, som godkändes genom rådets beslut 2010/48/EG ([1]), särskilt artikel 9 i konventionen, bör personer med funktionshinder kunna använda betrodda tjänster och slutanvändarprodukter som används vid tillhandahållandet av dessa tjänster på samma villkor som andra konsumenter. När det är genomförbart bör därför betrodda tjänster som tillhandahålls och slutanvändarprodukter som används i samband med tillhandahållandet av dessa tjänster göras tillgängliga för personer med funktionsnedsättning. Genomförbarhetsbedömningen bör inbegripa tekniska och ekonomiska överväganden.

(30) Medlemsstaterna bör utse ett eller flera tillsynsorgan för genomförandet av tillsynsverksamheten enligt denna förordning. Medlemsstaterna bör också kunna fatta beslut, efter ömsesidig överenskommelse med en annan medlemsstat, om att utse ett tillsynsorgan på den andra medlemsstatens territorium.

(31) Tillsynsorgan bör samarbeta med dataskyddsmyndigheter, t.ex. genom att informera dem om resultatet av granskningar av kvalificerade tillhandahållare av betrodda tjänster, när det förefaller ha skett en överträdelse av reglerna om skydd för personuppgifter. Bestämmelsen om information bör särskilt gälla säkerhetstillbud och personuppgiftsöverträdelser.

(32) För att öka användarnas förtroende för den inre marknaden bör det åligga alla tillhandahållare av betrodda tjänster att tillämpa goda säkerhetsförfaranden som är lämpliga i förhållande till de risker som deras verksamhet är förenad med.

(33) Bestämmelser om användningen av pseudonymer i certifikat bör inte hindra medlemsstaterna från att kräva identifiering av personer i enlighet med unionsrätten eller nationell rätt.

(34) För att säkerställa en jämförbar säkerhetsnivå i fråga om kvalificerade betrodda tjänster bör alla medlemsstater följa gemensamma grundläggande tillsynskrav. För att underlätta enhetlig tillämpning av dessa krav i hela unionen bör medlemsstaterna införa jämförbara förfaranden och utbyta information om sin tillsynsverksamhet och bästa praxis på området.

(35) Alla tillhandahållare av betrodda tjänster bör omfattas av kraven i denna förordning, särskilt de som gäller säkerhet och skadeståndsansvar, för att säkerställa vederbörlig noggrannhet, insyn och ansvarighet i sina verksamheter och tjänster. Med tanke på den typ av tjänster som de tillhandahåller bör det emellertid med avseende på dessa krav göras åtskillnad mellan kvalificerade och icke kvalificerade tillhandahållare av betrodda tjänster.

(36) Inrättandet av ett tillsynssystem för alla tillhandahållare av betrodda tjänster bör säkerställa lika villkor för säkerheten och tillförlitligheten i deras åtgärder och tjänster, och därigenom bidra till användarskyddet och till en fungerande inre marknad. Icke-kvalificerade tillhandahållare av betrodda tjänster bör omfattas av mindre omfattande, förebyggande tillsynsverksamhet i efterhand som är anpassad till arten av deras tjänster och åtgärder. Tillsynsorganet bör därför inte ha någon allmän skyldighet att utöva tillsyn av icke-kvalificerade tillhandahållare av betrodda tjänster. Tillsynsorganet bör endast vidta åtgärder när det har informerats (t.ex. av den icke-kvalificerade tillhandahållaren av betrodda tjänster själv, av ett annat tillsynsorgan, genom anmälan från en användare eller en affärspartner eller på grundval av en egen utredning) om att en icke-kvalificerad tillhandahållare av betrodda tjänster inte uppfyller kraven i denna förordning.

([1]) Rådets beslut 2010/48/EG av den 26 november 2009 om ingående från Europeiska gemenskapens sida av Förenta nationernas konvention om rättigheter för personer med funktionsnedsättning (EUT L 23, 27.1.2010, s. 35).

(37) Denna förordning bör föreskriva skadeståndsansvar för alla tillhandahållare av betrodda tjänster. Den fastställer särskilt det system för skadeståndsansvar enligt vilket alla tillhandahållare av betrodda tjänster bör ha skadeståndsansvar för skada som åsamkats en fysisk eller juridisk person genom underlåtenhet att uppfylla kraven i denna förordning. För att underlätta bedömningen av den ekonomiska risk som tillhandahållare av betrodda tjänster kan vara tvungna att bära eller som de bör täcka genom försäkring, tillåts tillhandahållare av betrodda tjänster genom denna förordning att på vissa villkor fastställa begränsningar för användningen av de tjänster de tillhandahåller, varvid de inte ska hållas ansvariga för skada som uppkommit genom sådan användning av tjänster som överskrider dessa begränsningar. Kunder bör vederbörligen informeras i förväg om begränsningarna. Sådana begränsningar bör vara igenkännliga för tredje man, t.ex. genom att information om begränsningarna bifogas villkoren för den tillhandahållna tjänsten eller genom andra igenkännliga medel. För att dessa principer ska kunna genomföras bör denna förordning tillämpas i enlighet med nationella bestämmelser om skadeståndsansvar. Denna förordning påverkar därför inte dessa nationella bestämmelser om t.ex. definitionen av skada, avsikt, oaktsamhet eller relevanta tillämpliga procedurregler.

(38) Det är mycket viktigt att säkerhetsincidenter och bedömningar av säkerhetsrisker anmäls så att berörda parter kan förses med tillräcklig information i händelse av en säkerhetsincident eller en integritetsförlust.

(39) För att kommissionen och medlemsstaterna ska kunna bedöma hur effektiv den mekanism för anmälan av överträdelser som införs genom denna förordning är, bör tillsynsorganen vara skyldiga att överlämna sammanfattande information till kommissionen och till Europeiska byrån för nät- och informationssäkerhet (Enisa).

(40) För att kommissionen och medlemsstaterna ska kunna bedöma hur effektiv den förstärkta tillsynsmekanism som införs genom denna förordning är, bör tillsynsorganen vara skyldiga att rapportera om sin verksamhet. Detta skulle kraftigt bidra till att underlätta utbytet av god praxis mellan tillsynsorganen och säkerställa kontrollen av att väsentliga tillsynskrav genomförs på ett enhetligt och verkningsfullt sätt i alla medlemsstater.

(41) För att säkerställa att kvalificerade betrodda tjänster är hållbara och varaktiga samt för att öka användarnas förtroende för kontinuiteten i dessa tjänster, bör tillsynsorganen kontrollera befintlighet och korrekt tillämpning av bestämmelser om planer för verksamhetens upphörande när kvalificerade tillhandahållare av betrodda tjänster upphör med sin verksamhet.

(42) För att underlätta tillsynen av kvalificerade tillhandahållare av betrodda tjänster, t.ex. när en sådan tillhandahåller sina tjänster i en annan medlemsstat och inte omfattas av tillsyn där, eller när en tillhandahållares datorer är placerade i en annan medlemsstat än den där tillhandahållaren är etablerad, bör ett system för ömsesidigt bistånd mellan medlemsstaternas tillsynsorgan inrättas.

(43) För att säkerställa att kvalificerade tillhandahållare av betrodda tjänster och de tjänster de tillhandahåller uppfyller de krav som fastställs i denna förordning bör en bedömning av överensstämmelse utföras av organ för bedömning av överensstämmelse, och de rapporter om överensstämmelsebedömning dessa resulterar i bör av den kvalificerade tillhandahållaren av betrodda tjänster lämnas in till tillsynsorganet. Om tillsynsorganet begär att en kvalificerad tillhandahållare av betrodda tjänster ska lämna in en särskild rapport om överensstämmelsebedömning, bör tillsynsorganet särskilt respektera principen om god förvaltning, inbegripet skyldigheten att motivera beslut, samt proportionalitetsprincipen. Tillsynsorganet bör därför vederbörligen motivera sitt beslut om krav på särskild överensstämmelsebedömning.

(44) Målet med denna förordning är att säkerställa ett konsekvent ramverk i syfte att tillhandahålla en hög nivå av säkerhet och rättssäkerhet för betrodda tjänster. I detta avseende bör kommissionen när den behandlar bedömning av överensstämmelse av produkter och tjänster i tillämpliga fall söka synergier med befintliga relevanta europeiska och internationella system så som Europaparlamentets och rådets förordning (EG) nr 765/2008 [1] om krav för ackreditering av organ för bedömning av överensstämmelse och marknadskontroll av produkter.

[1] Europaparlamentets och rådets förordning (EG) nr 765/2008 av den 9 juli 2008 om krav för ackreditering och marknadskontroll i samband med saluföring av produkter och upphävande av förordning (EEG) nr 339/93 (EUT L 218, 13.8.2008, s. 30).

(45) För att få till stånd en effektiv initieringsprocess, som bör leda till att kvalificerade tillhandahållare av betrodda tjänster och de kvalificerade betrodda tjänster de tillhandahåller införs i förteckningar över betrodda tjänsteleverantörer, bör man uppmuntra inledande kontakter mellan potentiella kvalificerade tillhandahållare av betrodda tjänster och behöriga tillsynsorgan, i syfte att underlätta den *due diligence*-granskning som ska leda fram till tillhandahållandet av kvalificerade betrodda tjänster.

(46) Förteckningar över betrodda tjänsteleverantörer kan vara viktiga för att hjälpa till att bygga upp förtroendet bland aktörer på marknaden, eftersom de visar att tillhandahållaren av tjänster vid tidpunkten för tillsynen hade status som kvalificerad.

(47) För att användare ska kunna dra full nytta av och veta att de kan förlita sig på nättjänster är det nödvändigt att de har förtroende för nättjänsterna och att dessa är lättillgängliga. Det bör därför inrättas ett EU-förtroendemärke för att identifiera kvalificerade betrodda tjänster som tillhandhålls av kvalificerade tillhandahållare av betrodda tjänster. Ett sådant EU-förtroendemärke av kvalificerade betrodda tjänster skulle göra tydlig åtskillnad mellan kvalificerade betrodda tjänster och andra betrodda tjänster och på så sätt bidra till insynen på marknaden. Det bör vara frivilligt för kvalificerade tillhandahållare av betrodda tjänster att använda sig av ett EU-förtroendemärke och detta bör inte medföra några andra krav än de som föreskrivs i denna förordning.

(48) Det krävs en hög tillitsnivå för att säkerställa ömsesidigt erkännande av elektroniska underskrifter, men i vissa fall, som t.ex. inom ramen för kommissionens beslut 2009/767/EG [1] bör även elektroniska underskrifter med en lägre säkerhetsgrad godtas.

(49) Denna förordning bör fastställa principen om att en elektronisk underskrift inte bör förvägras rättslig verkan på grund av att den har elektronisk form eller inte uppfyller kraven för en kvalificerad elektronisk underskrift. Den rättsliga verkan av elektroniska underskrifter ska emellertid definieras i nationell rätt, med undantag för kraven i denna förordning på att en kvalificerad elektronisk underskrift ska ha samma rättsliga verkan som en handskriven underskrift.

(50) Eftersom behöriga myndigheter i medlemsstaterna för närvarande använder olika avancerade elektroniska underskrifter av olika format för att underteckna sina dokument elektroniskt är det nödvändigt att se till att åtminstone ett visst antal format av avancerade elektroniska underskrifter kan stödjas tekniskt av medlemsstaterna när de erhåller dokument som undertecknats elektroniskt. På samma sätt skulle det när behöriga myndigheter i medlemsstaterna använder avancerade elektroniska stämplar vara nödvändigt att se till att de stöder åtminstone ett visst antal format av avancerade elektroniska stämplar.

(51) Det bör vara möjligt för undertecknare att anförtro anordningar för skapande av kvalificerade elektroniska underskrifter till tredje man, förutsatt att lämpliga mekanismer och förfaranden tillämpas för att se till att undertecknaren har användningen av sina uppgifter för skapande av elektroniska underskrifter uteslutande under sin egen kontroll och att kraven för kvalificerade elektroniska underskrifter uppfylls genom anordningens användning.

(52) Om miljön för skapande av elektroniska underskrifter styrs av en tillhandahållare av betrodda tjänster på uppdrag av undertecknaren, kommer elektroniska underskrifter på distans med säkerhet att utvecklas på grund av sina många ekonomiska fördelar. För att säkerställa att dessa elektroniska underskrifter får samma rättsliga erkännande som elektroniska underskrifter som skapas i en miljö som helt och hållet styrs av användaren bör emellertid tillhandahållare av tjänster för elektroniska underskrifter på distans tillämpa särskilda säkerhetsförfaranden för förvaltning och administration samt använda tillförlitliga system och produkter, bland annat säkra elektroniska kommunikationskanaler, för att säkerställa en tillförlitlig miljö för skapande av elektroniska underskrifter som undertecknaren använder uteslutande under sin egen kontroll. För en kvalificerad elektronisk underskrift som skapas med en anordning för skapande av elektroniska underskrifter på distans bör de krav som gäller för kvalificerade tillhandahållare av betrodda tjänster och som anges i denna förordning tillämpas.

[1] Kommissionens beslut 2009/767/EG av den 16 oktober 2009 om åtgärder som underlättar användningen av förfaranden på elektronisk väg genom gemensamma kontaktpunkter i enlighet med Europaparlamentets och rådets direktiv 2006/123/EG om tjänster på den inre marknaden (EUT L 274, 20.10.2009, s. 36).

(53) Tillfälligt upphävande av kvalificerade certifikat är etablerad operativ praxis för tillhandahållare av betrodda tjänster i ett antal medlemsstater som skiljer sig från återkallande och medför en tillfällig förlust av giltighet för ett certifikat. Rättsäkerheten kräver att ett certifikats status som tillfälligt upphävt alltid ska anges klart och tydligt. Tillhandahållare av betrodda tjänster bör därför ansvara för att klart och tydligt ange ett certifikats status och, om detta upphävs, den exakta tidsperiod under vilket certifikatet har tillfälligt upphävts. Denna förordning bör inte ålägga tillhandahållare av betrodda tjänster eller medlemsstater att använda sig av tillfälligt upphävande men bör tillhandahålla transparensregler för när och hur en sådan möjlighet finns.

(54) Gränsöverskridande erkännande av kvalificerade elektroniska underskrifter förutsätter gränsöverskridande interoperabilitet och erkännande av kvalificerade certifikat. Därför bör inte kvalificerade certifikat omfattas av några obligatoriska krav som går utöver kraven i denna förordning. På nationell nivå bör man dock få inkludera särskilda egenskaper, t.ex. unika identifierare, i kvalificerade certifikat, under förutsättning att sådana särskilda egenskaper inte hindrar gränsöverskridande interoperabilitet och erkännande av kvalificerade certifikat och elektroniska underskrifter.

(55) It-säkerhetscertifiering som bygger på internationella standarder, såsom ISO 15408 och besläktade utvärderingsmetoder och arrangemang för ömsesidigt erkännande, utgör ett viktigt verktyg för att kontrollera säkerheten hos kvalificerade anordningar för skapande av elektroniska underskrifter och bör främjas. Innovativa lösningar och tjänster, såsom undertecknande via mobil och datamoln, förlitar sig emellertid på tekniska och organisatoriska lösningar för kvalificerade anordningar för skapande av elektroniska underskrifter, för vilka det eventuellt ännu inte finns tillgängliga säkerhetsstandarder eller för vilka den första it-säkerhetscertifieringen pågår. Säkerhetsnivån för sådana kvalificerade anordningar för skapande av elektroniska underskrifter skulle kunna utvärderas genom alternativa processer endast om sådana säkerhetsstandarder inte finns tillgängliga eller om den första it-säkerhetscertifieringen pågår. De processerna bör vara jämförbara med standarderna för it-säkerhetscertifiering i den mån deras säkerhetsnivåer är likvärdiga. Förfarandena skulle dessutom kunna underlättas av en sakkunnighetsbedömning.

(56) I denna förordning bör det fastställas krav på kvalificerade anordningar för skapande av elektroniska underskrifter för att säkerställa de avancerade elektroniska underskrifternas funktionalitet. Denna förordning bör inte omfatta hela den systemmiljö där sådana anordningar används. Därför bör omfattningen av certifieringen av kvalificerade anordningar för skapande av elektroniska underskrifter begränsas till den hårdvara och systemprogramvara som används för att hantera och skydda uppgifterna för skapande av underskrifter som skapas, lagras eller behandlas i anordningen för skapande av underskrifter. I enlighet med vad som fastställs i relevanta standarder bör certifieringsskyldigheterna inte omfatta tillämpningar för skapande av underskrifter.

(57) För att säkerställa rättssäkerheten avseende en underskrifts giltighet är det nödvändigt att specificera vilka komponenter i en kvalificerad elektronisk underskrift som bör bedömas av den förlitande part som utför valideringen. Genom att specificera kraven på kvalificerade tillhandahållare av betrodda tjänster som kan tillhandahålla en kvalificerad valideringstjänst till förlitande parter som inte själva vill eller kan utföra valideringen av kvalificerade elektroniska underskrifter bör dessutom privat och offentlig sektor stimuleras att investera i sådana tjänster. Sammantaget bör dessa krav göra kvalificerad validering av elektroniska underskrifter enkel och bekväm för alla parter på unionsnivå.

(58) När en transaktion kräver en kvalificerad elektronisk stämpel från en juridisk person bör en kvalificerad elektronisk underskrift från ett behörigt ombud för den juridiska personen vara lika godtagbar.

(59) Elektroniska stämplar bör utgöra bevis för att ett elektroniskt dokument har utfärdats av en juridisk person och säkerställa visshet om dokumentets ursprung och integritet.

(60) Tillhandahållare av betrodda tjänster som utfärdar kvalificerade certifikat för elektroniska stämplar bör vidta de åtgärder som krävs för att kunna fastställa identiteten för den fysiska person som representerar den juridiska person som har fått ett kvalificerat certifikat för en elektronisk stämpel, om sådan identifiering krävs på nationell nivå inom ramen för juridiska eller administrativa förfaranden.

(61) Genom denna förordning bör långsiktigt bevarande av uppgifter säkerställas, för att säkerställa den rättsliga giltigheten hos elektroniska underskrifter och elektroniska stämplar över längre tidsperioder och garantera att de kan valideras oavsett kommande tekniska förändringar.

(62) I syfte att säkerställa säkerheten hos kvalificerad elektronisk tidsstämpling bör det i denna förordning krävas att man använder en avancerad elektronisk stämpel eller en avancerad elektronisk underskrift eller andra likvärdiga metoder. Sannolikt kan innovation leda till ny teknik som kan säkerställa en likvärdig säkerhetsnivå för tidsstämpling. Vid användning av någon annan metod än avancerade elektroniska stämplar eller avancerade elektroniska underskrifter bör det åligga tillhandahållaren av betrodda tjänster att i rapporten om bedömning av överensstämmelse visa att denna metod säkerställer en likvärdig säkerhetsnivå och att den är förenlig med skyldigheterna i denna förordning.

(63) Elektroniska dokument är viktiga för vidareutveckling av gränsöverskridande elektroniska transaktioner på den inre marknaden. Denna förordning bör fastställa principen om att ett elektroniskt dokument inte bör förvägras rättslig verkan på grund av att det har elektronisk form, för att säkerställa att elektroniska transaktioner inte kommer att ogillas enbart på grund av att ett dokument har elektronisk form.

(64) När kommissionen behandlar formaten för avancerade elektroniska underskrifter och stämplar ska den bygga vidare på den praxis, de standarder och den lagstiftning som redan finns, i synnerhet kommissionens beslut 2011/130/EU [1].

(65) Elektroniska stämplar kan användas för att autentisera ett dokument som utfärdats av en juridisk person, men även för att autentisera en juridisk persons digitala tillgångar, t.ex. programvarukoder eller servrar.

(66) Det är av avgörande betydelse att det föreskrivs en rättslig ram för att främja gränsöverskridande erkännande mellan befintliga nationella rättssystem för elektroniska tjänster för rekommenderade leveranser. Den ramen skulle också kunna öppna nya marknadsmöjligheter för unionens tillhandahållare av betrodda tjänster att erbjuda nya paneuropeiska tjänster för elektroniska tjänster för rekommenderade leveranser.

(67) Tjänster för autentisering av webbplatser innebär möjlighet för en besökare på en webbplats att försäkra sig om att en verklig och legitim enhet står bakom webbplatsen. Dessa tjänster bidrar till att bygga upp förtroendet för näthandeln, eftersom användarna kommer att ha förtroende för en webbplats som har autentiserats. Tillhandahållande och användning av tjänster för autentisering av webbplatser är fullständigt frivilligt. För att autentiseringen av webbplatser ska kunna bli ett sätt att stärka förtroendet, ge användaren en bättre upplevelse och främja tillväxten på den inre marknaden bör man emellertid i denna förordning föreskriva minimiskyldigheter vad gäller säkerhet och skadeståndsansvar för tillhandahållarna och deras tjänster. Därför har hänsyn tagits till resultaten av befintliga initiativ ledda av industrin, t.ex. forumet för certifieringsinstanser och försäljare av webbläsare – CA/B Forum. Dessutom bör denna förordning inte hindra användning av andra sätt eller metoder för att autentisera webbplatser som inte omfattas av denna förordning och förordningen bör inte heller hindra tillhandahållare av autentiseringstjänster i tredjeland från att tillhandahålla sina tjänster till kunder i unionen. En tillhandahållare från ett tredjeland bör dock endast kunna få sina tjänster för autentisering av webbplatser erkända som kvalificerade i enlighet med denna förordning om ett internationellt avtal mellan unionen och det land i vilket tillhandahållaren är etablerad har ingåtts.

(68) Begreppet *juridisk person* enligt bestämmelserna om etablering i fördraget om Europeiska unionens funktionssätt (EUF-fördraget) ger aktörer möjlighet att fritt välja den juridiska form de anser vara lämplig för att bedriva sin verksamhet. Följaktligen omfattar begreppet *juridisk person* enligt EUF-fördraget alla enheter, oberoende av juridisk form, som bildats i enlighet med eller som omfattas av rätten i en medlemsstat.

(69) Unionens institutioner, organ och byråer uppmanas att erkänna elektronisk identifiering och betrodda tjänster som omfattas av denna förordning för administrativt samarbete som drar nytta av framför allt befintlig god praxis och resultaten av pågående projekt på de områden som omfattas av denna förordning.

[1] Kommissionens beslut 2011/130/EU av den 25 februari 2011 om fastställande av minimikrav för behandling över gränserna av dokument som signerats elektroniskt av behöriga myndigheter i enlighet med Europaparlamentets och rådets direktiv 2006/123/EG om tjänster på den inre marknaden (EUT L 53, 26.2.2011, s. 66).

(70) I syfte att på ett flexibelt och snabbt sätt kunna komplettera vissa detaljerade tekniska aspekter av denna förordning bör befogenheten att anta akter i enlighet med artikel 290 i EUF-fördraget delegeras till kommissionen med avseende på de kriterier som ska uppfyllas av organ med ansvar för certifieringen av kvalificerade anordningar för skapande av elektroniska underskrifter. Det är av särskild betydelse att kommissionen genomför lämpliga samråd under sitt förberedande arbete, inklusive på expertnivå. När kommissionen förbereder och utarbetar delegerade akter bör den se till att relevanta handlingar översänds samtidigt till Europaparlamentet och rådet och att detta sker så snabbt som möjligt och på lämpligt sätt.

(71) För att säkerställa enhetliga villkor för genomförandet av denna förordning, bör kommissionen tilldelas genomförandebefogenheter, särskilt för att ange referensnummer till standarder vilkas användning skulle skapa presumtion för överensstämmelse med vissa krav i denna förordning. Dessa befogenheter bör utövas i enlighet med Europaparlamentets och rådets förordning (EU) nr 182/2011 ([1]).

(72) När kommissionen antar delegerade akter eller genomförandeakter bör den ta vederbörlig hänsyn till de standarder och tekniska specifikationer som utarbetats av europeiska och internationella standardiseringsorgan, särskilt Europeiska standardiseringskommittén (CEN), Europeiska institutet för telekommunikationsstandarder (Etsi), Internationella standardiseringsorganisationen (ISO) och Internationella teleunionen (ITU), i syfte att säkerställa en hög nivå av säkerhet och interoperabilitet när det gäller elektronisk identifiering och betrodda tjänster.

(73) Av rättssäkerhets- och tydlighetsskäl bör direktiv 1999/93/EG upphävas.

(74) För att säkerställa rättssäkerheten för marknadsoperatörer som redan använder kvalificerade certifikat som utfärdas för fysiska personer i enlighet med direktiv 1999/93/EG är det nödvändigt att föreskriva en tillräckligt lång övergångsperiod. Övergångsåtgärder bör även fastställas för säkra anordningar för skapande av underskrifter vars överensstämmelse har fastställts i enlighet med direktiv 1999/93/EG samt för tillhandahållare av certifikattjänster som utfärdar kvalificerade certifikat före den 1 juli 2016. Slutligen är det också nödvändigt att göra det möjligt för kommissionen att anta genomförandeakter och delegerade akter före det datumet.

(75) De tillämpningsdagar som anges i denna förordning påverkar inte medlemsstaternas befintliga skyldigheter enligt unionsrätten, särskilt direktiv 2006/123/EG.

(76) Eftersom målen för denna förordning inte i tillräcklig utsträckning kan uppnås av medlemsstaterna utan snarare, på grund av åtgärdens omfattning, kan uppnås bättre på unionsnivå, kan unionen vidta åtgärder i enlighet med subsidiaritetsprincipen i artikel 5 i fördraget om Europeiska unionen. I enlighet med proportionalitetsprincipen i samma artikel går denna förordning inte utöver vad som är nödvändigt för att uppnå dessa mål.

(77) Europeiska datatillsynsmannen har hörts i enlighet med artikel 28.2 i Europaparlamentets och rådets förordning (EG) nr 45/2001 ([2]) och avgav ett yttrande den 27 september 2012 ([3]).

([1]) Europaparlamentets och rådets förordning (EU) nr 182/2011 av den 16 februari 2011 om fastställande av allmänna regler och principer för medlemsstaternas kontroll av kommissionens utövande av sina genomförandebefogenheter (EUT L 55, 28.2.2011, s. 13).

([2]) Europaparlamentets och rådets förordning (EG) nr 45/2001 av den 18 december 2000 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter (EGT L 8, 12.1.2001, s. 1).

([3]) EUT C 28, 30.1.2013, s. 6.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

KAPITEL I

ALLMÄNNA BESTÄMMELSER

Artikel 1

Syfte

I syfte att säkerställa en väl fungerande inre marknad och uppnå en lämplig säkerhetsnivå för medel för elektronisk identifiering och betrodda tjänster fastställs i denna förordning

a) de villkor på vilka medlemsstaterna erkänner medel för elektronisk identifiering av fysiska och juridiska personer som omfattas av ett anmält system för elektronisk identifiering hos en annan medlemsstat,

b) regler för betrodda tjänster, i synnerhet för elektroniska transaktioner, och

c) en rättslig ram för elektroniska underskrifter, elektroniska stämplar, elektronisk tidsstämpling, elektroniska dokument, elektroniska tjänster för rekommenderade leveranser och certifikattjänster för autentisering av webbplatser.

Artikel 2

Tillämpningsområde

1. Denna förordning gäller system för elektronisk identifiering som har anmälts av en medlemsstat, och tillhandahållare av betrodda tjänster som är etablerade inom unionen.

2. Denna förordning gäller inte tillhandahållande av betrodda tjänster som till följd av nationell rätt eller avtal mellan en avgränsad uppsättning deltagare endast används inom slutna system.

3. Denna förordning påverkar inte nationell rätt eller unionsrätt som avser ingående av avtal och deras giltighet eller andra rättsliga eller förfarandemässiga skyldigheter avseende formkrav.

Artikel 3

Definitioner

I denna förordning gäller följande definitioner:

1. *elektronisk identifiering:* en process inom vilken personidentifieringsuppgifter i elektronisk form, som unikt avser en fysisk eller juridisk person eller en fysisk person som företräder en juridisk person, används.

2. *medel för elektronisk identifiering:* en materiell och/eller immateriell enhet som innehåller personidentifieringsuppgifter och som används för autentisering för nättjänster.

3. *personidentifieringsuppgifter:* en uppsättning uppgifter som gör det möjligt att fastställa identiteten på en fysisk eller juridisk person eller en fysisk person som företräder en juridisk person.

4. *system för elektronisk identifiering:* ett system för elektronisk identifiering genom vilket medel för elektronisk identifiering utfärdas till en fysisk eller juridisk person eller en fysisk person som företräder en juridisk person.

5. *autentisering:* en elektronisk process som gör det möjligt att bekräfta den elektroniska identifieringen för en fysisk eller juridisk person, eller ursprunget för och integriteten hos uppgifter i elektronisk form.

6. *förlitande part:* en fysisk eller juridisk person som förlitar sig på en elektronisk identifiering eller betrodda tjänster.

7. *offentligt organ:* en statlig, regional eller lokal myndighet, ett organ som lyder under offentlig rätt eller en sammanslutning som bildats av en eller flera sådana myndigheter eller ett eller flera sådana offentligrättsliga organ, eller en privat enhet som av minst en av dessa myndigheter, enheter eller sammanslutningar har bemyndigats att tillhandahålla offentliga tjänster när de agerar i enlighet med ett sådant bemyndigande.

8. *offentligrättsligt organ:* ett organ enligt definitionen i artikel 2.1.4 i Europaparlamentets och rådets direktiv 2014/24/EU ([1]).

9. *undertecknare:* en fysisk person som skapar en elektronisk underskrift.

10. *elektronisk underskrift:* uppgifter i elektronisk form som är fogade till eller logiskt knutna till andra uppgifter i elektronisk form och som används av undertecknaren för att skriva under.

11. *avancerad elektronisk underskrift:* en elektronisk underskrift som uppfyller kraven enligt artikel 26.

12. *kvalificerad elektronisk underskrift:* en avancerad elektronisk underskrift som skapas med hjälp av en kvalificerad anordning för underskriftframställning och som är baserad på ett kvalificerat certifikat för elektroniska underskrifter.

13. *uppgifter för skapande av elektroniska underskrifter:* unika uppgifter som undertecknaren använder för att skapa en elektronisk underskrift.

14. *certifikat för elektroniska underskrifter:* ett elektroniskt intyg som kopplar valideringsuppgifter för en elektronisk underskrift till en fysisk person och bekräftar åtminstone namnet eller pseudonymen på den personen.

15. *kvalificerat certifikat för elektroniska underskrifter:* ett certifikat för elektroniska underskrifter som utfärdas av en kvalificerad tillhandahållare av betrodda tjänster och uppfyller kraven i bilaga I.

16. *betrodd tjänst:* en elektronisk tjänst som vanligen tillhandahålls mot ekonomisk ersättning och som består av

    a) skapande, kontroll och validering av elektroniska underskrifter, elektroniska stämplar eller elektroniska tidsstämplingar, elektroniska tjänster för rekommenderade leveranser och certifikat med anknytning till dessa tjänster, eller

    b) skapande, kontroll och validering av certifikat för autentisering av webbplatser, eller

    c) bevarande av elektroniska underskrifter, stämplar eller certifikat med anknytning till dessa tjänster.

17. *kvalificerad betrodd tjänst:* en betrodd tjänst som uppfyller tillämpliga krav i denna förordning.

([1]) Europaparlamentets och rådets direktiv 2014/24/EU av den 26 februari 2014 om offentlig upphandling och om upphävande av direktiv 2004/18/EU (EUT L 94, 28.3.2014, s. 65).

18. *organ för bedömning av överensstämmelse:* ett organ enligt definitionen i artikel 2.13 i förordning (EG) nr 765/2008 som i enlighet med den förordningen är ackrediterat för överensstämmelsebedömning av en kvalificerad tillhandahållare av en betrodd tjänst och den kvalificerade betrodda tjänst som denne tillhandahåller.

19. *tillhandahållare av betrodda tjänster:* en fysisk eller juridisk person som tillhandahåller en eller flera betrodda tjänster, antingen i egenskap av kvalificerade eller icke kvalificerade tillhandahållare av betrodda tjänster.

20. *kvalificerad tillhandahållare av betrodda tjänster:* en tillhandahållare av betrodda tjänster som tillhandahåller en eller flera kvalificerade betrodda tjänster och som beviljats status som kvalificerad av tillsynsorganet.

21. *produkt:* maskinvara eller programvara, eller relevanta komponenter i maskinvara eller programvara, som är avsedda att användas för tillhandahållande av betrodda tjänster.

22. *anordning för underskriftframställning:* en konfigurerad programvara eller maskinvara som används för att skapa en elektronisk underskrift.

23. *kvalificerad anordning för underskriftframställning:* en anordning för skapande av elektroniska underskrifter som uppfyller kraven i bilaga II.

24. *skapare av en stämpel:* en juridisk person som skapar en elektronisk stämpel.

25. *elektronisk stämpel:* 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.

26. *avancerad elektronisk stämpel:* en elektronisk stämpel som uppfyller kraven enligt artikel 36.

27. *kvalificerad elektronisk stämpel:* en avancerad elektronisk stämpel som skapas med hjälp av en kvalificerad anordning för skapande av elektroniska stämplar och som är baserat på ett kvalificerat certifikat för elektroniska stämplar.

28. *uppgifter för skapande av elektroniska stämplar:* unika uppgifter som skaparen av den elektroniska stämpeln använder för att skapa en elektronisk stämpel.

29. *certifikat för elektroniska stämplar:* ett elektroniskt intyg som kopplar valideringsuppgifter för en elektronisk stämpel till en juridisk person och bekräftar namnet på den personen.

30. *kvalificerat certifikat för elektroniska stämplar:* ett certifikat för en elektronisk stämpel som utfärdas av en kvalificerad tillhandahållare av betrodda tjänster och uppfyller kraven i bilaga III.

31. *anordning för skapande av elektroniska stämplar:* en konfigurerad programvara eller maskinvara som används för att skapa en elektronisk stämpel.

32. *kvalificerad anordning för skapande av elektroniska stämplar:* en anordning för skapande av elektroniska stämplar som efter nödvändig anpassning uppfyller kraven i bilaga II.

33. *elektronisk tidsstämpling:* uppgifter i elektronisk form som binder andra uppgifter i elektronisk form till en viss tidpunkt och därmed utgör bevis för att de senare uppgifterna existerade vid den tidpunkten.

34. *kvalificerad elektronisk tidsstämpling:* en elektronisk tidsstämpling som uppfyller de krav som fastställs i artikel 42.

35. *elektroniskt dokument:* innehåll lagrat i elektronisk form, i synnerhet som ljud-, bild- eller audiovisuell inspelning.

36. *elektronisk tjänst för rekommenderad leverans:* en tjänst som gör det möjligt att överföra uppgifter mellan tredje män på elektronisk väg och tillhandahåller bevis avseende de överförda uppgifternas hantering, inklusive bevis för uppgifternas sändning och mottagande, och som skyddar överförda uppgifter mot risken för förlust, stöld, skada eller otillåtna ändringar.

37. *kvalificerad elektronisk tjänst för rekommenderad leverans:* en elektronisk tjänst för rekommenderad leverans som uppfyller de krav som fastställs i artikel 44.

38. *certifikat för autentisering av webbplatser:* ett intyg som gör det möjligt att autentisera en webbplats och koppla webbplatsen till den fysiska eller juridiska person som certifikatet utfärdats för.

39. *kvalificerat certifikat för autentisering av webbplatser:* ett certifikat för autentisering av webbplatser som utfärdas av en kvalificerad tillhandahållare av betrodda tjänster och uppfyller kraven i bilaga IV.

40. *valideringsuppgifter:* uppgifter som används för att validera en elektronisk underskrift eller en elektronisk stämpel.

41. *validering:* en process genom vilken en elektronisk underskrifts giltighet kontrolleras och bekräftas.

Artikel 4

Inremarknadsprincipen

1. Tillhandahållande av betrodda tjänster i en medlemsstat som utförs av en tillhandahållare av betrodda tjänster som är etablerad i en annan medlemsstat får inte begränsas av skäl som omfattas av de områden som regleras i denna förordning.

2. Produkter och betrodda tjänster som överensstämmer med denna förordning ska omfattas av fri rörlighet på den inre marknaden.

Artikel 5

Behandling och skydd av uppgifter

1. Personuppgifter ska behandlas i enlighet med direktiv 95/46/EG.

2. Utan att det påverkar rättsverkan av pseudonymer enligt nationell rätt ska användningen av pseudonymer vid elektroniska transaktioner inte förbjudas.

KAPITEL II

ELEKTRONISK IDENTIFIERING

Artikel 6

Ömsesidigt erkännande

1. När det enligt nationell rätt eller enligt nationella administrativa förfaranden krävs en elektronisk identifiering där medel för elektronisk identifiering och autentisering används för att få åtkomst till en nättjänst som tillhandahålls av ett offentligt organ i en medlemsstat, ska de medel för elektronisk identifiering som utfärdats i en annan medlemsstat erkännas i den första medlemsstaten för gränsöverskridande autentisering för den tjänsten via internet, förutsatt att

a) medlet för elektronisk identifiering är utfärdat inom ramen för ett system för elektronisk identifiering som ingår i den förteckning som offentliggjorts av kommissionen enligt artikel 9,

b) tillitsnivån för medlet för elektronisk identifiering motsvarar en tillitsnivå som är lika hög som eller högre än den tillitsnivå som det berörda offentliga organet kräver för åtkomst till denna nättjänst i den första medlemsstaten, förutsatt att tillitsnivån för detta medel för elektronisk identifiering motsvarar tillitsnivån väsentlig eller hög,

c) det offentliga organet i fråga använder tillitsnivån väsentlig eller hög i samband med åtkomst till nättjänsten.

Ett sådant erkännande ska ske senast tolv månader efter det att kommissionen offentliggör den förteckning som avses i led a i första stycket.

2. Ett medel för elektronisk identifiering som utfärdats inom ramen för ett system för elektronisk identifiering som ingår i den förteckning som kommissionen offentliggjort enligt artikel 9 och som motsvarar tillitsnivån låg får erkännas av offentliga organ för gränsöverskridande autentisering för den tjänst som tillhandahålls via internet av dessa organ.

Artikel 7

Berättigande till anmälan av system för elektronisk identifiering

Ett system för elektronisk identifiering ska vara berättigat till anmälan enligt artikel 9.1 om samtliga följande villkor är uppfyllda:

a) Medlet för elektronisk identifiering inom ramen för systemet för elektronisk identifiering ska vara utfärdat

i) av den anmälande medlemsstaten,

ii) på uppdrag av den anmälande medlemsstaten, eller

iii) oberoende av den anmälande medlemsstaten och erkännas av den medlemsstaten.

b) Medlet för elektronisk identifiering inom systemet för elektronisk identifiering ska kunna användas för att få åtkomst till åtminstone en tjänst som tillhandahålls av ett offentligt organ och som kräver elektronisk identifiering i den anmälande medlemsstaten.

c) Systemet för elektronisk identifiering och det medel för elektronisk identifiering som utfärdats inom ramen för det ska uppfylla kraven för åtminstone en av de tillitsnivåer som anges i den genomförandeakt som avses i artikel 8.3.

d) Den anmälande medlemsstaten ska se till att de personidentifieringsuppgifter som unikt representerar personen i fråga, i enlighet med de tekniska specifikationer, standarder och förfaranden för den relevanta tillitsnivå som anges i den genomförandeakt som avses i artikel 8.3, tillskrivs den fysiska eller juridiska person som avses i artikel 3.1 vid tidpunkten för utfärdandet av medlet för elektronisk identifiering inom detta system.

e) Den part som utfärdar medlet för elektronisk identifiering inom detta system ska se till att medlet för elektronisk identifiering tilldelas den person som avses i led d i denna artikel i enlighet med de tekniska specifikationer, standarder och förfaranden för den relevanta tillitsnivå som anges i den genomförandeakt som avses i artikel 8.3.

f) Den anmälande medlemsstaten ska se till att autentisering är tillgänglig via internet så att alla förlitande parter som är etablerade på någon annan medlemsstats territorium kan bekräfta de personidentifieringsuppgifter som tas emot i elektronisk form.

För andra förlitande parter än offentliga organ får den anmälande medlemsstaten fastställa tillträdesvillkoren för autentiseringen. Sådan gränsöverskridande autentisering ska tillhandahållas kostnadsfritt när den utförs i samband med en nättjänst som tillhandahålls av ett offentligt organ.

Medlemsstaterna får inte ålägga förlitande parter som har för avsikt att utföra en sådan autentisering oproportionella tekniska krav om sådana krav skulle hindra eller avsevärt försvåra kompatibiliteten mellan anmälda system för elektronisk identifiering.

g) Minst sex månader före anmälan enligt artikel 9.1 ska den anmälande medlemsstaten när det gäller den skyldighet som anges i artikel 12.5 förse andra medlemsstater med en beskrivning av detta system i enlighet med de förfaranden som fastställts genom de genomförandeakter som avses i artikel 12.7.

h) System för elektronisk identifiering ska uppfylla kraven i den genomförandeakt som avses i artikel 12.8.

Artikel 8

Tillitsnivåer för system för elektronisk identifiering

1. I ett system för elektronisk identifiering som anmälts i enlighet med artikel 9.1 ska tillitsnivåerna låg, väsentlig och/eller hög specificeras för medel för elektronisk identifiering som har utfärdats inom det systemet.

2. Tillitsnivåerna låg, väsentlig och hög ska uppfylla följande kriterier för respektive nivå:

a) Tillitsnivå låg ska inom ramen för ett system för elektronisk identifiering avse ett medel för elektronisk identifiering som ger en begränsad grad av tillförlitlighet avseende en persons påstådda eller styrkta identitet, och definieras med hänvisning till tekniska specifikationer, standarder och förfaranden som avser detta, inbegripet tekniska kontroller, vilkas syfte är att väsentligt minska risken för missbruk eller ändring av identiteten.

b) Tillitsnivå väsentlig ska inom ramen för ett system för elektronisk identifiering avse ett medel för elektronisk identifiering som ger en väsentlig grad av tillförlitlighet avseende en persons påstådda eller styrkta identitet, och definieras med hänvisning till tekniska specifikationer, standarder och förfaranden som avser detta, inbegripet tekniska kontroller, vilkas syfte är att väsentligt minska risken för missbruk eller ändring av identiteten.

c) Tillitsnivå hög ska inom ramen för ett system för elektronisk identifiering avse ett medel för elektronisk identifiering som ger en högre grad av tillförlitlighet avseende en persons påstådda eller styrkta identitet än tillitsnivån väsentlig, och definieras med hänvisning till tekniska specifikationer, standarder och förfaranden som avser detta, inbegripet tekniska kontroller, vilkas syfte är att förhindra risken för missbruk eller ändring av identiteten.

3. Senast den 18 september 2015, med beaktande av relevanta internationella standarder, och om inte annat följer av punkt 2, ska kommissionen genom genomförandeakter fastställa tekniska minimispecifikationer, standarder och förfaranden genom vilka tillitsnivåerna låg, väsentlig och hög specificeras för medel för elektronisk identifiering för tillämpningen av punkt 1.

Dessa tekniska minimispecifikationer, standarder och förfaranden ska fastställas med hänvisning till tillförlitligheten och kvaliteten i följande delar:

a) Förfarandet för att styrka och kontrollera identiteten på fysiska eller juridiska personer som ansöker om utfärdande av medel för elektronisk identifiering.

b) Förfarandet för att utfärda det begärda medlet för elektronisk identifiering.

c) Den autentiseringsmekanism genom vilken den fysiska eller juridiska personen använder medlet för elektronisk identifiering för att bekräfta sin identitet för en förlitande part.

d) Den enhet som utfärdar medlen för elektronisk identifiering.

e) Varje annat organ som deltar i ansökningen om utfärdande av medel för elektronisk identifiering.

f) De tekniska och säkerhetsrelaterade specifikationerna för de utfärdade medlen för elektronisk identifiering.

Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

Artikel 9

Anmälan

1. Den anmälande medlemsstaten ska till kommissionen anmäla följande uppgifter samt utan onödigt dröjsmål anmäla eventuella senare ändringar av dessa:

a) En beskrivning av systemet för elektronisk identifiering, inbegripet dess tillitsnivåer och av utfärdaren eller utfärdarna av medel för elektronisk identifiering inom systemet.

b) Det tillämpliga systemet för tillsyn och information om systemet för skadeståndsansvar med avseende på följande:

i) Den part som utfärdar medlet för elektronisk identifiering.

ii) Den part som handhar autentiseringsförfarandet.

c) Den myndighet eller de myndigheter som ansvarar för systemet för elektronisk identifiering.

d) Information om den enhet eller de enheter som hanterar registreringen av de unika personidentifieringsuppgifterna.

e) En beskrivning av hur kraven i den genomförandeakt som avses i artikel 12.8 har uppfyllts.

f) En beskrivning av den autentisering som avses i artikel 7 f.

g) System för tillfälligt upphävande eller återkallelse av det anmälda systemet för elektronisk identifiering eller autentisering eller av de berörda utsatta delarna.

2. Kommissionen ska ett år från dagen för tillämpning av de genomförandeakter som avses i artiklarna 8.3 och 12.8 offentliggöra en förteckning över de system för elektronisk identifiering som anmälts enligt punkt 1 i den här artikeln och de grundläggande uppgifterna om dessa i *Europeiska unionens officiella tidning*.

3. Om kommissionen tar emot en anmälan efter utgången av den period som avses i punkt 2 ska den i *Europeiska unionens officiella tidning* offentliggöra ändringarna i den förteckning som avses i punkt 2 inom två månader från den dag då anmälan mottogs.

4. En medlemsstat får lämna in en begäran till kommissionen om att ta bort ett system för elektronisk identifiering som anmälts av medlemsstaten från den förteckning som avses i punkt 2. Kommissionen ska offentliggöra motsvarande ändringar i förteckningen i *Europeiska unionens officiella tidning* inom en månad från den dag då medlemsstatens begäran mottogs.

5. Kommissionen får genom genomförandeakter fastställa förutsättningar, format och förfaranden för de anmälningar som avses i punkt 1. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

Artikel 10

Säkerhetsincidenter

1. Om antingen det system för elektronisk identifiering som anmälts i enlighet med artikel 9.1 eller den autentisering som avses i artikel 7 f utsätts för intrång eller delvis äventyras på ett sätt som påverkar tillförlitligheten i systemets gränsöverskridande autentisering ska den anmälande medlemsstaten utan dröjsmål tillfälligt upphäva eller återkalla denna gränsöverskridande autentisering eller de berörda utsatta delarna och informera andra medlemsstater och kommissionen.

2. När en incident eller ett äventyrande som avses i punkt 1 har åtgärdats ska den anmälande medlemsstaten återinföra den gränsöverskridande autentiseringen och utan onödigt dröjsmål informera andra medlemsstater och kommissionen om detta.

3. Om en incident eller ett äventyrande som avses i punkt 1 inte åtgärdas inom tre månader från det tillfälliga upphävandet eller återkallelsen, ska den anmälande medlemsstaten till övriga medlemsstater och kommissionen anmäla att systemet för elektronisk identifiering har dragits tillbaka.

Kommissionen ska utan onödigt dröjsmål offentliggöra motsvarande ändringar i den förteckning som avses i artikel 9.2 i *Europeiska unionens officiella tidning*.

Artikel 11

Skadeståndsansvar

1. Den anmälande medlemsstaten ska ha skadeståndsansvar för skada som åsamkats en fysisk eller juridisk person avsiktligt eller på grund av oaktsamhet genom dess underlåtenhet att uppfylla sina skyldigheter enligt artikel 7 d och f vid en gränsöverskridande transaktion.

2. Den part som utfärdat medlet för elektronisk identifiering ska ha skadeståndsansvar för skada som åsamkats en fysisk eller juridisk person avsiktligt eller på grund av oaktsamhet genom underlåtenhet att uppfylla den skyldighet som avses i artikel 7 e vid en gränsöverskridande transaktion.

3. Den part som handhar autentiseringsförfarandet ska ha skadeståndsansvar för skada som åsamkats en fysisk eller juridisk person avsiktligt eller på grund av oaktsamhet genom underlåtenhet att säkerställa korrekt handhavande av den autentisering som avses i artikel 7 f vid en gränsöverskridande transaktion.

4. Punkterna 1, 2 och 3 ska tillämpas i enlighet med nationella bestämmelser om skadeståndsansvar.

5. Punkterna 1, 2 och 3 påverkar inte det skadeståndsansvar enligt nationell rätt som gäller för parter i en transaktion där de använda medlen för elektronisk identifiering omfattas av det system för elektronisk identifiering som anmälts i enlighet med artikel 9.1.

Artikel 12

Samarbete och interoperabilitet

1. De nationella system för elektronisk identifiering som anmälts i enlighet med artikel 9.1 ska vara interoperabla.

2. Med avseende på tillämpningen av punkt 1 ska ett interoperabilitetsramverk fastställas.

3. Interoperabilitetsramverket ska uppfylla följande kriterier:

a) Det ska ha som mål att vara teknikneutralt och ska inte diskriminera mellan särskilda nationella tekniska lösningar för elektronisk identifiering i en medlemsstat.

b) Det ska, när det är möjligt, följa europeiska och internationella standarder.

c) Det ska främja tillämpningen av principen om ett inbyggt integritetsskydd.

d) Det ska säkerställa att personuppgifter behandlas i enlighet med direktiv 95/46/EG.

4. Interoperabilitetsramverket ska bestå av följande:

a) Hänvisning till tekniska minimikrav avseende tillitsnivåerna i artikel 8.

b) Sammankoppling av nationella tillitsnivåer för anmälda system för elektronisk identifiering med tillitsnivåerna enligt artikel 8.

c) Hänvisning till tekniska minimikrav för interoperabilitet.

d) Hänvisning till en minimuppsättning personidentifieringsuppgifter som är unika för en fysisk eller juridisk person och som är tillgänglig via system för elektronisk identifiering.

e) Förfaranderegler.

f) Arrangemang för tvistlösning.

g) Gemensamma standarder för driftsäkerhet.

5. Medlemsstaterna ska samarbeta med avseende på följande:

a) Interoperabiliteten i de system för elektronisk identifiering som anmälts enligt artikel 9.1 och de system för elektronisk identifiering som medlemsstaterna avser att anmäla.

b) Säkerheten i systemen för elektronisk identifiering.

6. Samarbetet mellan medlemsstaterna ska bestå av följande:

a) Utbyte av information, erfarenhet och god praxis när det gäller system för elektronisk identifiering och särskilt i fråga om tekniska krav avseende interoperabilitet och tillitsnivåer.

b) Utbyte av information, erfarenheter och god praxis när det gäller arbete med tillitsnivåer för system för elektronisk identifiering enligt artikel 8.

c) Sakkunnigbedömning av system för elektronisk identifiering som omfattas av denna förordning.

d) Bedömning av relevant utveckling inom sektorn för elektronisk identifiering.

7. Senast den 18 mars 2015 ska kommissionen genom genomförandeakter fastställa nödvändiga förfaranden för att underlätta det samarbete mellan medlemsstaterna som avses i punkterna 5 och 6 i syfte att främja en hög nivå av förtroende och säkerhet som står i proportion till risknivån.

8. Senast den 18 september 2015 ska kommissionen, i enlighet med de kriterier som fastställs i punkt 3 och med beaktande av resultaten av samarbetet mellan medlemsstaterna, för att fastställa enhetliga villkor för tillämpningen av kraven i punkt 1 anta genomförandeakter om det interoperabilitetsramverk som anges i punkt 4.

9. De genomförandeakter som avses i punkterna 7 och 8 i denna artikel ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

KAPITEL III

BETRODDA TJÄNSTER

AVSNITT 1

Allmänna bestämmelser

Artikel 13

Skadeståndsansvar och bevisbörda

1. Utan att det påverkar tillämpningen av punkt 2 ska tillhandahållare av betrodda tjänster ha skadeståndsansvar för skada som åsamkats en fysisk eller juridisk person avsiktligt eller på grund av oaktsamhet genom underlåtenhet att uppfylla kraven i denna förordning.

Bevisbördan för avsikt eller oaktsamhet hos en icke-kvalificerad tillhandahållare av betrodda tjänster ska vila på den fysiska eller juridiska person som gör gällande sådan skada som avses i första stycket.

Avsikt eller oaktsamhet hos en kvalificerad tillhandahållare av betrodda tjänster ska anses föreligga såvida inte en kvalificerad tillhandahållare av betrodda tjänster bevisar att den skada som avses i första stycket har uppstått utan avsikt eller oaktsamhet hos den kvalificerade tillhandahållaren av betrodda tjänster.

2. Om en tillhandahållare av betrodda tjänster vederbörligen informerar sina kunder i förväg om de begränsningar som gäller för användningen av de tjänster de tillhandahåller och dessa begränsningar är möjliga för tredje man att ta del av, ska tillhandahållarna av betrodda tjänster inte ha skadeståndsansvar för skador som uppstår vid sådan användning av tjänster som överskrider de angivna begränsningarna.

3. Punkterna 1 och 2 ska tillämpas i enlighet med nationella bestämmelser om skadeståndsansvar.

Artikel 14

Internationella aspekter

1. Betrodda tjänster som tillhandahålls av tillhandahållare av betrodda tjänster som är etablerade i ett tredjeland ska erkännas som rättsligt likvärdiga med kvalificerade betrodda tjänster som tillhandahålls av kvalificerade tillhandahållare av betrodda tjänster som är etablerade inom unionen, under förutsättning att de betrodda tjänsterna från tredjelandet är erkända enligt ett avtal som ingåtts mellan unionen och det berörda tredjelandet eller en internationell organisation i enlighet med artikel 218 i EUF-fördraget.

2. Avtal som avses i punkt 1 ska särskilt säkerställa att

a) de krav som är tillämpliga på kvalificerade tillhandahållare av betrodda tjänster som är etablerade inom unionen och de kvalificerade betrodda tjänster som de tillhandahåller uppfylls av tillhandahållarna av betrodda tjänster i det tredjeland eller den internationella organisation med vilket eller vilken avtalet ingås och av de betrodda tjänster som de tillhandahåller,

b) de kvalificerade betrodda tjänster som tillhandahålls av kvalificerade tillhandahållare av betrodda tjänster som är etablerade inom unionen erkänns som rättsligt likvärdiga med betrodda tjänster som tillhandahålls av tillhandahållare av betrodda tjänster i det tredjeland eller den internationella organisation med vilket eller vilken avtalet ingås.

Artikel 15

Tillgänglighet för personer med funktionshinder

När det är genomförbart ska betrodda tjänster som tillhandahålls och slutanvändarprodukter som används i samband med tillhandahållandet av dessa tjänster göras tillgängliga för personer med funktionshinder.

Artikel 16

Sanktioner

Medlemsstaterna ska fastställa bestämmelser om de sanktioner som ska tillämpas vid överträdelser av denna förordning. Sanktionerna ska vara effektiva, proportionella och avskräckande.

AVSNITT 2

Tillsyn

Artikel 17

Tillsynsorgan

1. Medlemsstaterna ska utse ett tillsynsorgan som är etablerat inom deras territorium eller, efter ömsesidig överenskommelse med en annan medlemsstat, ett tillsynsorgan som är etablerat i den andra medlemsstaten. Det organet ska ansvara för tillsynsuppgifter i den medlemsstat som utsett organet.

Tillsynsorgan ska tilldelas nödvändiga befogenheter och adekvata resurser för utövande av sina uppgifter.

2. Medlemsstaterna ska meddela kommissionen namn på och adress till sina respektive utsedda tillsynsorgan.

3. Tillsynsorganet ska ha följande roll:

a) Utöva tillsyn över kvalificerade tillhandahållare av betrodda tjänster som är etablerade i den medlemsstat där de har utsetts för att genom tillsynsverksamhet på förhand och i efterhand se till att de kvalificerade tillhandahållarna av betrodda tjänster och de kvalificerade betrodda tjänster som de tillhandahåller uppfyller kraven i denna förordning.

b) Vid behov vidta åtgärder avseende icke-kvalificerade tillhandahållare av betrodda tjänster som är etablerade i den medlemsstat där de har utsetts genom tillsynsverksamhet i efterhand om de tar del av påståenden att dessa icke-kvalificerade tillhandahållare av betrodda tjänster eller de betrodda tjänster som de tillhandahåller inte uppfyller kraven i denna förordning.

4. Vid tillämpningen av punkt 3 och med förbehåll för de begränsningar som anges däri ska tillsynsorganets uppgifter särskilt innefatta följande:

a) Samarbete med andra tillsynsorgan och bistånd till dem i enlighet med artikel 18.

b) Analys av de rapporter om överensstämmelsebedömning som avses i artiklarna 20.1 och 21.1.

c) Information till andra tillsynsorgan samt allmänheten om säkerhetsincidenter eller integritetsförluster i enlighet med artikel 19.2.

d) Rapportering till kommissionen om sin huvudverksamhet i enlighet med punkt 6 i denna artikel.

e) Granskningsverksamhet eller framställningar till ett organ för bedömning av överensstämmelse om att detta ska göra en överensstämmelsebedömning av kvalificerade tillhandahållare av betrodda tjänster i enlighet med artikel 20.2.

f) Samarbete med dataskyddsmyndigheterna, främst genom att utan onödigt dröjsmål informera dem om resultatet av granskningar av kvalificerade tillhandahållare av betrodda tjänster, när det förefaller ha skett en överträdelse av reglerna för skydd för personuppgifter.

g) Beviljande av status som kvalificerad tillhandahållare av betrodda tjänster och till de tjänster som de tillhandahåller samt återkallande av denna status i enlighet med artiklarna 20 och 21.

h) Information till det organ som är ansvarigt för den nationella förteckning över betrodda tjänsteleverantörer som avses i artikel 22.3 om sina beslut om beviljande eller återkallande av status som kvalificerad, såvida inte det organet även är tillsynsorganet.

i) Kontroll av befintlighet och korrekt tillämpning av bestämmelser om planer för verksamhetens upphörande i sådana fall när den kvalificerade tillhandahållaren av betrodda tjänster upphör med sin verksamhet, inbegripet hur information hålls tillgänglig i enlighet med artikel 24.2 h.

j) Åläggande av krav på tillhandahållare av betrodda tjänster att åtgärda varje underlåtenhet att uppfylla kraven i denna förordning.

5. Medlemsstaterna får kräva att tillsynsorganet ska inrätta, underhålla och uppdatera en infrastruktur för betrodda tjänster i enlighet med villkoren i nationell rätt.

6. Senast den 31 mars varje år ska varje tillsynsorgan till kommissionen överlämna en rapport om det föregående kalenderårets huvudverksamhet tillsammans med en sammanfattning av överträdelseanmälningar som har inkommit från tillhandahållare av betrodda tjänster i enlighet med artikel 19.2.

7. Kommissionen ska göra den årsrapport som avses i punkt 6 tillgänglig för medlemsstaterna.

8. Kommissionen får genom genomförandeakter fastställa format och förfaranden för den rapport som avses i punkt 6. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

Artikel 18

Ömsesidigt bistånd

1. Tillsynsorganen ska samarbeta med sikte på att utbyta god praxis.

Ett tillsynsorgan ska, efter att ha mottagit en motiverad begäran från ett annat tillsynsorgan, ge det organet bistånd så att deras åtgärder kan vidtas på ett enhetligt sätt. Det ömsesidiga biståndet kan bland annat omfatta begäranden om information och tillsynsåtgärder, t.ex. begäranden om att utföra inspektioner avseende de rapporter om överensstämmelsebedömning som avses i artiklarna 20 och 21.

2. Ett tillsynsorgan som tar emot en begäran om bistånd får vägra att tillmötesgå denna begäran på grundval av något av följande skäl:

a) Tillsynsorganet är inte behörigt att tillhandahålla det bistånd som begärs.

b) Det begärda biståndet står inte i proportion till den tillsynsverksamhet som tillsynsorganet utför i enlighet med artikel 17.

c) Det skulle stå i strid med denna förordning att tillhandahålla det begärda biståndet.

3. Där så är lämpligt får medlemsstaterna bemyndiga sina respektive tillsynsorgan att vidta gemensamma åtgärder där personal från andra medlemsstaters tillsynsorgan deltar. De berörda medlemsstaterna ska besluta om och inrätta arrangemangen och förfarandena för sådana gemensamma åtgärder i enlighet med sin nationella rätt.

Artikel 19

Säkerhetskrav på tillhandahållare av betrodda tjänster

1. Kvalificerade och icke kvalificerade tillhandahållare av betrodda tjänster ska vidta lämpliga tekniska och organisatoriska åtgärder för att hantera riskerna för säkerheten hos de betrodda tjänster som de tillhandahåller. Med beaktande av den senaste tekniska utvecklingen ska dessa åtgärder säkerställa att säkerhetsnivån står i proportion till graden av risk. I synnerhet ska åtgärder vidtas för att förhindra eller minimera säkerhetsincidenters inverkan samt för att informera berörda parter om de negativa effekterna av eventuella sådana incidenter.

2. Kvalificerade och icke kvalificerade tillhandahållare av betrodda tjänster ska, utan otillbörligt dröjsmål och under alla omständigheter inom 24 timmar efter upptäckt, underrätta tillsynsorganet och i förekommande fall andra relevanta organ, såsom det behöriga nationella organet för informationssäkerhet eller dataskyddsmyndigheten, om alla säkerhetsincidenter eller integritetsförluster som i betydande omfattning påverkar den betrodda tjänst som tillhandahålls eller på de personuppgifter som ingår i denna.

När det är troligt att säkerhetsincidenten eller integritetsförlusten kommer att ha negativ inverkan på en fysisk eller juridisk person till vilken den betrodda tjänsten har tillhandahållits, ska tillhandahållaren av betrodda tjänster utan onödigt dröjsmål även underrätta den fysiska eller juridiska personen om säkerhetsincidenten eller integritetsförlusten.

När så är lämpligt, särskilt om säkerhetsincidenten eller integritetsförlusten rör två eller flera medlemsstater, ska det underrättade tillsynsorganet informera tillsynsorganen i övriga berörda medlemsstater samt Enisa.

Det underrättade tillsynsorganet ska informera allmänheten eller kräva att tillhandahållaren av betrodda tjänster gör det, om den slår fast att ett avslöjande av säkerhetsincidenten eller integritetsförlusten ligger i allmänhetens intresse.

3. Tillsynsorganet ska en gång om året till Enisa överlämna en sammanfattning av de anmälningar om säkerhetsincidenter eller som inkommit från tillhandahållare av betrodda tjänster.

4. Kommissionen får, genom genomförandeakter,

a) ytterligare specificera de åtgärder som avses i punkt 1, och

b) fastställa format och förfaranden, inklusive tidsfrister, som ska vara tillämpliga för de ändamål som avses i punkt 2.

Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

AVSNITT 3

Kvalificerade betrodda tjänster

Artikel 20

Tillsyn över kvalificerade tillhandahållare av betrodda tjänster

1. Kvalificerade tillhandahållare av betrodda tjänster ska minst en gång vartannat år och på egen bekostnad granskas av ett organ för bedömning av överensstämmelse. Syftet med denna granskning ska vara att bekräfta att de kvalificerade tillhandahållarna av betrodda tjänster och de kvalificerade betrodda tjänster som de tillhandahåller uppfyller kraven i denna förordning. De kvalificerade tillhandahållarna av betrodda tjänster ska lämna in den resulterande rapporten om överensstämmelsebedömning till tillsynsorganet inom en period av tre arbetsdagar efter mottagande av denna.

2. Tillsynsorganet får, utan att det påverkar tillämpningen av punkt 1, när som helst granska eller begära att ett organ för bedömning av överensstämmelse gör en överensstämmelsebedömning av de kvalificerade tillhandahållarna av betrodda tjänster på dessa tillhandahållare av betrodda tjänsters egen bekostnad för att bekräfta att dessa och de kvalificerade betrodda tjänster som de tillhandahåller uppfyller kraven i denna förordning. Vid misstänkta överträdelser av reglerna om skydd för personuppgifter ska tillsynsorganet informera dataskyddsmyndigheterna om sina granskningsresultat.

3. När tillsynsorganet begär att den kvalificerade tillhandahållaren av betrodda tjänster ska åtgärda en underlåtenhet att uppfylla kraven i denna förordning och när tillhandahållaren inte gör detta, och i tillämpliga fall inom den tidsfrist som fastställts av tillsynsorganet, får tillsynsorganet med beaktande av i synnerhet underlåtenhetens omfattning, varaktighet och följder återkalla den tillhandahållarens eller den berörda tillhandahållna tjänstens status som kvalificerad samt informera det organ som avses i artikel 22.3 för att de förteckningar över betrodda tjänsteleverantörer som avses i artikel 22.1 ska kunna uppdateras. Tillsynsorganet ska informera den kvalificerade tillhandahållaren av betrodda tjänster om återkallandet av dess eller den berörda tjänstens status som kvalificerad.

4. Kommissionen får genom genomförandeakter fastställa referensnummer till följande standarder:

a) Ackreditering av organ för bedömning av överensstämmelse och för den rapport om överensstämmelsebedömning som avses i punkt 1.

b) Granskningsregler som organen för bedömning av överensstämmelse ska följa vid sina överensstämmelsebedömningar av kvalificerade tillhandahållare av betrodda tjänster som avses i punkt 1.

Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

Artikel 21

Igångsättande av en kvalificerad betrodd tjänst

1. När tillhandahållare av betrodda tjänster som inte har status som kvalificerade har för avsikt att börja tillhandahålla kvalificerade betrodda tjänster, ska de anmäla sin avsikt till tillsynsorganet och samtidigt lämna in en rapport om överensstämmelsebedömning som utfärdats av ett organ för bedömning av överensstämmelse.

2. Tillsynsorganet ska kontrollera huruvida tillhandahållaren av betrodda tjänster och de betrodda tjänster som denne tillhandahåller uppfyller kraven i denna förordning, och i synnerhet kraven för kvalificerade tillhandahållare av betrodda tjänster och för de kvalificerade betrodda tjänster som de tillhandahåller.

Om tillsynsorganet kommer fram till att tillhandahållaren av betrodda tjänster och de betrodda tjänster som denne tillhandahåller uppfyller de krav som avses i första stycket, ska det bevilja status som kvalificerad till tillhandahållare av betrodda tjänster och de betrodda tjänster som denne tillhandahåller samt informera det organ som avses i artikel 22.3 för att de förteckningar över betrodda tjänsteleverantörer som avses i artikel 22.1 ska kunna uppdateras, senast tre månader efter anmälan i enlighet med punkt 1 i denna artikel.

Om kontrollen inte har slutförts inom tre månader från anmälan, ska tillsynsorganet informera tillhandahållaren av betrodda tjänster om detta och ange orsakerna till förseningen samt när kontrollen beräknas vara slutförd.

3. Kvalificerade tillhandahållare av betrodda tjänster får börja tillhandahålla den kvalificerade betrodda tjänsten efter det att status som kvalificerad har angetts i de förteckningar över betrodda tjänsteleverantörer som avses i artikel 22.1.

4. Kommissionen får genom genomförandeakter fastställa format och förfaranden för de ändamål som avses i punkterna 1 och 2. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

Artikel 22

Förteckningar över betrodda tjänsteleverantörer

1. Varje medlemsstat ska upprätta, underhålla och offentliggöra förteckningar med uppgifter om kvalificerade tillhandahållare av betrodda tjänster som den ansvarar för, tillsammans med uppgifter om de kvalificerade betrodda tjänster som dessa tillhandahåller.

2. Medlemsstaterna ska på ett säkert sätt upprätta, underhålla och offentliggöra elektroniskt undertecknade eller förseglade förteckningar som avses i punkt 1 i en form som lämpar sig för automatiserad behandling.

3. Medlemsstaterna ska utan onödigt dröjsmål till kommissionen lämna information om det organ som ansvarar för att upprätta, underhålla och offentliggöra nationella förteckningar över betrodda tjänsteleverantörer, samt närmare uppgifter om var dessa förteckningar offentliggörs, de certifikat som används för att underteckna eller försegla förteckningarna över betrodda tjänsteleverantörer och eventuella ändringar i dem.

4. Kommissionen ska se till att den information som avses i punkt 3 genom en säker kanal görs tillgänglig för allmänheten i elektroniskt undertecknad eller förseglad form som lämpar sig för automatiserad behandling.

5. Senast den 18 september 2015 ska kommissionen genom genomförandeakter ange den information som avses i punkt 1 och fastställa de tekniska specifikationer och format som ska gälla för förteckningar över betrodda tjänsteleverantörer för de ändamål som avses i punkterna 1–4. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

Artikel 23

EU-förtroendemärke för kvalificerade betrodda tjänster

1. Efter det att den kvalificerade status som avses i artikel 21.2 andra stycket har angetts i den förteckning över betrodda tjänsteleverantörer som avses i artikel 22.1, får kvalificerade tillhandahållare av betrodda tjänster använda sig av EU-förtroendemärket för att på ett enkelt, igenkännligt och tydligt sätt ange de kvalificerade betrodda tjänster som de tillhandahåller.

2. Vid användning av det EU-förtroendemärke som avses i punkt 1 ska kvalificerade tillhandahållare av betrodda tjänster se till att en länk till den relevanta förteckningen över betrodda tjänsteleverantörer finns på deras webbplats.

3. Senast den 1 juli 2015 ska kommissionen genom genomförandeakter fastställa specifikationer med avseende på formatet för EU-förtroendemärket för kvalificerade betrodda tjänster och särskilt för dess presentation, sammansättning, storlek och utformning. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

Artikel 24

Krav på kvalificerade tillhandahållare av betrodda tjänster

1. En kvalificerad tillhandahållare av betrodda tjänster ska, när den utfärdar ett kvalificerat certifikat för en betrodd tjänst, på lämpligt sätt och i enlighet med nationell rätt kontrollera identiteten och i förekommande fall eventuella särskilda attribut för den fysiska eller juridiska person till vilken det kvalificerade certifikatet utfärdas.

Den information som avses i första stycket ska kontrolleras av den kvalificerade tillhandahållaren av betrodda tjänster antingen direkt eller via tredje man i enlighet med nationell rätt på något av följande sätt:

a) Genom fysisk närvaro av den fysiska personen eller av en behörig företrädare för den juridiska personen.

b) På distans, med hjälp av medel för elektronisk identifiering, där en fysisk närvaro av den fysiska personen eller en behörig företrädare för den juridiska personen vid tidpunkt före utfärdandet av det kvalificerade certifikatet säkerställs och som uppfyller kraven i artikel 8 när det gäller tillitsnivåerna väsentlig eller hög.

c) Genom ett certifikat för en kvalificerad elektronisk underskrift eller en kvalificerad elektronisk stämpel som utfärdats i enlighet med led a eller b.

d) Med hjälp av andra identifieringsmetoder som erkänns på nationell nivå och som erbjuder garantier som är likvärdiga med fysisk närvaro. Likvärdiga garantier ska bekräftas av ett organ för bedömning av överensstämmelse.

2. En kvalificerad tillhandahållare av betrodda tjänster som tillhandahåller kvalificerade betrodda tjänster ska

a) informera tillsynsorganet om alla ändringar av tillhandahållandet av dess kvalificerade betrodda tjänster, och om den har för avsikt att upphöra med denna verksamhet,

b) ha personal, och i förekommande fall underleverantörer, som har den sakkunskap, den tillförlitlighet samt de erfarenheter och kvalifikationer som behövs och som har genomgått lämplig utbildning om regler för säkerhet och skydd för personuppgifter och ska tillämpa förfaranden för administration och förvaltning som överensstämmer med europeiska eller internationella standarder,

c) när det gäller risken för ansvar vid skador i enlighet med artikel 13 förfoga över tillräckliga ekonomiska medel och/eller skaffa sig lämplig ansvarsförsäkring i enlighet med nationell rätt,

d) innan den ingår ett avtalsförhållande på ett tydligt och uttömmande sätt informera de personer som vill använda en kvalificerad betrodd tjänst om de exakta villkor som gäller för användning av den tjänsten, inbegripet om eventuella begränsningar av användningen,

e) använda tillförlitliga system och produkter som är skyddade mot ändringar och säkerställa den tekniska säkerheten och tillförlitligheten hos den process som stöds av dessa,

f) använda tillförlitliga system för att lagra uppgifter som har lämnats till den, i en form som kan kontrolleras så att

i) de är offentligt tillgängliga för hämtning endast i de fall där samtycke från den person som uppgifterna rör har erhållits,

ii) endast behöriga personer kan föra in uppgifter och göra ändringar i de lagrade uppgifterna, och

iii) uppgifternas äkthet kan kontrolleras,

g) vidta lämpliga åtgärder mot förfalskning och stöld av uppgifter,

h) under en lämplig tidsperiod registrera och hålla tillgänglig, även efter det att den kvalificerade tillhandahållaren av betrodda uppgifter har upphört med sin verksamhet, all relevant information om uppgifter som den kvalificerade tillhandahållaren av betrodda tjänster har utfärdat och tagit emot, särskilt för att vid rättsliga förfaranden kunna lägga fram bevis och för att säkerställa tjänstens kontinuitet; registreringen får göras elektroniskt,

i) ha en uppdaterad plan för verksamhetens upphörande i syfte att säkerställa tjänstens kontinuitet i enlighet med bestämmelser som kontrollerats av tillsynsorganet i enlighet med artikel 17.4 i,

j) säkerställa laglig behandling av personuppgifter i enlighet med direktiv 95/46/EG,

k) då det är fråga om kvalificerade tillhandahållare av betrodda tjänster som utfärdar kvalificerade certifikat, upprätta och uppdatera en certifikatdatabas,

3. Om en kvalificerad tillhandahållare av betrodda tjänster som utfärdar kvalificerade certifikat beslutar att återkalla ett certifikat, ska den registrera ett sådant återkallande i sin certifikatdatabas och offentliggöra återkallandet av statusen för certifikatet i god tid och i alla händelser inom 24 timmar efter mottagandet av begäran. Återkallandet ska få verkan omedelbart efter offentliggörandet.

4. Med avseende på punkt 3 ska kvalificerade tillhandahållare av betrodda tjänster som utfärdar kvalificerade certifikat informera eventuella förlitande parter om giltigheten eller statusen som återkallad hos de kvalificerade certifikat som de utfärdat. Informationen ska, åtminstone på certifikatnivå, när som helst och utöver certifikatets giltighetsperiod göras tillgängligt på ett automatiskt sätt som är tillförlitligt, kostnadsfritt och effektivt.

5. Kommissionen får genom genomförandeakter fastställa referensnummer till standarder för tillförlitliga system och produkter, vilka uppfyller kraven i punkt 2 e och f i denna artikel. Överensstämmelse med kraven i denna artikel ska förutsättas när tillförlitliga system och produkter uppfyller dessa standarder. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

AVSNITT 4

Elektroniska underskrifter

Artikel 25

Rättslig verkan av elektroniska underskrifter

1. En elektronisk underskrift får inte förvägras rättslig verkan eller giltighet som bevis vid rättsliga förfaranden enbart på grund av att underskriften har elektronisk form eller inte uppfyller kraven för kvalificerade elektroniska underskrifter.

2. En kvalificerad elektronisk underskrift ska ha motsvarande rättsliga verkan som en handskriven underskrift.

3. En kvalificerad elektronisk underskrift som är baserad på ett kvalificerat certifikat som utfärdats i en medlemsstat ska erkännas som en kvalificerad elektronisk underskrift i alla andra medlemsstater.

Artikel 26

Krav med avseende på avancerade elektroniska underskrifter

En avancerad elektronisk underskrift ska uppfylla följande krav:

a) Den ska vara unikt knuten till undertecknaren.

b) Undertecknaren ska kunna identifieras genom den.

c) Den ska vara skapad på grundval av uppgifter för skapande av elektroniska underskrifter som undertecknaren med hög grad av tillförlitlighet kan använda uteslutande under sin egen kontroll.

d) Den ska vara kopplad till de uppgifter som den används för att underteckna på ett sådant sätt att alla efterföljande ändringar av uppgifterna kan upptäckas.

Artikel 27

Elektroniska underskrifter i offentliga tjänster

1. Om en medlemsstat kräver en avancerad elektronisk underskrift för användningen av en nättjänst som erbjuds av ett offentligt organ eller på ett offentligt organs vägnar, ska medlemsstaten erkänna avancerade elektroniska underskrifter, avancerade elektroniska underskrifter som är baserade på ett kvalificerat certifikat för elektroniska underskrifter och kvalificerade elektroniska underskrifter i åtminstone de format eller med de metoder som anges i de genomförandeakter som avses i punkt 5.

2. Om en medlemsstat kräver en avancerad elektronisk underskrift som är baserad på ett kvalificerat certifikat för användningen av en nättjänst som erbjuds av ett offentligt organ eller på ett offentligt organs vägnar, ska medlemsstaten erkänna avancerade elektroniska underskrifter som är baserade på ett kvalificerat certifikat och kvalificerade elektroniska underskrifter i åtminstone de format eller med de metoder som anges i de genomförandeakter som avses i punkt 5.

3. Medlemsstaterna ska för gränsöverskridande användning av nättjänster som erbjuds av ett offentligt organ inte kräva en elektronisk underskrift med en högre säkerhetsnivå än den som gäller för kvalificerade elektroniska underskrifter.

4. Kommissionen får genom genomförandeakter fastställa referensnummer till standarder för avancerade elektroniska underskrifter. Överensstämmelse med de krav på avancerade elektroniska underskrifter som avses i punkterna 1 och 2 i denna artikel samt i artikel 26 ska förutsättas när en avancerad elektronisk underskrift uppfyller dessa standarder. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

5. Kommissionen ska senast den 18 september 2015 och med beaktande av befintliga rutiner, standarder och unionsrättsakter, genom genomförandeakter, fastställa referensformat för avancerade elektroniska underskrifter eller referensmetoder i de fall alternativa format används. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

Artikel 28

Kvalificerade certifikat för elektroniska underskrifter

1. Kvalificerade certifikat för elektroniska underskrifter ska uppfylla kraven i bilaga I.

2. Kvalificerade certifikat för elektroniska underskrifter ska inte omfattas av några obligatoriska krav som går utöver kraven i bilaga I.

3. Kvalificerade certifikat för elektroniska underskrifter får omfatta extra, icke-obligatoriska, särskilda attribut. Dessa attribut ska inte påverka kvalificerade elektroniska underskrifters kompatibilitet eller erkännande.

4. Om ett kvalificerat certifikat för elektroniska underskrifter har återkallats efter den ursprungliga aktiveringen, ska det förlora sin giltighet från och med tidpunkten för återkallandet, och dess status som giltigt ska inte under några omständigheter återgå.

5. På följande villkor får medlemsstaterna fastställa nationella bestämmelser för tillfälligt upphävande av ett kvalificerat certifikat för elektroniska underskrifter:

a) Om ett kvalificerat certifikat för en elektronisk underskrift tillfälligt har upphävts, ska certifikatet vara ogiltigt under tiden för det tillfälliga upphävandet.

b) Perioden för det tillfälliga upphävandet ska tydligt anges i certifikatdatabasen och certifikatets status som tillfälligt upphävt ska under perioden för det tillfälliga upphävandet vara synlig genom den tjänst som tillhandahåller information om certifikatets status.

6. Kommissionen får genom genomförandeakter fastställa referensnummer till standarder för kvalificerade certifikat för elektroniska underskrifter. Överensstämmelse med kraven i bilaga I ska förutsättas när ett kvalificerat certifikat för elektroniska underskrifter uppfyller dessa standarder. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

Artikel 29

Krav på anordningar för skapande av kvalificerade elektroniska underskrifter

1. Anordningar för skapande av kvalificerade elektroniska underskrifter ska uppfylla kraven i bilaga II.

2. Kommissionen får genom genomförandeakter fastställa referensnummer till standarder för anordningar för skapande av kvalificerade elektroniska underskrifter. Överensstämmelse med kraven i bilaga II ska förutsättas när en anordning för skapande av kvalificerade elektroniska underskrifter uppfyller dessa standarder. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

Artikel 30

Certifiering av anordningar för skapande av kvalificerade elektroniska underskrifter

1. Lämpliga offentliga eller privata organ som utsetts av medlemsstaterna ska certifiera att anordningar för skapande av kvalificerade elektroniska underskrifter överensstämmer med kraven i bilaga II.

2. Medlemsstaterna ska underrätta kommissionen om namnet på och adressen till det offentliga eller privata organ som avses i punkt 1. Kommissionen ska göra den informationen tillgänglig för medlemsstaterna.

3. Den certifiering som avses i punkt 1 ska bygga på något av följande:

a) Ett förfarande för säkerhetsutvärdering som utförts i enlighet med någon av de standarder för säkerhetsutvärdering av informationsteknikprodukter som finns med i den förteckning som fastställts i enlighet med andra stycket.

b) Ett annat förfarande än det som avses i led a, förutsatt att det omfattar jämförbara säkerhetsnivåer och att det offentliga eller privata organ som avses i punkt 1 underrättar kommissionen om förfarandet. Detta förfarande får endast användas vid avsaknad av sådana standarder som avses i led a eller medan en sådan säkerhetsutvärdering som avses i led a pågår.

Kommissionen ska genom genomförandeakter upprätta en förteckning över standarder för den säkerhetsbedömning av informationsteknikprodukter som avses i led a. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

4. Kommissionen ska ha befogenhet att anta delegerade akter i enlighet med artikel 47 rörande fastställandet av särskilda kriterier som ska uppfyllas av de utsedda organ som avses i punkt 1 i den här artikeln.

Artikel 31

Offentliggörande av en förteckning över certifierade anordningar för skapande av kvalificerade elektroniska underskrifter

1. Medlemsstaterna ska utan onödigt dröjsmål och senast en månad efter det att certifieringen slutförts till kommissionen lämna information om anordningar för skapande av kvalificerade elektroniska underskrifter som har certifierats av de organ som avses i artikel 30.1. De ska utan onödigt dröjsmål och senast en månad efter det att en certifiering har upphört att gälla även informera kommissionen om anordningar för skapande av elektroniska underskrifter som inte längre är certifierade.

2. Kommissionen ska på grundval av den information som inkommit upprätta, offentliggöra och underhålla en förteckning över certifierade anordningar för skapande av kvalificerade elektroniska underskrifter.

3. Kommissionen får genom genomförandeakter fastställa format och förfaranden som ska vara tillämpliga för de ändamål som avses i punkt 1. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

Artikel 32

Krav på validering av kvalificerade elektroniska underskrifter

1. Genom valideringsförfarandet för en kvalificerad elektronisk underskrift ska den kvalificerade elektroniska underskriftens giltighet bekräftas under förutsättning att

a) det certifikat som stöder underskriften vid tidpunkten för undertecknandet var ett kvalificerat certifikat för elektroniska underskrifter som överensstämmer med bilaga I,

b) det kvalificerade certifikatet har utfärdats av en kvalificerad tillhandahållare av betrodda tjänster och var giltigt vid tidpunkten för undertecknandet,

c) valideringsuppgifterna för underskriften överensstämmer med de uppgifter som lämnats till den förlitande parten,

d) certifikatets unika uppsättning uppgifter som avser undertecknaren har tillhandahållits den förlitande parten på rätt sätt,

e) användningen av en eventuell pseudonym tydligt har angetts för den förlitande parten om en pseudonym användes vid tidpunkten för undertecknandet,

f) den elektroniska underskriften har skapats med hjälp av en anordning för skapande av kvalificerade elektroniska underskrifter,

g) integriteten hos de undertecknade uppgifterna inte har äventyrats,

h) kraven i artikel 26 var uppfyllda vid tidpunkten för undertecknandet.

2. Det system som används för att validera den kvalificerade elektroniska underskriften ska ge den förlitande parten det korrekta resultatet av valideringsförfarandet och ska göra det möjligt för den förlitande parten att upptäcka eventuella problem som är relevanta för säkerheten.

3. Kommissionen får genom genomförandeakter fastställa referensnummer till standarder för validering av kvalificerade elektroniska underskrifter. Överensstämmelse med kraven i punkt 1 ska förutsättas när valideringen av kvalificerade elektroniska underskrifter uppfyller dessa standarder. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

Artikel 33

Kvalificerad valideringstjänst för kvalificerade elektroniska underskrifter

1. En kvalificerad valideringstjänst för kvalificerade elektroniska underskrifter får endast tillhandahållas av en kvalificerad tillhandahållare av betrodda tjänster som

a) tillhandahåller validering i enlighet med artikel 32.1, och

b) gör det möjligt för förlitande parter att erhålla resultaten av valideringsförfarandet på ett automatiskt sätt som är tillförlitligt, effektivt och försett med en avancerad elektronisk underskrift eller en avancerad elektronisk stämpel från tillhandahållaren av den kvalificerade valideringstjänsten.

2. Kommissionen får genom genomförandeakter fastställa referensnummer till standarder för den kvalificerade valideringstjänst som avses i punkt 1. Överensstämmelse med kraven i punkt 1 ska förutsättas när valideringstjänsten för kvalificerade elektroniska underskrifter uppfyller dessa standarder. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

Artikel 34

Kvalificerad tjänst för bevarande av kvalificerade elektroniska underskrifter

1. En kvalificerad tjänst för bevarande av kvalificerade elektroniska underskrifter får endast tillhandahållas av en kvalificerad tillhandahållare av betrodda tjänster som använder förfaranden och tekniker som gör det möjligt att förlänga den kvalificerade elektroniska underskriftens tillförlitlighet utöver perioden för teknisk giltighet.

2. Kommissionen får genom genomförandeakter fastställa referensnummer till standarder för kvalificerade tjänster för bevarande av kvalificerade elektroniska underskrifter. Överensstämmelse med kraven i punkt 1 ska förutsättas när systemen för de kvalificerade tjänsterna för bevarande av kvalificerade elektroniska underskrifter uppfyller dessa standarder. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

AVSNITT 5

Elektroniska stämplar

Artikel 35

Rättslig verkan av elektroniska stämplar

1. En elektronisk stämpel får inte förvägras rättslig verkan eller giltighet som bevis vid rättsliga förfaranden enbart på grund av att det har elektronisk form eller att det inte uppfyller kraven för kvalificerade elektroniska stämplar.

2. En kvalificerad elektronisk stämpel ska omfattas av en presumtion om integritet hos de uppgifter som den kvalificerade elektroniska stämpeln är kopplad till och om att de har korrekt ursprung.

3. En kvalificerad elektronisk stämpel som är baserat på ett kvalificerat certifikat som har utfärdats i en medlemsstat ska erkännas som en kvalificerad elektronisk stämpel i alla andra medlemsstater.

Artikel 36

Krav med avseende på avancerade elektroniska stämplar

En elektronisk stämpel ska uppfylla följande krav:

a) Den ska vara knuten uteslutande till skaparen av stämpeln.

b) Skaparen av stämpeln ska kunna identifieras genom det.

c) Det ska vara skapat på grundval av uppgifter för skapande av elektroniska stämplar som stämpelns skapare med hög grad av tillförlitlighet under sin kontroll kan använda för skapande av elektroniska stämplar.

d) Den ska vara kopplad till de uppgifter den avser på ett sådant sätt att alla efterföljande ändringar av uppgifterna kan upptäckas.

Artikel 37

Elektroniska stämplar i offentliga tjänster

1. Om en medlemsstat kräver en avancerad elektronisk stämpel för användningen av en nättjänst som erbjuds av ett offentligt organ eller för organets räkning ska medlemsstaten erkänna avancerade elektroniska stämplar, avancerade elektroniska stämplar som är baserade på ett kvalificerat certifikat för elektroniska stämplar och kvalificerade elektroniska stämplar i åtminstone de format eller med användning av de metoder som anges i de genomförandeakter som avses i punkt 5.

2. Om en medlemsstat kräver en avancerad elektronisk stämpel som är baserad på ett kvalificerat certifikat för användningen av en nättjänst som erbjuds av ett offentligt organ eller för organets räkning, ska medlemsstaten erkänna avancerade elektroniska stämplar som är baserade på ett kvalificerat certifikat och kvalificerade elektroniska stämplar i åtminstone de format eller med användning av de metoder som anges i de genomförandeakter som avses i punkt 5.

3. Medlemsstaterna ska för gränsöverskridande användning av en nättjänst som erbjuds av ett offentligt organ inte kräva en elektronisk stämpel på en högre säkerhetsnivå än den som gäller för den kvalificerade elektroniska stämpeln.

4. Kommissionen får genom genomförandeakter fastställa referensnummer till standarder för avancerade elektroniska stämplar. Överensstämmelse med de krav på avancerade elektroniska stämplar som avses i punkterna 1 och 2 i denna artikel samt i artikel 36 ska förutsättas när en avancerad elektronisk stämpel uppfyller dessa standarder. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

5. Kommissionen ska senast den 18 september 2015, och med beaktande av befintliga rutiner, standarder och unionsrättsakter genom genomförandeakter fastställa referensformat för avancerade elektroniska stämplar eller referensmetoder i de fall alternativa format används. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

Artikel 38

Kvalificerade certifikat för elektroniska stämplar

1. Kvalificerade certifikat för elektroniska stämplar ska uppfylla kraven i bilaga III.

2. Kvalificerade certifikat för elektroniska stämplar ska inte omfattas av några obligatoriska krav som går utöver kraven i bilaga III.

3. Kvalificerade certifikat för elektroniska stämplar får omfatta extra, icke-obligatoriska, särskilda attribut. Dessa attribut ska inte påverka kvalificerade elektroniska stämplars interoperabilitet eller erkännande.

4. Om ett kvalificerat certifikat för en elektronisk stämpel har återkallats efter den ursprungliga aktiveringen ska det förlora sin giltighet från och med tidpunkten för återkallandet och dess status ska inte under några omständigheter återgå.

5. På följande villkor får medlemsstaterna fastställa nationella bestämmelser för tillfälligt upphävande av kvalificerade certifikat för elektroniska stämplar:

a) Om ett kvalificerat certifikat för elektroniska stämplar tillfälligt har upphävts ska certifikatet vara ogiltigt under perioden för det tillfälliga upphävandet.

b) Perioden för det tillfälliga upphävandet ska tydligt anges i certifikatdatabasen och certifikatets status som tillfälligt upphävt ska under perioden för det tillfälliga upphävandet vara synlig genom den tjänst som tillhandahåller information om certifikatets status.

6. Kommissionen får genom genomförandeakter fastställa referensnummer till standarder för kvalificerade certifikat för elektroniska stämplar. Överensstämmelse med kraven i bilaga III ska förutsättas när ett kvalificerat certifikat för elektroniska stämplar uppfyller dessa standarder. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

Artikel 39

Kvalificerade anordningar för skapande av elektroniska stämplar

1. Artikel 29 ska på motsvarande sätt gälla för kraven på kvalificerade anordningar för skapande av elektroniska stämplar.

2. Artikel 30 ska på motsvarande sätt gälla för certifieringen av kvalificerade anordningar för skapande av elektroniska stämplar.

3. Artikel 31 ska på motsvarande sätt gälla för offentliggörandet av en förteckning över certifierade kvalificerade anordningar för skapande av elektroniska stämplar.

Artikel 40

Validering och bevarande av kvalificerade elektroniska stämplar

Artiklarna 32, 33 och 34 ska på motsvarande sätt gälla för validering och bevarande av kvalificerade elektroniska stämplar.

AVSNITT 6

Elektroniska tidsstämplingar

Artikel 41

Rättslig verkan av elektroniska tidsstämplingar

1. En elektronisk tidsstämpling ska inte förvägras rättslig verkan eller giltighet som bevis vid rättsliga förfaranden enbart på grund av att den har elektronisk form eller inte uppfyller kraven för en kvalificerad elektronisk tidsstämpling.

2. En kvalificerad elektronisk tidsstämpling ska omfattas av en presumtion om korrekthet hos det datum och den tid som den anger och integritet hos de uppgifter som datumet och tiden är kopplade till.

3. En kvalificerad elektronisk tidsstämpling som utfärdats i en medlemsstat ska erkännas som en kvalificerad elektronisk tidsstämpling i alla medlemsstater.

Artikel 42

Krav på kvalificerade elektroniska tidsstämplingar

1. En kvalificerad elektronisk tidsstämpling ska uppfylla följande krav:

a) Den ska binda datumet och tiden till uppgifter så att möjligheten att uppgifterna ändras utan att det går att upptäcka rimligtvis kan uteslutas.

b) Den ska vara grundad på en korrekt tidskälla som är kopplad till samordnad universaltid.

c) Den ska vara undertecknad med hjälp av en avancerad elektronisk underskrift eller förseglad med en avancerad elektronisk stämpel från den kvalificerade tillhandahållaren av betrodda tjänster eller genom en likvärdig metod.

2. Kommissionen får genom genomförandeakter fastställa referensnummer till standarder för bindning av datum och tidpunkt till uppgifter och för korrekta tidskällor. Överensstämmelse med kraven i punkt 1 ska förutsättas när bindningen av datum och tidpunkt till uppgifter och den korrekta tidskällan uppfyller dessa standarder. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

AVSNITT 7

Elektroniska tjänster för rekommenderade leveranser

Artikel 43

Rättslig verkan av elektroniska tjänster för rekommenderade leveranser

1. Uppgifter som sänds och tas emot genom en elektronisk tjänst för rekommenderade leveranser får inte förvägras rättslig verkan eller giltighet som bevis vid rättsliga förfaranden enbart på grund av att de har elektronisk form eller inte uppfyller kraven på den kvalificerade elektroniska tjänsten för rekommenderade leveranser.

2. Uppgifter som sänds och tas emot genom en kvalificerad elektronisk tjänst för rekommenderade leveranser ska omfattas av en presumtion om uppgifternas integritet, om uppgifternas avsändande av den identifierade avsändaren, uppgifternas mottagande av den identifierade adressaten samt om riktigheten i det datum och den tidpunkt för avsändande och mottagande som anges i den kvalificerade elektroniska tjänsten för rekommenderade leveranser.

Artikel 44

Krav på kvalificerade elektroniska tjänster för rekommenderade leveranser

1. Kvalificerade elektroniska tjänster för rekommenderade leveranser ska uppfylla följande krav:

a) De ska tillhandahållas av en eller flera kvalificerade tillhandahållare av betrodda tjänster.

b) De ska med hög grad av tillförlitlighet säkerställa avsändarens identitet.

c) De ska säkerställa adressatens identitet innan uppgifterna levereras.

d) Avsändandet och mottagandet av uppgifter ska säkerställas genom en avancerad elektronisk underskrift eller en avancerad elektronisk stämpel från en kvalificerad tillhandahållare av betrodda tjänster på ett sätt som utesluter möjligheten att uppgifterna ändras utan att det går att upptäcka.

e) Eventuella ändringar av de uppgifter som behövs för att sända eller ta emot uppgifterna ska tydligt anges för uppgifternas avsändare och adressat.

f) Datumet och tidpunkten för avsändande, mottagande och eventuella ändringar av uppgifter måste anges genom en kvalificerad elektronisk tidsstämpling.

Om uppgifterna överförs mellan två eller flera kvalificerade tillhandahållare av betrodda tjänster ska kraven i leden a–f gälla för alla kvalificerade tillhandahållare av betrodda tjänster.

2. Kommissionen får genom genomförandeakter fastställa referensnummer till standarder för processer för att sända och ta emot uppgifter. Överensstämmelse med kraven i punkt 1 ska förutsättas när en process för att sända och ta emot uppgifter uppfyller dessa standarder. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

AVSNITT 8

Autentisering av webbplatser

Artikel 45

Krav på kvalificerade certifikat för autentisering av webbplatser

1. Kvalificerade certifikat för autentisering av webbplatser ska uppfylla kraven i bilaga IV.

2. Kommissionen får genom genomförandeakter fastställa referensnummer till standarder för kvalificerade certifikat för autentisering av webbplatser. Överensstämmelse med kraven i bilaga IV ska förutsättas när ett kvalificerat certifikat för autentisering av webbplatser uppfyller dessa standarder. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

KAPITEL IV

ELEKTRONISKA DOKUMENT

Artikel 46

Rättslig verkan av elektroniska dokument

Ett elektroniskt dokument får inte förvägras rättslig verkan eller giltighet som bevis vid rättsliga förfaranden enbart på grund av att det har elektronisk form.

KAPITEL V

DELEGERING AV BEFOGENHETER OCH GENOMFÖRANDEBESTÄMMELSER

Artikel 47

Utövande av delegeringen

1. Befogenheten att anta delegerade akter ges till kommissionen med förbehåll för de villkor som anges i denna artikel.

2. Den befogenhet att anta delegerade akter som avses i artikel 30.4 ska ges till kommissionen tills vidare från och med den 17 september 2014.

3. Den delegering av befogenhet som avses i artikel 30.4 får när som helst återkallas av Europaparlamentet eller rådet. Ett beslut om återkallelse innebär att delegeringen av den befogenhet som anges i beslutet upphör att gälla. Beslutet får verkan dagen efter det att det offentliggörs i *Europeiska unionens officiella tidning*, eller vid ett senare i beslutet angivet datum. Det påverkar inte giltigheten av delegerade akter som redan har trätt i kraft.

4. Så snart kommissionen antar en delegerad akt ska den samtidigt delge Europaparlamentet och rådet denna.

5. En delegerad akt som antas enligt artikel 30.4 ska träda i kraft endast om varken Europaparlamentet eller rådet har gjort invändningar mot den delegerade akten inom en period av två månader från den dag då akten delgavs Europaparlamentet och rådet, eller om både Europaparlamentet och rådet, före utgången av den perioden, har underrättat kommissionen om att de inte kommer att invända. Denna period ska förlängas med två månader på Europaparlamentets eller rådets initiativ.

Artikel 48

Kommittéförfarande

1. Kommissionen ska biträdas av en kommitté. Denna kommitté ska vara en kommitté i den mening som avses i förordning (EU) nr 182/2011.

2. När det hänvisas till denna punkt ska artikel 5 i förordning (EU) nr 182/2011 tillämpas.

KAPITEL VI

SLUTBESTÄMMELSER

Artikel 49

Översyn

Kommissionen ska göra en översyn över denna förordnings tillämpning och rapportera resultaten till Europaparlamentet och rådet senast den 1 juli 2020. Kommissionen ska särskilt utvärdera huruvida det är lämpligt att ändra denna förordnings tillämpningsområde eller dess särskilda bestämmelser, som artiklarna 6, 7 f, 34, 43, 44 eller 45, med beaktande av den erfarenhet som erhållits vid tillämpningen av denna förordning samt den tekniska och rättsliga utvecklingen och marknadsutvecklingen.

Den rapport som avses i första stycket ska vid behov åtföljas av lagstiftningsförslag.

Dessutom ska kommissionen vart fjärde år efter den rapport som avses i första stycket lämna en rapport till Europaparlamentet och rådet om framstegen med att uppfylla målen för denna förordning.

Artikel 50

Upphävande

1. Direktiv 1999/93/EG ska upphöra att gälla med verkan från och med den 1 juli 2016.

2. Hänvisningar till det upphävda direktivet ska anses som hänvisningar till den här förordningen.

Artikel 51

Övergångsbestämmelser

1. Säkra anordningar för skapande av underskrifter vilkas överensstämmelse har fastställts i enlighet med artikel 3.4 i direktiv 1999/93/EG ska anses som kvalificerade anordningar för skapande av elektroniska underskrifter enligt denna förordning.

2. Kvalificerade certifikat som utfärdats till fysiska personer enligt direktiv 1999/93/EG ska anses som kvalificerade certifikat för elektroniska underskrifter enligt denna förordning till dess att de löper ut.

3. Tillhandahållare av en certifieringstjänst som utfärdar certifikat enligt direktiv 1999/93/EG ska lämna in en rapport om bedömning av överensstämmelse till tillsynsorganet så snart som möjligt och senast den 1 juli 2017. Fram till dess att denna rapport har inlämnats och tillsynsorganet har slutfört sin bedömning av den ska tillhandahållaren av certifieringstjänsten anses vara en kvalificerad tillhandahållare av betrodda tjänster enligt denna förordning.

4. Om en tillhandahållare av certifieringstjänster som utfärdar kvalificerade certifikat enligt direktiv 1999/93/EG inte lämnar in någon rapport om bedömning av överensstämmelse till tillsynsorganet inom den tidsfrist som avses i punkt 3 ska denna tillhandahållare av certifieringstjänster inte anses vara en kvalificerad tillhandahållare av betrodda tjänster enligt denna förordning från och med den 2 juli 2017.

Artikel 52

Ikraftträdande

1. Denna förordning träder i kraft den tjugonde dagen efter det att den har offentliggjorts i *Europeiska unionens officiella tidning*.

2. Den ska tillämpas från och med den 1 juli 2016, med undantag för följande:

a) Artiklarna 8.3, 9.5, 12.2–12.9, 17.8, 19.4, 20.4, 21.4, 22.5, 23.3, 24.5, 27.4, 27.5, 28.6, 29.2, 30.3, 30.4, 31.3, 32.3, 33.2, 34.2, 37.4, 37.5, 38.6, 42.2, 44.2, 45.2, 47 och 48 ska tillämpas från och med den 17 september 2014.

b) Artiklarna 7, 8.1, 8.2, 9, 10, 11 och 12.1 ska tillämpas från och med tillämpningsdagen för de genomförandeakter som avses i artiklarna 8.3 och 12.8.

c) Artikel 6 ska tillämpas från och med tre år efter tillämpningsdagen för de genomförandeakter som avses i artiklarna 8.3 och 12.8.

3. Om det anmälda systemet för elektronisk identifiering före det datum som avses i punkt 2 c i denna artikel finns upptaget i den förteckning som kommissionen offentliggjort enligt artikel 9, ska medlet för elektronisk identifiering inom ramen för detta system enligt artikel 6 erkännas senast 12 månader efter systemets offentliggörande, dock inte före det datum som avses i punkt 2 c i denna artikel.

4. Trots vad som sägs i punkt 2 c i denna artikel får en medlemsstat besluta att ett medel för elektronisk identifiering inom ramen för ett system för elektronisk identifiering som har anmälts i enlighet med artikel 9.1 av en annan medlemsstat ska erkännas i den första medlemsstaten från och med tillämpningsdagen för de genomförandeakter som avses i artiklarna 8.3 och 12.8. De berörda medlemsstaterna ska underrätta kommissionen. Kommissionen ska offentliggöra denna information.

Denna förordning är till alla delar bindande och direkt tillämplig i alla medlemsstater.

Utfärdad i Bryssel 23 juli 2014.

På Europaparlamentets vägnar	*På rådets vägnar*
M. SCHULZ	S. GOZI
Ordförande	*Ordförande*

BILAGA I

KRAV PÅ KVALIFICERADE CERTIFIKAT FÖR ELEKTRONISKA UNDERSKRIFTER

Kvalificerade certifikat för elektroniska underskrifter ska innehålla följande:

a) En uppgift, åtminstone i en form som lämpar sig för automatiserad behandling, om att certifikatet har utfärdats som ett kvalificerat certifikat för elektroniska underskrifter.

b) En uppsättning uppgifter som otvetydigt avser den kvalificerade tillhandahållare av betrodda tjänster som utfärdar de kvalificerade certifikaten, inbegripet uppgift om åtminstone vilken medlemsstat tillhandahållaren är etablerad i, samt

— för juridiska personer: namn och, i tillämpliga fall, registreringsnummer i enlighet med vad som uppgetts i officiella handlingar,

— för fysiska personer: personens namn.

c) Åtminstone undertecknarens namn eller en pseudonym. Om en pseudonym används ska detta tydligt anges.

d) Valideringsuppgifter för elektroniska underskrifter som stämmer överens med uppgifterna för skapande av elektroniska underskrifter.

e) Detaljerade uppgifter om när certifikatet börjar respektive upphör att gälla.

f) Certifikatets identifieringskod, som måste vara unik för den kvalificerade tillhandahållaren av betrodda tjänster.

g) Den avancerade elektroniska underskriften eller den avancerade elektroniska stämpeln för den kvalificerade tillhandahållare av betrodda tjänster som utfärdar certifikatet.

h) Uppgift om var det certifikat som stöder den avancerade elektroniska underskrift eller den avancerade elektroniska stämpeln som avses i led g finns tillgängligt kostnadsfritt.

i) Uppgift om var de tjänster som kan användas för att göra förfrågningar om det kvalificerade certifikatets giltighet är lokaliserade.

j) Om de uppgifter för skapande av elektroniska underskrifter som avser valideringsuppgifterna för elektroniska underskrifter är placerade i en kvalificerad anordning för skapande av elektroniska underskrifter, en lämplig uppgift som anger detta, åtminstone i en form som lämpar sig för automatiserad behandling.

BILAGA II

KRAV PÅ KVALIFICERADE ANORDNINGAR FÖR SKAPANDE AV ELEKTRONISKA UNDERSKRIFTER

1. Kvalificerade anordningar för skapande av elektroniska underskrifter ska genom lämpliga tekniker och förfaranden säkerställa att åtminstone

   a) konfidentialiteten för de uppgifter för skapande av elektroniska underskrifter som används för att skapa elektroniska underskrifter är säkerställd på rimligt sätt,

   b) de uppgifter för skapande av elektroniska underskrifter som används för att skapa elektroniska underskrifter i praktiken endast kan förekomma en gång,

   c) de uppgifter för skapande av elektroniska underskrifter som används för att skapa elektroniska underskrifter med rimlig säkerhet inte kan härledas och att den elektroniska underskriften på ett tillförlitligt sätt är skyddad mot förfalskning med den teknik som för närvarande finns tillgänglig,

   d) de uppgifter för skapande av elektroniska underskrifter som används för att skapa elektroniska underskrifter kan skyddas på ett tillförlitligt sätt av den legitime undertecknaren så att andra inte kan använda dem.

2. Kvalificerade anordningar för skapande av elektroniska underskrifter får inte förändra de uppgifter som ska undertecknas eller hindra att dessa uppgifter läggs fram för undertecknaren före undertecknandet.

3. Generering eller hantering av uppgifter för skapande av elektroniska underskrifter för undertecknarens räkning får endast utföras av en kvalificerad tillhandahållare av betrodda tjänster.

4. Kvalificerade tillhandahållare av betrodda tjänster som för undertecknarens räkning hanterar uppgifter för skapande av elektroniska underskrifter får, utan att det påverkar tillämpningen av punkt 1 d, endast kopiera dessa uppgifter för framställning av säkerhetskopior om följande krav är uppfyllda:

   a) Tillitsnivån för de kopierade uppsättningarna av uppgifter måste vara densamma som för de ursprungliga uppsättningarna av uppgifter.

   b) Antalet kopierade uppsättningar av uppgifter får inte överskrida det minsta antal som krävs för att säkerställa tjänstens kontinuitet.

BILAGA III

KRAV PÅ KVALIFICERADE CERTIFIKAT FÖR ELEKTRONISKA STÄMPLAR

Kvalificerade certifikat för elektroniska stämplar ska innehålla följande:

a) En uppgift, åtminstone i en form som lämpar sig för automatiserad behandling, om att certifikatet har utfärdats som ett kvalificerat certifikat för elektroniska stämplar.

b) En uppsättning uppgifter som otvetydigt avser den kvalificerade tillhandahållare av betrodda tjänster som utfärdar de kvalificerade certifikaten, inbegripet uppgift om åtminstone vilken medlemsstat tillhandahållaren är etablerad i, samt

— för juridiska personer: namn och, i tillämpliga fall, registreringsnummer i enlighet med vad som uppgetts i de officiella handlingarna,

— för fysiska personer: personens namn.

c) Åtminstone namnet på skaparen av stämpeln och, i förekommande fall, registreringsnummer i enlighet med vad som uppgetts i officiella handlingar.

d) Valideringsuppgifter för elektroniska stämplar som stämmer överens med uppgifterna för skapande av elektroniska stämplar.

e) Detaljerade uppgifter om när certifikatet börjar respektive upphör att gälla.

f) Certifikatets identifieringskod, som måste vara unik för den kvalificerade tillhandahållaren av betrodda tjänster.

g) Den avancerade elektroniska underskriften eller den avancerade elektroniska stämpeln för den kvalificerade tillhandahållare av betrodda tjänster som utfärdar certifikatet.

h) Uppgift om var det certifikat som stöder den avancerade elektroniska underskrift eller den avancerade elektroniska stämpeln som avses i led g är tillgängligt kostnadsfritt.

i) Uppgift om var de tjänster som kan användas för att göra förfrågningar om det kvalificerade certifikatets giltighet är lokaliserade.

j) Om de uppgifter för skapande av elektroniska stämplar som har koppling till uppgifterna för validering av elektroniska stämplar är placerade i en kvalificerad anordning för skapande av elektroniska stämplar, en lämplig uppgift om detta, åtminstone i en form som lämpar sig för automatiserad behandling.

BILAGA IV

KRAV PÅ KVALIFICERADE CERTIFIKAT FÖR AUTENTISERING AV WEBBPLATSER

Kvalificerade certifikat för autentisering av webbplatser ska innehålla följande:

a) En uppgift, åtminstone i en form som lämpar sig för automatiserad behandling, om att certifikatet har utfärdats som ett kvalificerat certifikat för autentisering av webbplatser.

b) En uppsättning uppgifter som otvetydigt avser den kvalificerade tillhandahållare av betrodda tjänster som utfärdar de kvalificerade certifikaten, inbegripet uppgift om åtminstone vilken medlemsstat tillhandahållaren är etablerad i, samt

— för juridiska personer: namn och, i tillämpliga fall, registreringsnummer i enlighet med vad som uppgetts i officiella handlingar,

— för fysiska personer: personens namn.

c) För fysiska personer: åtminstone namnet på den person som certifikatet utfärdats för eller en pseudonym. Om en pseudonym används ska detta tydligt anges.

För juridiska personer: åtminstone namnet på den juridiska person som certifikatet utfärdats för och, i förekommande fall, registreringsnummer i enlighet med vad som uppgetts i officiella handlingar.

d) Adressuppgifter, inbegripet åtminstone stad och stat, för den fysiska eller juridiska person som certifikatet utfärdats för och, i förekommande fall, i enlighet med vad som uppgetts i officiella handlingar.

e) Det eller de domännamn som drivs av den fysiska eller juridiska person som certifikatet utfärdats för.

f) Detaljerade uppgifter om när certifikatet börjar respektive upphör att gälla.

g) Certifikatets identifieringskod, som måste vara unik för den kvalificerade tillhandahållaren av betrodda tjänster.

h) Den avancerade elektroniska underskriften eller den avancerade elektroniska stämpeln för den kvalificerade tillhandahållare av betrodda tjänster som utfärdar certifikatet.

i) Uppgift om var det certifikat som stöder den avancerade elektroniska underskriften eller den avancerade elektroniska stämpeln som avses i led h finns tillgängligt kostnadsfritt.

j) Uppgift om var de tjänster är lokaliserade som kan användas för att göra förfrågningar om det kvalificerade certifikatets giltighet.

Statens offentliga utredningar 2021

Kronologisk förteckning

1. Säker och kostnadseffektiv it-drift – rättsliga förutsättningar för utkontraktering. I.
2. Krav på kunskaper i svenska och samhällskunskap för svenskt medborgarskap. Ju.
3. Skolbibliotek för bildning och utbildning. U.
4. Informationsöverföring inom vård och omsorg. S.
5. Ett förbättrat system för arbetskraftsinvandring. Ju.
6. God och nära vård. Rätt stöd till psykisk hälsa. S.
7. Förstärkt skydd för väljarna vid röstmottagningen. Ju.
8. När behovet får styra – ett tandvårdssystem för en mer jämlik tandhälsa. Vol. 1 & Vol. 2, bilagor + Sammanfattning (häfte). S.
9. Vem kan man lita på? Enkel och ändamålsenlig användning av betrodda tjänster i den offentliga förvaltningen. I.

Statens offentliga utredningar 2021

Systematisk förteckning

Infrastrukturdepartementet

Säker och kostnadseffektiv it-drift – rättsliga förutsättningar för utkontraktering. [1]

Vem kan man lita på? Enkel och ändamålsenlig användning av betrodda tjänster i den offentliga förvaltningen. [9]

Justitiedepartementet

Krav på kunskaper i svenska och samhällskunskap för svenskt medborgarskap. [2]

Ett förbättrat system för arbetskraftsinvandring. [5]

Förstärkt skydd för väljarna vid röstmottagningen. [7]

Socialdepartementet

Informationsöverföring inom vård och omsorg. [4]

God och nära vård. Rätt stöd till psykisk hälsa. [6]

När behovet får styra – ett tandvårdssystem för en mer jämlik tandhälsa. Vol. 1 & Vol. 2, bilagor + Sammanfattning (häfte). [8]

Utbildningsdepartementet

Skolbibliotek för bildning och utbildning. [3]

Regeringskansliet

103 33 Stockholm Växel 08-405 10 00 www.regeringen.se

ISBN 978-91-525-0029-3 ISSN 0375-250X

Omslag: Elanders Sverige AB
Bild: Agneta S Öberg