PTS

Datum
2017-02-24

Rapport:

Vägledning

För betrodda tjänster i Sverige enligt eIDAS – Utgåva 2

Vägledning
För betrodda tjänster i Sverige enligt eIDAS – Utgåva 2

Diarienummer
17-4465

ISSN
1650-9862

Post- och telestyrelsen
Box 5398
102 49 Stockholm

08-678 55 00
pts@pts.se
www.pts.se

Innehåll

1 Inledning

Den 1 juli 2016 började EU:s förordning[1] om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden (eIDAS-förordningen) tillämpas i Sverige.

Elektronisk identifiering och elektroniska underskrifter är viktiga förutsättningar för att privatpersoner och företag ska kunna använda digitala tjänster. Men för att ett system med elektronisk identifiering ska fungera krävs att alla inblandade parter uppfattar det som tillförlitligt. Förordningen innehåller därför en rättslig ram för ett antal tjänster som tillhandahållare av funktioner för elektroniskt identifiering och elektroniska underskrifter vanligen erbjuder (betrodda tjänster). Förordningen innehåller även regler för tillhandahållarna av sådana tjänster. Syftet är att öka förtroendet för elektroniska transaktioner på den inre marknaden genom att ge en gemensam grund för ett säkert elektroniskt samspel mellan företag, medborgare och offentliga myndigheter.

Det finns många krav på berörda aktörer i eIDAS-förordningen men detaljerade regler saknas. Istället har EU-kommissionen (kommissionen) i förordningen fått möjlighet att anta genomförandeakter som ska fastställa referenser till standarder som mer i detalj ska beskriva tekniska krav och andra regler. De flesta genomförandeakter är inte obligatoriska för kommissionen att anta och endast ett fåtal av de genomförandeakter som kommissionen har möjlighet att ta fram är på plats.

Den 1 juli 2016 trädde även en svensk lag och förordning med kompletterande bestämmelser till eIDAS-förordningen ikraft.[2] I den svenska förordningen har regeringen utsett Post- och telestyrelsen (PTS) till tillsynsmyndighet. I lagen finns bl.a. bestämmelser om tillsyn och PTS mandat att utfärda föreskrifter[3] på några av de områden som berörs i eIDAS-förordningen. Men med hänsyn till att detta är ett relativt oprövat regelverk vars effekter på marknaden ännu är oklara har PTS hittills valt att inte utnyttja dessa bemyndiganden. Det är möjligt att PTS längre fram gör en annan bedömning. Istället har PTS valt att

[1] 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 upphävande av direktiv 1999/93/EG.

[2] Lag (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering och förordning (2016:576) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering.

[3] PTS har rätt att meddela föreskrifter om skyldighet för tillhandahållare av betrodda tjänster att betala avgift och PTS planerar att ta ut en avgift om 25 000 kronor per år från 2017. PTS har vidare rätt att föreskriva om krav för ackreditering av organ för bedömning av överenstämmelse, hur bedömningar av överenstämmelse ska göras och rapportering av bedömningar av överenstämmelse.

samla det stöd och de rekommendationer som myndigheten bedömer som nödvändiga för att eIDAS-förordningen ska kunna tillämpas i detta dokument.

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 som vill etablera sig som kvalificerade sådana. Vägledningen riktar sig även mot icke kvalificerade tillhandahållare av betrodda tjänster, berörda myndigheter och andra organ.

Vägledningen är inte bindande utan endast en beskrivning av det regelverk som gäller och det stöd som finns i form av standarder.

2 Bakgrund

2.1 eIDAS-förordningen avseende betrodda tjänster

Syftet med eIDAS-förordningen är att säkerställa en väl fungerande marknad och uppnå en lämplig säkerhetsnivå för medel för elektronisk identifiering och betrodda tjänster (artikel 1).

I förordningen slås principen om en inre marknad fast (artikel 4). Den som tillhandahåller betrodda tjänster i en medlemsstat får inte hindras att tillhandahålla sådana tjänster i en annan medlemsstat av skäl som anges i förordningen. Anordningar för underskrifter och stämplar, och betrodda tjänster som överensstämmer med förordningen ska omfattas av fri rörlighet på den inre marknaden.

I förordningen finns allmänna bestämmelser om betrodda tjänster och kvalificerade betrodda tjänster samt särskilda bestämmelser om elektroniska underskrifter, elektroniska stämplar, elektroniska tidsstämplingar, elektroniska tjänster för rekommenderade leveranser och autentisering av webbplatser. Dessutom finns det bestämmelser om elektroniska dokument som är innehåll lagrat i elektronisk form som även omfattar ljud- och bildinspelningar och audiovisuella inspelningar.

2.1.1 Tillämpningsområde

eIDAS-förordningen gäller system för elektronisk identifiering som en medlemsstat har anmält och tillhandahållare av betrodda tjänster som är etablerade inom unionen (artikel 2.1).

Förordningen gäller däremot inte tillhandahållande av betrodda tjänster som till följd av nationell lagstiftning eller avtal mellan en avgränsad krets deltagare endast används inom slutna system (artikel 2.2). I ingresspunkt 21 utvecklas vad som menas med slutna system. Där anges att förordningen inte gäller tillhandahållare av tjänster som endast används inom slutna system mellan en avgränsad uppsättning deltagare och som inte påverkar tredje man. Som exempel nämns system som inrättats i företag eller offentlig förvaltning för hantering av interna förfaranden. I ingresspunkten anges vidare att endast betrodda tjänster som tillhandahålls för allmänheten och som påverkar tredje man bör uppfylla de krav som ställs i förordningen.

Förordningen påverkar inte heller bestämmelser i nationell lagstiftning eller unionslagstiftningen som avser ingående av avtal och deras giltighet eller andra rättsliga eller förfarandemässiga skyldigheter avseende formkrav (artikel 2.3). Förordningen bör inte heller inverka på nationella formkrav avseende offentliga register, i synnerhet inte kommersiella register eller fastighetsregister (ingresspunkt 21). I svensk lagstiftning ställs för närvarande inte några krav på

att använda kvalificerade betrodda tjänster vare sig mellan enskilda eller gentemot offentliga organ.

2.1.2 Definitioner

I artikel 3 återfinns vissa definitioner. Där anges bl.a. att med en *betrodd tjänst* avses 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 samt elektroniska tjänster för rekommenderade leveranser och certifikat med anknytning till dessa tjänster. Med betrodda tjänster avses också skapande, kontroll och validering av certifikat för autentisering av webbplatser samt bevarande av elektroniska underskrifter, stämplar och certifikat med anknytning till dessa tjänster.

En *elektronisk stämpel* utgör för en juridisk person motsvarigheten till en elektronisk underskrift av en fysisk person.

Med *elektronisk tidsstämpling* avses 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 angivna tidpunkten.

Elektroniska tjänster för rekommenderade leveranser gör det möjligt att överföra uppgifter mellan tredje män på elektronisk väg på ett sätt som tillhandahåller bevis om uppgifternas hantering, inklusive sändande och mottagande, och som skyddar uppgifterna mot risken för förlust, stöld, skada eller otillåtna ändringar.

Genom *autentisering av webbplatser* är det möjligt att bekräfta att en fysisk eller juridisk person är kopplad till en viss webbplats och att uppgifterna på webbplatsen är korrekta.

2.1.3 Kvalificerade betrodda tjänster

I artiklarna 20–24 finns särskilda bestämmelser om kvalificerade betrodda tjänster. Den som vill tillhandahålla sådana tjänster ska anmäla detta till tillsynsmyndigheten och samtidigt lämna in en rapport med en överens-stämmelsebedömning som är utfärdad av ett ackrediterat organ för bedömning av överensstämmelse[4]. Om tillhandahållaren och dennes betrodda tjänster uppfyller förordningens krav beviljas dessa status som kvalificerade och förs upp på en nationell förteckning (eng. *trusted list*) över kvalificerade tillhandahållare av betrodda tjänster inom EU och de tjänster som dessa tillhandahåller. Det finns även ett förfarande för återkallande av en tillhandahållares eller en tjänsts status som kvalificerad om kraven inte längre uppfylls.

[4] Organen brukar benämnas som certifieringsorgan eller Conformity Assessment Body (CAB).

För kvalificerade tillhandahållare av betrodda tjänster gäller särskilda krav på, t.ex.

- Kontroll av identiteten hos den till vilken ett kvalificerat certifikat utfärdas
- Personalens utbildning och kunskaper
- Ekonomisk förmåga att bära risken för verksamheten,
- Teknisk säkerhet och tillförlitlighet hos system,
- Löpande planering för att kunna garantera tjänstens kontinuitet i fall av verksamhetens upphörande[5]

Förordningen innehåller också krav på att kvalificerade tillhandahållare av betrodda tjänster återkommande ska granskas av ackrediterade organ i syfte att kontrollera att tillhandahållarna uppfyller förordningens krav.

2.1.4 Övergångsbestämmelser

När eIDAS-förordningen trädde i kraft upphörde direktiv 1999/93/EG om ett gemenskapsramverk för elektroniska signaturer (signaturdirektivet)[6] att gälla. Detsamma gällde för den svenska lagen (2000:832) om kvalificerade elektroniska signaturer.[7]

I artikel 51 i eIDAS-förordningen finns vissa övergångsbestämmelser. Bl.a. anges att säkra anordningar för underskrifter och kvalificerade certifikat till fysiska personer som fastställts enligt signaturdirektivet ska anses som kvalificerade anordningar för skapande av elektroniska underskrifter och kvalificerade certifikat för elektroniska underskrifter enligt eIDAS-förordningen.

2.1.5 Nationell ansvarsfördelning gällande betrodda tjänster

Regeringen har i förordning med kompletterande bestämmelser till eIDAS-förordningen och i berörda myndigheters instruktioner fördelat ansvaret gällande eIDAS i Sverige.[8]

PTS är utsedd till tillsynsmyndighet och ska fullgöra tillsynsorganets uppgifter enligt eIDAS-förordningen samt utöva tillsyn över efterlevnaden av lagen med

[5] Se kapitel 9 nedan.
[6] Europaparlamentets och rådets direktiv 1999/93/EG av den 13 december 1999 om ett gemenskapsramverk för elektroniska signaturer.
[7] Övergångsbestämmelser till lag (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering.
[8] Förordning (2016:576) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering, förordning (2007:951) med instruktion för Post- och telestyrelsen, förordning (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap, förordning (2007:854) med instruktion för Försvarets materielverk, förordning (2009:895) med instruktion för Styrelsen för ackreditering och teknisk kontroll.

kompletterande bestämmelser till eIDAS-förordningen och föreskrifter som meddelats med stöd av lagen. PTS har rätt att meddela föreskrifter om skyldighet för tillhandahållare av betrodda tjänster att betala avgift för PTS tillsynsverksamhet. PTS har vidare rätt att föreskriva om krav för ackreditering av organ för bedömning av överenstämmelse, hur bedömningar av överenstämmelse ska göras och rapportering av bedömningar av överenstämmelse.

Myndigheten för samhällsskydd och beredskaps (MSB) får meddela föreskrifter om säkerhetsegenskaper (s.k. skyddsprofiler) för anordningar för skapande av kvalificerade elektroniska underskrifter och stämplar. PTS har rätt att föreskriva om eventuella ytterligare krav på certifiering av sådana anordningar.

Försvarets materielverk ansvarar, genom det nationella certifieringsorganet för IT-säkerhet vid myndigheten (FMV/CSEC), för certifiering av anordningar för skapande av kvalificerade elektroniska underskrifter och stämplar enligt artiklarna 30 och 39 i eIDAS-förordningen.

Styrelsen för ackreditering och teknisk kontroll (Swedac) är Sveriges nationella ackrediteringsorgan. Ett organ för bedömning av överenstämmelse som vill bli ackrediterat enligt eIDAS-förordningen måste lämna en ansökan till Swedac. Därefter prövar och bedömer Swedac om organet uppfyller de krav som ställs i förordning (EG) nr 765/2008,[9] kraven i lagen (2011:791) om ackreditering och teknisk kontroll med tillhörande förordning samt kraven i de föreskrifter som Swedac har meddelat.

Ekonomistyrningsverket har ett regeringsuppdrag att arbeta med e-handel och s-sense. Det uppdraget har utökats till att även omfatta samordning, bevakning och informationsspridning avseende CEF[10]-byggblocket eDelivery[11]. Inom ramen för den utvidgningen ingår även att bevaka elektroniska tjänster för elektronisk leverans enligt eIDAS-förordningen och stödja arbetet med just den specifika betrodda tjänsten, då den i många sammanhang likställs med eDelivery-byggblocket ur ett tekniskt perspektiv.

[9] Europaparlamentets och rådets förordning (EG) nr 765/2008 om krav för ackreditering och marknadskontroll i samband med saluföring av produkter och upphävande av förordning (EEG) nr 339/93.
[10] CEF: https://ec.europa.eu/digital-single-market/en/connecting-europe-facility.
[11] CEF eDelivery: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery.

2.2 Genomförandeakter och standarder

2.2.1 Genomförandeakter

eIDAS-förordningen innehåller inte några detaljerade regler utan kommissionen har i förordningen istället fått möjlighet att i genomförandeakter fastställa de mer detaljerade bestämmelserna. Flertalet genomförandeakter ger kommissionen möjlighet att referera till standard på området. Om kommissionen refererar till en standard innebär det inte att alla tillhandahållare måste följa den standarden, men om den utpekade standarden följs antas att kraven i förordningen är uppfyllda. Beträffande många av genomförandeakterna är det i dagsläget oklar när och om kommissionen kommer att ta fram sådan akter.

2.2.2 Standarder som refereras av kommissionen

Kommissionen har gett de europeiska standardiseringsorganisationerna CEN[12] och ETSI[13] i uppdrag att ta fram standarder på området betrodda tjänster, i enlighet med standardiseringsmandat M/460[14].
Standardiseringsorganisationerna har tagit fram ett gemensamt paket av standarder på området säkra elektroniska transaktioner för e-handel och e-tjänster i Europa. Syftet med mandatet är att skapa förutsättningar för interoperabilitet och ett europeiskt standardramverk. Dessa standarder är anpassade efter förordningen och utgör grunden för beslutade genomförandeakter och avser även att utgöra grunden för kommande genomförandeakter.

I avvaktan på att kommissionen tar fram genomförandeakter anser PTS att det är lämpligt att använda de standarder som CEN och ETSI beslutat på området för betrodda tjänster. En del av dessa standarder är även europeiska normer (EN) och när sådana finns anser PTS att det kan vara lämpligt att de används. När det saknas europeiska normer anser PTS att det kan vara lämpligt att använda antingen befintliga europeiska standarder eller utkast till europeiska normer. Anledningen till detta är att PTS anser det troligt att kommissionen vid ett eventuellt framtagande av genomförandeakter kommer att referera till dessa standarder.

2.2.3 Alternativa standarder

Kraven i genomförandeakterna innebär att andra standarder än de som pekas ut av kommissionen kan användas. Men för att leva upp till de standarder som refereras i genomförandeakterna förutsätts i många fall att vissa utpekade

[12] European Committee for Standardization.
[13] European Telecommunications Standards Institute.
[14] http://www.etsi.org/images/files/ECMandates/m460.pdf.

bestämmelser i förordningen också efterlevs av de kvalificerade tillhandahållarna.

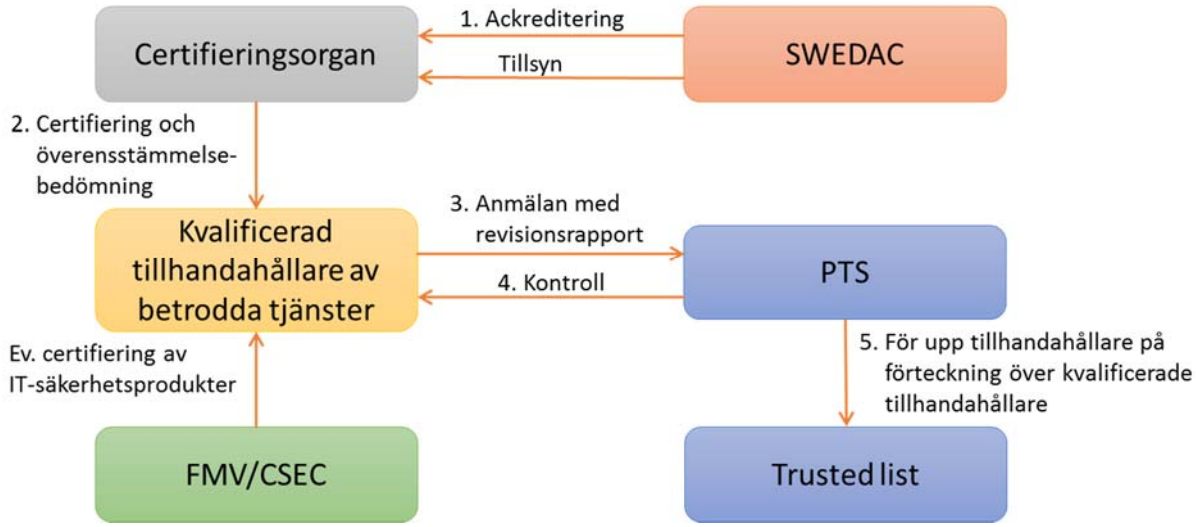
Det finns dock undantag från möjligheten att använda alternativa standarder när det gäller kraven på säkra anordningar enligt artiklarna 30 och 39. De standarder som pekas ut i dessa artiklar är obligatoriska för kvalificerade tillhandahållare att följa.

Om andra standarder än de som pekas ut av kommissionen eller de som anges i denna vägledning används kan handläggningstiden för den initiala kontrollen ta längre tid. Detta eftersom PTS kontroll av rapporten om bedömning av överensstämmelse då i högre utsträckning kommer att innebära en kontroll av använda alternativa standarder.

3 Etablering av kvalificerade tillhandahållare och kvalificerade betrodda tjänster

3.1 Allmänt

I förordningen finns krav för hur en kvalificerad tillhandahållare av betrodda tjänster etablerar och anmäler sig till PTS. Kraven anger även hur en betrodd tjänst får statusen som en kvalificerad betrodd tjänst.



För att tillhandahållare ska kunna tillhandahålla kvalificerade betrodda tjänster krävs att de:

1. Anlitar ett i EU ackrediterat organ för bedömning av överensstämmelse.
2. Följer förordningens regler avseende tillhandahållare och de betrodda tjänster tillhandahållaren erbjuder.[15]
3. Anmäler till PTS att man avser tillhandahålla kvalificerade betrodda tjänster.
4. Efter kontroll av verksamheten och tjänsterna kan PTS bevilja tillhandahållare status som kvalificerad tillhandahållare av betrodda tjänster respektive kvalificerad status för de tillhandahållna betrodda tjänsterna.
5. De kvalificerade tillhandahållarna och de kvalificerade betrodda tjänsterna förs upp på *trusted list* (nationell förteckning). PTS

[15] Se kapitel 4-7 nedan.

kommer att behöva information om tillhandahållare, tjänster och i förekommande fall certifikat som ska inkluderas i listan för att uppfylla kraven i genomförandeakten[16] på området.

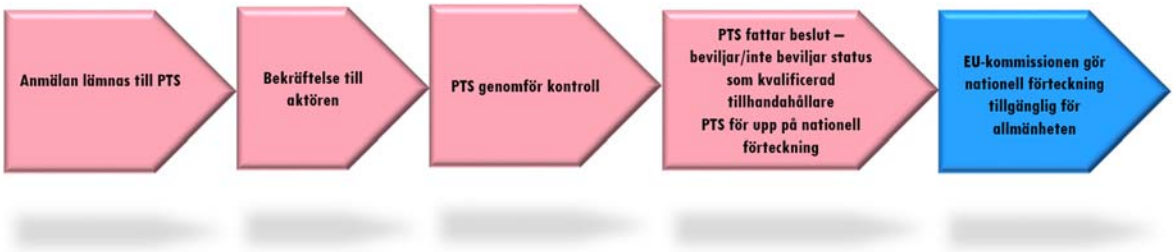
Tillhandahållare som vill bli kvalificerade behöver vända sig till ett ackrediterat organ för bedömning av överenstämmelse. Det finns för närvarande inget sådant organ som är ackrediterat i Sverige. Det finns ett fåtal organ som är ackrediterade i Europa och fler som håller på att ackrediteras. Frågor om ackrediterade organ i Sverige kan ställas till Swedac. Den inre marknaden innebär att tillhandahållaren kan vända sig till ett organ för bedömning av överenstämmelse som är ackrediterat i ett annat medlemsland i EU.

För det fall att en tillhandahållare av en kvalificerad betrodd tjänst, som vill påbörja verksamheten, tillhandahåller en tjänst som innebär att de utfärdar eller lagrar privata nycklar ska dessa nycklar skyddas i en anordning för skapande av elektroniska underskrifter och stämplar. Kontroll av en sådan tjänst sker i samband med etableringen. Se vidare kapitel 7 nedan.

3.2 Process för igångsättande av en kvalificerad betrodd tjänst

Tillhandahållaren skickar in anmälan och rapporten från överensstämmelsebedömningen till PTS. Därefter kommer PTS att kontrollera rapporten från överensstämmelsebedömningen. Denna kontroll leder till att PTS fattar ett beslut om tillhandahållaren och de tillhandahållna tjänsterna uppfyller kraven eller inte. Om kraven är uppfyllda ges statusen som kvalificerad dels till tillhandahållaren, dels till respektive betrodd tjänst. Det görs praktiskt genom att dessa tillhandahållare och tjänster förs upp på den nationella förteckningen, även kallad *trusted list*.

[16] 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 (Text av betydelse för EES).



3.3 Tidsfrister

Av förordningen (artikel 21.2) följer att om kontrollen av en tillhandahållare och dess tjänster inte har slutförts inom tre månader från det att anmälan gavs in, ska PTS informera tillhandahållaren om detta och ange orsaken till förseningen samt när kontrollen beräknas vara slutförd. Tidsfristen beräknas från dagen då tillhandahållaren ger in anmälan till PTS.

3.4 PTS handläggning av anmälan

PTS handläggning av anmälan består dels av en kontroll av rapporten från överensstämmelsebedömningen, dels av ytterligare kontroller som myndigheten anser nödvändiga för att bekräfta att tillhandahållaren och de betrodda tjänsterna uppfyller samtliga krav i förordningen och tillhörande genomförandeakter. Mer information finns på PTS webbplats (www.pts.se/eIDAS).

4 Krav som omfattar såväl kvalificerade som icke kvalificerade tillhandahållare

Vissa bestämmelser i förordningen berör alla tillhandahållare, dvs. även tillhandahållare som inte är kvalificerade i förordningens mening. Såväl kvalificerade som icke kvalificerade tillhandahållare omfattas bl.a. av kraven som gäller skadeståndsansvar (artikel 13) och säkerhet (artikel 19). Av ingresspunkt 35 följer att syftet med regleringen är att säkerställa att även de icke kvalificerade tillhandahållarna har vederbörlig noggrannhet, insyn och ansvarighet i sina verksamheter och tjänster. Det anges dock att med tanke på den typ av tjänster som tillhandahålls bör det göras åtskillnad mellan kraven på kvalificerade och på icke kvalificerade tillhandahållare.

4.1 Skadeståndsansvar (artikel 13)

Bestämmelsen i artikel 13 om skadeståndsansvar gäller både kvalificerade och icke kvalificerade tillhandahållare av betrodda tjänster. Av artikelns första stycke framgår att alla tillhandahållare har skadeståndsansvar för skada som åsamkats en fysisk eller juridisk person avsiktligt eller på grund av oaktsamhet genom underlåtenhet att uppfylla kraven förordningen.

I andra och tredje stycket finns regler om bevisbördan. För icke kvalificerade tillhandahållare vilar bevisbördan för avsikt eller oaktsamhet på den fysiska eller juridiska person som gör gällande sådan skada. Bevisbördan för kvalificerade tillhandahållare är uttryckt som så att avsikt eller oaktsamhet hos den kvalificerade tillhandahållaren ska anses föreligga om inte den kvalificerade tillhandahållaren bevisar att skadan har uppstått utan avsikt eller oaktsamhet.

Reglerna om skadeståndsansvar ska tillämpas i enlighet med nationella bestämmelser, dvs. förutom bestämmelserna i artikel 13 är det de svenska reglerna om skada, oaktsamhet etc. som ska användas.

4.2 Säkerhetskrav och incidentrapportering (artikel 19)

Förordningens krav på säkerhet enligt artikel 19.1 omfattar såväl kvalificerade som icke kvalificerade tillhandahållare av betrodda tjänster.[17] Alla tillhandahållare ska vidta lämpliga tekniska och organisatoriska åtgärder för att hantera riskerna för säkerheten i de betrodda tjänster som de tillhandahåller. Säkerhetsnivån ska stå i proportion till graden av risk med beaktande av

[17] Se vidare i kap. 6 nedan.

teknikutvecklingen. Åtgärder ska vidtas för att förhindra och minimera säkerhetsincidenter och informera berörda parter om inträffade incidenters konsekvenser.

Detta torde medföra att tillhandahållares säkerhetsarbete ska bedrivas långsiktigt, kontinuerligt och systematiskt samt att det ska finnas en tydlig rollfördelning med särskilt utpekade ansvariga. Exempel på åtgärder och stöd i detta arbete finns i standarder som EN 319 401 som pekar ut vilka policydokument som kan behövas och som refererar till ISO/IEC 27002:2013 för åtgärder.

I artikel 19.2 anges att alla tillhandahållare, kvalificerade och icke kvalificerade, utan dröjsmål, senast inom 24 timmar ska rapportera säkerhets- eller integritetsincidenter till PTS. Det gäller de incidenter som i betydande omfattning påverkar den betrodda tjänst som tillhandahålls eller de personuppgifter som ingår i denna. Alla tillhandahållare har vidare en skyldighet att underrätta fysisk eller juridisk person som påverkats negativt på grund av den inträffade incidenten.

4.3 Tillsyn (artikel 17)

PTS roll som tillsynsmyndighet framgår av artikel 17.3. Tillsynen omfattar både kvalificerade och icke kvalificerade tillhandahållare av betrodda tjänster som är etablerade i Sverige.

4.3.1 Tillsyn över kvalificerade tillhandahållare

Tillsynen över kvalificerade tillhandahållare går ut på att genom såväl förebyggande verksamhet som kontroller i efterhand se till att tillhandahållarna och deras tjänster uppfyller förordningens krav (artikel 17.3 a).

4.3.2 Tillsyn över icke kvalificerade tillhandahållare

När det gäller icke-kvalificerade tillhandahållare framgår det av förordningen (artikel 17.3 b) att PTS ska agera när myndigheten tar del av information eller uppgifter om att en icke kvalificerad tillhandahållare eller en betrodd tjänst som denne tillhandahåller inte uppfyller kraven i förordningen.

5 Regler för överensstämmelsebedömning

5.1 Överensstämmelsebedömning

Tillhandahållare av betrodda tjänster som har för avsikt att börja tillhandahålla kvalificerade betrodda tjänster ska enligt artikel 21 i förordningen anmäla detta till PTS. Tillhandahållaren ska samtidigt lämna in en rapport om överensstämmelsebedömning som är utfärdad av ett certifieringsorgan. Certifieringsorganet ska vara ackrediterat för uppgiften att göra bedömningar av överenstämmelse för de kvalificerade tjänster enligt eIDAS-förordningen som tillhandahållaren vill anmäla. PTS ska då kontrollera att tillhandahållaren och de betrodda tjänster som tillhandahålls uppfyller kraven i förordningen. De allmänna kraven på de kvalificerade tillhandahållarna av betrodda tjänster framgår av artikel 24.

Kommissionen har rätt att ta fram genomförandeakter som refererar till standarder för ackreditering av organ för överensstämmelsebedömning och för granskningsregler för överensstämmelsebedömning (artikel 20.4). Kommissionen har vid publiceringen av den här vägledningen ännu inte inlett arbetet med dessa genomförandeakter.

När det gäller granskningsregler för överensstämmelsebedömningen anser PTS att det kan vara lämpligt att använda den europeiska normen EN 319 403. Av normen följer att certifiering är den kontrollform som organet bör arbeta efter.

5.1.1 Lämpliga standarder

De policy- och säkerhetskrav som överensstämmelsebedömningen bör göras emot finns i europeiska standarder och normer. Den europeiska normen med generella säkerhetskrav på tillhandahållare av betrodda tjänster, EN 319 401, kan enligt PTS uppfattning vara lämplig att använda vid överensstämmelsebedömningen.

5.2 Rapport om överensstämmelsebedömning

Tillhandahållare av betrodda tjänster som önskar ha status som kvalificerade sådana ska i samband med anmälan till PTS överlämna en rapport om överensstämmelsebedömning. Denna överensstämmelsebedömning ska enligt bestämmelserna i artiklarna 20 och 21 omfatta såväl tillhandahållaren som de betrodda tjänster som denne tillhandahåller och som önskas vara kvalificerade.

Kommissionen får ta fram genomförandeakter som refererar till standarder för rapporten om överensstämmelsebedömningen. Detta arbete är ännu inte påbörjat.

Rapporten om överensstämmelsebedömning kommer att vara en viktig del av både PTS initiala kontroll och beslut om en tillhandahållare ska få statusen som kvalificerad tillhandahållare och om de betrodda tjänster som denne tillhandahåller är kvalificerade. Rapporten behöver därför visa att varje, för det enskilda fallet tillämplig bestämmelse i förordningen, uppfylls. Rapporten behöver vidare visa hur kraven efterlevs.

5.2.1 Lämpliga standarder

I avvaktan på att kommissionen tar fram genomförandeakter anser PTS att det är lämpligt att rapporten från överensstämmelsebedömningen åtminstone innehåller den information som specificeras enligt EN 319 403.

6 Krav på kvalificerade betrodda tjänster

6.1 Kvalificerade certifikat för elektroniska underskrifter och stämplar

I förordningens artiklar 25 och 35 anges vilken rättslig verkan en elektronisk underskrift respektive en elektronisk stämpel har. Av artiklarna 26 och 36 följer vilka krav som ställs på en underskrift och en stämpel för att de ska ses som avancerade elektroniska underskrifter och stämplar. En kvalificerad underskrift eller stämpel är enligt definitionerna i artikel 2 en avancerad underskrift eller stämpel som baserar sig på ett kvalificerat certifikat och skapas med hjälp av en kvalificerad anordning. I artiklarna 27 och 37 regleras medlemsländernas skyldigheter att godta elektroniska underskrifter och stämplar från andra medlemsländer.

För att ett certifikat ska anses kvalificerat ska det uppfylla kraven i artiklarna 28 och 38 samt förordningens bilaga 1. Certifikaten ska inte omfattas av några ytterligare krav än de som framgår av förordningen. Certifikaten får däremot omfatta extra attribut, om attributen inte påverkar stämplarnas eller underskrifters kompabilitet och erkännanden. Om ett kvalificerat certifikat spärras ska det ses som ogiltigt från tidpunkten för när en begäran om spärrning sker. Statusen ska inte i efterhand kunna ändras så att det ses som giltigt.

Kommissionen har tagit fram en genomförandeakt avseende format för avancerade elektroniska underskrifter och stämplar[18].

Kommissionen får även ta fram genomförandeakter som refererar till standarder för kvalificerade certifikat för elektroniska underskrifter och stämplar. Detta arbete har ännu inte inletts.

6.1.1 Lämpliga standarder

Kommissionen har tagit fram genomförandeakter på ett område där de har rätt att ta fram genomförandeakter gällande format för underskrifter och stämplar. De har däremot inte tagit fram genomförandeakter som refererar till standarder för certifikat format eller för utfärdare av kvalificerade certifikat. I avvaktan på att kommissionen tar fram genomförandeakter för utfärdare av kvalificerade

[18] 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 (Text av betydelse för EES).

certifikat anser PTS att en lämplig standard på området kan vara EN 319 411-1 och EN 319 411-2.

6.2 Kvalificerad valideringstjänst

Enligt artikel 32 i förordningen ska valideringsförfarandet från en kvalificerad valideringstjänst bekräfta en kvalificerad elektronisk underskrift om den skapats med ett kvalificerat certifikat i enlighet med bilaga 1. Alla uppgifter från certifikatet och anordningen ska tillhandahållas till den som förlitar sig på valideringen. Den förlitande parten förutsätts få det korrekta resultatet av valideringsförfarandet och det ska göra det möjligt för den förlitande parten att upptäcka eventuella problem som är relevanta för säkerheten.

Av artikel 33 följer att en kvalificerad valideringstjänst endast får erbjudas av en kvalificerad tillhandahållare av betrodda tjänster. Förlitande parter ska kunna ta del av resultatet 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.

Kommissionen får ta fram genomförandeakter som refererar till standarder för validering av kvalificerade elektroniska underskrifter respektive standarder för kvalificerade valideringstjänster. Kommissionen har ännu inte inlett arbetet med dessa genomförandeakter.

6.2.1 Lämpliga standarder

I avvaktan på att kommissionen tar fram genomförandeakter anser PTS att lämplig standard för valideringsprocesser kan vara EN 319 102-1.

6.3 Kvalificerad tjänst för bevarande av kvalificerade elektroniska underskrifter

Av artikel 34 i förordningen följer att en kvalificerad tjänst för bevarande av kvalificerade elektroniska signaturer endast får tillhandahållas av en kvalificerad tillhandahållare av betrodda tjänster. Denna tillhandahållare ska använda tekniker och förfaranden som gör det möjligt att förlänga den kvalificerade elektroniska underskriftens tillförlitlighet utöver perioden för teknisk giltighet.

Kommissionen får ta fram genomförandeakter som refererar till standarder för kvalificerade tjänster för bevarande av kvalificerade elektroniska underskrifter. Kommissionen har ännu inte inlett arbetet med genomförandeakter på detta område.

6.3.1 Lämpliga standarder

PTS anser att EN 319 521 kan vara en lämplig standard för tillhandahållare av kvalificerade tjänster för bevarande av kvalificerade elektroniska underskrifter.

6.4 Kvalificerade elektroniska tidsstämplingar

Enligt artikel 42 i förordningen ska kvalificerade elektroniska tidsstämplingar binda datum och tid till uppgifter på ett sådant sätt att förändringar kan upptäckas. Tidsstämplingstjänsten ska basera sig på en korrekt tidkälla som är kopplad till samordnad universal tid (UTC). Tidsstämpeln ska vara undertecknad med en avancerad elektronisk underskrift eller stämpel från den kvalificerade tillhandahållaren alternativt genom en annan metod som ger likvärdigt skydd.

Kommissionen får ta fram genomförandeakter som refererar till standarder för bindning av datum och tidpunkt till uppgifter och för korrekta tidkällor. Detta arbete är ännu inte påbörjat.

6.4.1 Lämpliga standarder

I avvaktan på att kommissionen tar fram genomförandeakter anser PTS att lämplig standard för krav på tillhandahållare av elektroniska tidsstämplingar kan vara EN 319 421.

6.5 Kvalificerade elektroniska tjänster för rekommenderade leveranser

Enligt artikel 44 i förordningen ska kvalificerade elektroniska tjänster för rekommenderade leveranser tillhandahållas av en eller flera kvalificerade tillhandahållare av betrodda tjänster. De förstnämnda tjänsterna ska med hög grad av tillförlitlighet säkerställa avsändarens identitet. De ska säkerställa adressatens identitet innan uppgifterna levereras. Avsändandet och mottagandet av uppgifter ska säkerställas genom en avancerad elektronisk[19] underskrift eller en avancerad elektronisk stämpel[20] från en kvalificerad tillhandahållare av betrodda tjänster på ett sätt som utesluter möjligheten att uppgifterna ändras utan att det går att upptäcka. Eventuella ändringar av de uppgifter som behövs för att sända eller ta emot uppgifterna ska tydligt anges för uppgifternas avsändare och adressat. Datumet och tidpunkten för avsändande, mottagande och eventuella ändringar av uppgifter måste anges genom en kvalificerad elektronisk tidsstämpling.

Kommissionen får enligt artikel 44.2 ta fram genomförandeakter som refererar till standarder för processer för att sända och ta emot uppgifter.

[19] Underskrift i enlighet med artikel 26.
[20] Stämpel i enlighet med artikel 36.

Kommissionen har ännu inte inlett arbetet med genomförandeakter på detta område.

6.5.1 Lämpliga standarder

I avvaktan på att kommissionen tar fram genomförandeakter anser PTS att lämplig standard för krav på tillhandahållare av kvalificerade tjänster för rekommenderade leveranser på längre sikt kan vara EN 319 511. Den europeiska normen är ännu inte publicerad och i avvaktan på att den fastställs kan ETSI TS 102 640-3 vara en lämplig standard att använda.

6.6 Kvalificerade certifikat för autentisering av webbplatser

Enligt artikel 45 ska kvalificerade certifikat för autentisering uppfylla kraven i bilaga IV i förordningen.

Kommissionen får ta fram genomförandeakter som refererar till standarder för kvalificerade certifikat för autentisering av webbplatser. Arbetet med genomförandeakter på detta område har ännu inte inletts.

6.6.1 Lämpliga standarder

Det finns flera olika standarder för certifikatformat. PTS anser däremot att lämpliga standarder för utfärdare av kvalificerade certifikat, i likhet med utfärdande av kvalificerade certifikat för underskrifter och stämplar, för autentisering av webbplatser kan vara EN 319 411-1 och EN 319 411-2.

7 Krav på tillförlitliga IT-system och kvalificerade anordningar för underskrifter och stämplar

I eIDAS-förordningen ställs krav på att kvalificerade tillhandahållare av betrodda tjänster använder tillförlitliga IT-system. För att en kvalificerad underskrift eller stämpel ska kunna skapas krävs det att en certifierad anordning används.

7.1 Tillförlitliga IT-system

En kvalificerad tillhandahållare som tillhandahåller kvalificerade betrodda tjänster ska använda tillförlitliga system och produkter i sin verksamhet (artikel 24.2 e och f).

Kommissionen har rätt att ta fram genomförandeakter som refererar standarder för tillförlitliga system och produkter. Det arbetet har ännu inte inletts.

7.1.1 Lämpliga standarder

PTS konstaterar att det fanns motsvarande krav på tillförlitliga produkter, så kallade HSM (Hardware Security Module), som används för lagring eller generering av krypteringsnycklar inom ramen för det tidigare gällande signaturdirektivet. I avvaktan på att kommissionen tar fram genomförandeakter anser PTS att sådana HSM som är godkända enligt signaturdirektivet kan vara lämpliga att fortsätta användas för kvalificerade betrodda tjänster. PTS anser vidare att det kan vara lämpligt att använda de europeiska normer som har tagits fram för tillförlitliga IT-system: EN 419 211, EN 419 221, EN 419 231 och EN 419 241.

7.2 Anordningar för skapande av kvalificerade elektroniska underskrifter och stämplar

Enligt artikel 29 ska kraven på anordningar för skapande av kvalificerade elektroniska underskrifter uppfylla kraven i bilaga II i förordningen. Kommissionen har rätt att ta fram genomförandeakter som refererar till standarder för anordningar för skapande av kvalificerade elektroniska underskrifter. Arbetet med sådana genomförandeakter har inte inletts.

Kraven på de organ som ska certifiera anordningarna framgår av artikel 30. Det anges att certifieringen kan ske genom två olika metoder.

- Den första metoden bygger på en säkerhetsutvärdering som ska utföras enligt någon av de standarder för säkerhetsutvärdering av IT-produkter som fastställs genom kommissionens genomförandeakter.
- Den andra, alternativa metoden, får endast användas vid avsaknaden av sådana standarder eller under den tid en sådan säkerhetsutvärdering pågår. För att den alternativa metoden ska få användas krävs att den omfattar jämförbara säkerhetsnivåer samt att kommissionen underrättas.

Enligt övergångsreglerna i förordningens artikel 51 ska säkra anordningar för skapande av kvalificerade elektroniska signaturer i enlighet med signaturdirektivet ses som kvalificerade anordningar för skapande av kvalificerade elektroniska underskrifter.

Kommissionens genomförandeakt om standarder för säkerhetsutvärdering av IT-säkerhetsprodukter beslutades[21] och trädde i kraft den 16 maj 2016. Genomförandeakten anger att det för närvarande saknas standarder för anordningar som innebär att krypteringsnycklar lagras eller genereras för undertecknare på distans. Istället hänvisas till det alternativa förfarandet enligt förordningens artikel 30.3 b som innebär att en motsvarande säkerhetsnivå ska nås och att kommissionen ska underrättas om förfarandet.

Kommissionen har vidare rätt att ta fram delegerade akter, d.v.s. sådana akter som kommissionen själv kan besluta, om särskilda kriterier som ska uppfyllas av de utsedda certifieringsorganen (artikel 30.4). Arbete med dessa delegerade akter har inte inletts

I förordningens artikel 31 anges att medlemsländerna (i Sverige FMV/CSEC) ska notifiera kommissionen om anordningar som certifierats i medlemsländerna. Kommissionen ska utifrån notifieringarna upprätta en förteckning över certifierade anordningar.

Av artikel 39 följer att motsvarande krav på certifiering gäller för anordningar för elektroniska stämplar.

[21] 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 (Text av betydelse för EES).

7.2.1 Lämpliga standarder

Genomförandeakten innehåller referenser till standarder som ska användas för kvalificerade anordningar. Dessa standarder listas i bilagan till genomförandeakten.

8 Incidentrapportering

Enligt artikel 19 finns det en skyldighet för såväl kvalificerade som icke kvalificerade tillhandahållare av betrodda tjänster att rapportera de säkerhersincidenter eller integritetsförluster som i betydande omfattning påverkar den betrodda tjänst som tillhandahålls eller personuppgifter som används i tjänsten. Vidare ska tillhandahållarna underrätta fysiska och juridiska personer som inträffade incidenter haft negativ inverkan på. PTS som tillsynsmyndighet har en skyldighet att en gång om året lämna en sammanfattning av rapporterade incidenter till EU:s byrå för nät- och informationssäkerhet (ENISA).

Kommissionen har enligt artikel 19.4 b rätt att ta fram genomförandeakter som fastställer format och förfaranden, med tidsfrister för incidentrapporteringen, men har inte inlett det arbetet. ENISA har emellertid arbetat med rekommendationer om incidentrapporteringen. Rekommendationerna riktar sig till tillsynsmyndigheterna och avser vilka incidenter som tillsynsmyndigheterna är skyldiga att rapportera vidare till ENISA.

Åtminstone de incidenter som möter kraven i rekommendationen från ENISA[22] bör rapporteras till PTS. Tillhandahållarna behöver därför åtminstone rapportera de incidenter och de uppgifter som omfattas av avsnitt 3 i ENISA:s rekommendation. Incidentrapporterna behöver, utöver uppgifter om vem som rapporterar och kontaktuppgifter, innehålla uppgifter om:

- Påverkade betrodda tjänster
- När incidenten inträffade och avslutades
- Konsekvenserna av incidenten för tillhandahållaren, användare och förlitande parter
- Beskrivning av incidenten
    - Grundorsak och eventuella andra underliggande orsaker
    - Vilka tillgångar som påverkats av incidenten
- Vilka åtgärder som vidtagits för att hantera incidenten
- Åtgärder för att undvika att motsvarande incident inträffar igen
- Lärdomar och förbättringar efter inträffad incident

[22] Proposal for Article 19 Incident reporting - Proposal for an Incident reporting framework for eIDAS Article 19.

8.1 Rapportering till PTS

Incidentrapporter lämnas till PTS genom e-post till brevlådan incidentrapport@pts.se. PTS kommer kvittera alla mottagna incidentrapporter. E-posten kan krypteras med hjälp av S/MIME och certifikat med publik nyckel för e-postlådan kan hämtas från https://incident.pts.se/.

Mer information om incidentrapportering finns på PTS webbplats (www.pts.se/eIDAS).

9 Upphörande av status som kvalificerad tillhandahållare

I förordningen finns även krav på vad en kvalificerad tillhandahållare av betrodda tjänster ska göra om denne vill upphöra med sin verksamhet.

9.1 Information till PTS

En tillhandahållare är skyldig att informera PTS om alla ändringar av tillhandahållandet av kvalificerade betrodda tjänster och om tillhandahållaren önskar upphöra med verksamheten. Men redan vid uppstarten av verksamheten måste tillhandahållaren presentera en plan för verksamhetens upphörande till PTS för att kunna beviljas status som kvalificerad.

Reglerna om upphörande av verksamheten ska säkerställa kontinuiteten hos kvalificerade betrodda tjänster. Därför föreskrivs det om skyldigheter som gäller för de kvalificerade tillhandahållarna under relativt lång tid efter det att den kvalificerade betrodda tjänsten har upphört. Den som vill bli kvalificerad tillhandahållare av betrodda tjänster måste därför redan vid uppstarten av verksamheten ha en långsiktig plan och åtskilda resurser för det fall verksamheten skulle upphöra.

9.2 Bevarande av information

I artikel 24.2 h i eIDAS-förordningen anges att en kvalificerad tillhandahållare av betrodda tjänster ska registrera och hålla tillgänglig all relevant information om uppgifter som den kvalificerade tillhandahållaren av betrodda tjänster har utfärdat och tagit emot, under en lämplig tidsperiod. I artikeln anges vidare att detta särskilt ska ske för att vid rättsliga förfaranden kunna lägga fram bevis och för att säkerställa tjänsten kontinuitet. Slutligen anges att registreringen som tillhandahållaren måste göra får utföras elektroniskt.

Med relevant information enligt ovan avses bl.a. avtal och dokumentation som ligger till grund för varje enskilt utfärdande av ett certifikat. Situationer när det är viktigt att sådan information finns bevarad skulle exempelvis kunna vara att i rättsliga sammanhang kunna visa om en kvalificerad elektronisk underskrift eller stämpel har varit giltiga bakåt i tiden. Det skulle även kunna handla om hur en person identifierades när ett certifikat utfärdades av tillhandahållaren.

Mot bakgrund av ovanstående samt med hänsyn till den allmänna preskriptionstiden i svensk lag, bedömer PTS att en rimlig tid för att hålla de aktuella uppgifterna tillgängliga är åtminstone tio år från och med att giltighetstiden för det certifikat som uppgifterna är knutna till har upphört.

9.3 Offentliggöra återkallande av certifikat och informera förlitande parter

Av artikel 24.3 i eIDAS-förordningen följer att om en kvalificerad tillhandahållare som utfärdar kvalificerade certifikat, beslutar att återkalla ett certifikat ska återkallandet registreras i tillhandahållarens certifikatdatabas och offentliggöras. I artikeln anges att detta ska ske i god tid och inom 24 timmar efter mottagandet av begäran.

Av artikel 24.4 i samma förordning följer vidare att kvalificerade tillhandahållare i sådana situationer ska informera eventuella förlitande parter om att de kvalificerade certifikat som bolaget har utfärdat har status som återkallade. I artikeln anges även att informationen ska göras tillgänglig på ett automatiskt sätt som är tillförlitligt, kostnadsfritt och effektivt.

PTS bedömer att informationen bör hållas tillgänglig åtminstone till dess att det sista utfärdade certifikatets giltighetstid har löpt ut.

Bilaga 1

Beslutade genomförandeakter för betrodda tjänster

EU-kommissionen har fattat beslut om fyra genomförandeakter på området betrodda tjänster.

Förtroendemärke för kvalificerade tillhandahållare		
(EU) 2015/806	Artikel 23.3	Kommissionens genomförandeförordning om fastställande av specifikationer för utformningen av EU-förtroendemärket för kvalificerade betrodda tjänster.
Specifikationer för förteckningar över tillhandahållare		
(EU) 2015/1505	Artikel 22.5	Kommissionens genomförandebeslut om fastställande av tekniska minimispecifikationer och format rörande förteckningar över betrodda tjänsteleverantörer i enlighet med artikel 22.5.
Format för elektroniska underskrifter och stämplar		
(EU) 2015/1506	Artikel 27.5 Artikel 37.5	Kommissionens genomförandebeslut om fastställande av specifikationer rörande format för avancerade elektroniska underskrifter och avancerade elektroniska stämplar i enlighet med artiklarna 27.5 och 37.5.
Certifiering av anordningar för kvalificerade underskrifter och stämplar		
(EU) 2016/650	Artikel 30.3 Artikel 39.2	Kommissionens genomförandebeslut om fastställande av standarder för säkerhetsbedömning av kvalificerade anordningar för skapande av elektroniska underskrifter och stämplar enligt artiklarna 30.3 och 39.2.

Bilaga 2

Refererade standarder

Referens	Kort titel	Status	Kommentar
EN 319 102-1	Procedures for Creation and Validation of AdES Digital Signatures	Publicerad	Utfärdad av ETSI
EN 319 401	General Policy Requirements for TSPs Supporting	Publicerad	Utfärdad av ETSI
EN 319 403	Conformity Assessment of Trust Service Providers	Publicerad	Utfärdad av ETSI
EN 319 411-1	Policy requirements for certification authorities issuing public key certificates	Publicerad	Utfärdad av ETSI
EN 319 411-2	Policy requirements for certification authorities issuing QC	Publicerad	Utfärdad av ETSI
EN 319 421	Policy Requirements for TSPs providing Time-Stamping Services	Publicerad	Utfärdad av ETSI
EN 319 511	Policy and security requirements for registered electronic mail (REM) service providers	Under framtagande	Utfärdad av ETSI
ETSI TS 102 640-3	Information Security Policy Requirements for REM Management Domains	Publicerad	Alternativ standard i avvaktan på att EN 319 511 publiceras, utfärdad av ETSI
EN 319 521	Policy and security requirements for data preservation service providers	Under framtagande	Utfärdad av ETSI

Referens	Kort titel	Status	Kommentar
EN 419 211	Protection Profiles for secure signature creation devices; Part 1–6	Publicerad	Utfärdad av CEN
EN 419 221	Security requirements for trustworthy systems managing certificates for electronic signatures	Publicerad	Utfärdad av CEN
EN 419 231	Security requirements for trustworthy systems supporting timestamping	Publicerad	Utfärdad av CEN
EN 419 241	Security requirements for trustworthy systems supporting server signing (signature generation services)	Publicerad	Utfärdad av CEN