Promemoria

Kompletterande bestämmelser till EU-förordningen om elektronisk identifiering

Innehållsförteckning

1 Promemorians huvudsakliga innehåll

I promemorian lämnas förslag till de lagändringar som behövs för att komplettera Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden. En ny lag med kompletterande bestämmelser till EU-förordningen om elektronisk identifiering föreslås. Dessutom föreslås att lagen (2000:832) om kvalificerade elektroniska signaturer ska upphävas. Detta föranleder vidare följdändringar i ett antal lagar.

Lagändringarna föreslås träda i kraft den 1 juli 2016.

2 Förslag till lagtext

2.1 Förslag till lag med kompletterande bestämmelser till EU-förordningen om elektronisk identifiering

Inledande bestämmelser

1 § Denna lag kompletterar 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, i den ursprungliga lydelsen (EU-förordningen om elektronisk identifiering).

Termer och uttryck i lagen har samma betydelse som i EU-förordningen om elektronisk identifiering.

Granskning av kvalificerade tillhandahållare av betrodda tjänster

2 § Bestämmelser om ackreditering av sådana organ för bedömning av överensstämmelse som i enlighet med artikel 20 i EU-förordningen om elektronisk identifiering ska granska kvalificerade tillhandahållare av betrodda tjänster, finns i förordning (EG) nr 765/2008 om krav för ackreditering och marknadskontroll i samband med saluföring av produkter och upphävande av förordning (EEG) nr 229/93 och i lagen (2011:791) om ackreditering och teknisk kontroll.

Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om

1. krav för ackreditering av organ för bedömning av överensstämmelse,
2. rapportering av bedömningar av överensstämmelse, och
3. hur bedömningar av överensstämmelse ska göras.

Certifiering av anordningar

3 § Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om certifiering av anordningar för skapande av kvalificerade elektroniska underskrifter och anordningar för skapande av kvalificerade elektroniska stämplar.

Tillsyn

4 § Den myndighet som regeringen bestämmer (tillsynsmyndigheten) ska

1. fullgöra tillsynsorganets uppgifter enligt EU-förordningen om elektronisk identifiering och rättsakter som har meddelats med stöd av den förordningen, och
2. utöva tillsyn över denna lag och föreskrifter som har meddelats med stöd av lagen.

5 § Tillsynsmyndigheten har rätt att på begäran få de upplysningar och handlingar som behövs för tillsynen.

Tillsynsmyndigheten har också rätt att få tillträde till områden, lokaler och andra utrymmen där verksamhet som står under tillsyn bedrivs. Denna tillträdesrätt omfattar inte bostäder.

Tillsynsmyndigheten har rätt att få verkställighet hos Kronofogdemyndigheten av beslut som avser åtgärder enligt första och andra styckena. Då gäller bestämmelserna i utsökningsbalken om verkställighet av förpliktelser som inte avser betalningsskyldighet eller avhysning.

6 § Tillsynsmyndigheten får meddela de förelägganden och förbud som behövs för efterlevnaden av

1. EU-förordningen om elektronisk identifiering och rättsakter som har meddelats med stöd av den förordningen, och
2. denna lag och föreskrifter som har meddelats med stöd av lagen.

Förelägganden och förbud får förenas med vite.

Avgifter

7 § Regeringen eller, efter regeringens bemyndigande, tillsynsmyndigheten får meddela föreskrifter om skyldighet för tillhandahållare av betrodda tjänster att betala avgift för tillsynsmyndighetens verksamhet enligt denna lag.

Överklagande

8 § Tillsynsmyndighetens beslut enligt EU-förordningen om elektronisk identifiering och rättsakter som har meddelats med stöd av den förordningen, samt enligt denna lag och föreskrifter som har meddelats med stöd av lagen, får överklagas till allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

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

---

1. Denna lag träder i kraft den 1 juli 2016.
2. Genom lagen upphävs lagen (2000:832) om kvalificerade elektroniska signaturer.
3. Bestämmelserna om skadestånd i 14 och 15 §§ i den upphävda lagen ska fortsätta att gälla i fråga om skada som har åsamkats före upphävandet.

2.2 Förslag till lag om ändring i rättegångsbalken

Härigenom föreskrivs att 45 kap. 4 § rättegångsbalken ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*

45 kap.

4 §[1]

I stämningsansökan ska åklagaren uppge:

1. den tilltalade,
2. målsäganden, om någon sådan finns,
3. den brottsliga gärningen med uppgift om tid och plats för dess förövande och de övriga omständigheter som behövs för dess kännetecknande samt de bestämmelser som är tillämpliga,
4. de bevis som åberopas och vad som ska styrkas med varje bevis, samt
5. de omständigheter som gör domstolen behörig, om inte behörigheten framgår på annat sätt.

Vill åklagaren i samband med att åtalet väcks även väcka talan om enskilt anspråk enligt 22 kap. 2 §, ska åklagaren i ansökan lämna uppgift om anspråket och de omständigheter som det grundas på samt de bevis som åberopas och vad som ska styrkas med varje bevis.

Om den tilltalade är eller har varit anhållen eller häktad på grund av misstanke om brott som omfattas av åtalet, ska åklagaren ange detta i stämningsansökan. Uppgift ska dessutom lämnas om tiden för frihetsberövandet.

Har åklagaren några önskemål om hur målet ska handläggas, bör dessa anges i stämningsansökan.

Ansökan ska vara undertecknad av åklagaren. En ansökan som ges in på elektronisk väg ska vara undertecknad med en elektronisk *signatur enligt 2 § lagen (2000:832) om kvalificerade elektroniska signaturer* eller överföras på ett sätt som uppfyller motsvarande krav på säkerhet.	Ansökan ska vara undertecknad av åklagaren. En ansökan som ges in på elektronisk väg ska vara undertecknad med en *sådan avancerad* elektronisk *underskrift som avses i artikel 3 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, i den ursprungliga lydelsen,* eller överföras på ett sätt som uppfyller motsvarande krav på säkerhet.

[1] Senaste lydelse 2012:326.

Denna lag träder i kraft den 1 juli 2016.

2.3 Förslag till lag om ändring i socialförsäkringsbalken

Härigenom föreskrivs att 111 kap. 1, 5 och 6 §§ och rubriken närmast före 111 kap. 5 § socialförsäkringsbalken ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
111 kap.	
1 §	
I detta kapitel finns bestämmelser om	
– tillämpningsområdet i 2 §,	
– vad som är självbetjäningstjänster i 3 §,	
– när självbetjäningstjänster kan användas i 4 §,	
– elektronisk *signatur* i 5 och 6 §§, och	– elektronisk *underskrift* i 5 och 6 §§, och
– när en uppgift anses ha kommit in i 7 §.	
Elektronisk *signatur*	**Elektronisk *underskrift***
5 §	
En enskild som lämnar uppgifter i samband med att han eller hon använder en självbetjäningstjänst ska använda en sådan elektronisk *signatur* som avses i *2 § lagen (2000:832) om kvalificerade elektroniska signaturer*.	En enskild som lämnar uppgifter i samband med att han eller hon använder en självbetjäningstjänst ska använda en sådan elektronisk *underskrift* som avses i *artikel 3 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, i den ursprungliga lydelsen*.
Om det är fråga om att få tillgång till personuppgifter ska certifikat, till vilket en säker identifieringsfunktion är knuten, användas för kontroll av användarens identitet.	
6 §	
Om det finns någon annan metod än som avses i 5 § för identifiering eller skydd mot förvanskning av uppgifter som är tillräckligt säker med hänsyn till risken för integritetsintrång eller annan skada får dock den användas.	
Elektronisk *signatur* ska dock alltid användas när uppgifter ska lämnas på heder och samvete.	Elektronisk *underskrift* ska dock alltid användas när uppgifter ska lämnas på heder och samvete.

Denna lag träder i kraft den 1 juli 2016.

2.4 Lag om ändring i fastighetsbildningslagen (1970:988)

Härigenom föreskrivs att 4 kap. 8 § fastighetsbildningslagen (1970:988)[1] ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
4 kap.	
8 §[2]	
En ansökan om fastighetsbildning ska vara skriftlig och ges in till lantmäterimyndigheten. En muntlig ansökan som görs vid ett förrättningssammanträde ska dock godtas om den väckta frågan lämpligen kan prövas vid samma förrättning.	
Sökanden ska ange den åtgärd som han eller hon önskar genomförd samt uppge den eller de fastigheter som han eller hon för talan för. Om det kan anses skäligt att sökanden skaffar uppgifter om det eller om sökanden ändå har tillgång till uppgifterna, ska han eller hon också ange de andra fastigheter som saken angår samt namn på fastighetsägarna och på de innehavare av servitut, nyttjanderätt eller rätt till elektrisk kraft som kan beröras av åtgärden.	
En ansökan ska undertecknas eller signeras *elektroniskt* av sökanden eller sökandens ombud.	En ansökan ska undertecknas eller signeras *med en elektronisk underskrift* av sökanden eller sökandens ombud.
Till en ansökan ska sökanden bifoga de handlingar som han eller hon har och som är av betydelse för saken.	

Denna lag träder i kraft den 1 juli 2016.

[1] Lagen omtryckt 1992:1212.
[2] Senaste lydelse 2014:1342.

2.5 Förslag till lag om ändring i lagen (1978:599) om avbetalningsköp mellan näringsidkare m.fl.

Härigenom föreskrivs att 11 § lagen (1978:599) om avbetalningsköp mellan näringsidkare m.fl. ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
11 §[1]	
Säljaren får hos Kronofogdemyndigheten söka handräckning för att återta varan under förutsättning att det rörande avbetalningsköpet i en handling eller i någon annan läsbar och varaktig form som är tillgänglig för köparen har dokumenterats uppgifter om förbehållet om återtaganderätt, kontantpriset, kreditbeloppet, kreditavtalets löptid, kreditfordringen och tidpunkterna för betalning. Dokumentet ska ha undertecknats av köparen eller signerats av denne med en sådan avancerad elektronisk *signatur* som avses i *2 § lagen (2000:832) om kvalificerade elektroniska signaturer*.	Säljaren får hos Kronofogdemyndigheten söka handräckning för att återta varan under förutsättning att det rörande avbetalningsköpet i en handling eller i någon annan läsbar och varaktig form som är tillgänglig för köparen har dokumenterats uppgifter om förbehållet om återtaganderätt, kontantpriset, kreditbeloppet, kreditavtalets löptid, kreditfordringen och tidpunkterna för betalning. Dokumentet ska ha undertecknats av köparen eller signerats av denne med en sådan avancerad elektronisk *underskrift* som avses i *artikel 3 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, i den ursprungliga lydelsen*.

Denna lag träder i kraft den 1 juli 2016.

[1] Senaste lydelse 2012:67.

2.6 Förslag till lag om ändring i sparbankslagen (1987:619)

Härigenom föreskrivs att 1 kap. 4 § sparbankslagen (1987:619)[1] ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	1 kap.
	4 §[2]
En handling enligt denna lag som ska vara undertecknad får, om något annat inte anges, undertecknas med avancerad elektronisk *signatur enligt lagen (2000:832) om kvalificerade elektroniska signaturer*.	En handling enligt denna lag som ska vara undertecknad får, om något annat inte anges, undertecknas med *en sådan* avancerad elektronisk *underskrift som avses i artikel 3 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, i den ursprungliga lydelsen*.

Denna lag träder i kraft den 1 juli 2016.

[1] Lagen omtryckt 1996:1005.
[2] Senaste lydelse 2007:1460.

2.7 Förslag till lag om ändring i lagen (1987:667) om ekonomiska föreningar

Härigenom föreskrivs att 1 kap. 7 § lagen (1987:667) om ekonomiska föreningar ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
1 kap.	
7 §[1]	
En handling enligt denna lag som ska vara undertecknad får, om något annat inte anges, undertecknas med avancerad elektronisk *signatur enligt lagen (2000:832) om kvalificerade elektroniska signaturer*.	En handling enligt denna lag som ska vara undertecknad får, om något annat inte anges, undertecknas med *en sådan* avancerad elektronisk *underskrift som avses i artikel 3 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, i den ursprungliga lydelsen.*

Denna lag träder i kraft den 1 juli 2016.

[1] Senaste lydelse 2008:83.

2.8 Förslag till lag om ändring i bostadsrättslagen (1991:614)

Härigenom föreskrivs i fråga om bostadsrättslagen (1991:614)[1] att rubriken närmast före 1 kap. 9 § ska lyda ”Undertecknande med elektronisk underskrift”.

Denna lag träder i kraft den 1 juli 2016.

[1] Senaste lydelse av rubriken närmast före 1 kap. 9 § 2008:84.

2.9 Förslag till lag om ändring i stiftelselagen (1994:1220)

Härigenom föreskrivs att 1 kap. 9 § stiftelselagen (1994:1220) ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
1 kap.	
9 §[1]	
En handling enligt denna lag som ska vara undertecknad får, om något annat inte anges, undertecknas med avancerad elektronisk *signatur enligt lagen (2000:832) om kvalificerade elektroniska signaturer*.	En handling enligt denna lag som ska vara undertecknad får, om något annat inte anges, undertecknas med *en sådan* avancerad elektronisk *underskrift som avses i artikel 3 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, i den ursprungliga lydelsen.*

Denna lag träder i kraft den 1 juli 2016.

[1] Senaste lydelse 2008:86.

2.10 Förslag till lag om ändring i årsredovisningslagen (1995:1554)

Härigenom föreskrivs att 2 kap. 7 § och 8 kap. 3 a § årsredovisningslagen (1995:1554) ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
2 kap.	
7 §[1]	
I aktiebolag, ekonomiska föreningar och andra företag, som företräds av en styrelse, ska årsredovisningen skrivas under av samtliga styrelseledamöter. Om en verkställande direktör är utsedd, ska även denne skriva under årsredovisningen.	
I handelsbolag ska årsredovisningen skrivas under av samtliga obegränsat ansvariga delägare.	
I en gruppering enligt Europaparlamentets och rådets förordning (EG) nr 1082/2006 av den 5 juli 2006 om en europeisk gruppering för territoriellt samarbete (EGTS) ska årsredovisningen skrivas under av samtliga ledamöter i grupperingens församling samt av direktören.	
I stiftelser med anknuten förvaltning ska årsredovisningen skrivas under av förvaltaren eller, om ett handelsbolag är stiftelsens förvaltare, av samtliga bolagsmän som företräder bolaget.	
I övriga företag ska årsredovisningen skrivas under av den redovisningsskyldige eller dennes ställföreträdare.	
Om årsredovisningen upprättas i elektronisk form, ska den undertecknas med avancerad elektronisk *signatur enligt lagen (2000:832) om kvalificerade elektroniska signaturer*.	Om årsredovisningen upprättas i elektronisk form, ska den undertecknas med *en sådan* avancerad elektronisk *underskrift som avses i artikel 3 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, i den ursprungliga lydelsen*.
Om någon av dem som undertecknar årsredovisningen har anmält en avvikande mening, ska yttrandet fogas till redovisningen. I fall som avses i första stycket gäller detta dock endast om den avvikande meningen har antecknats till styrelsens protokoll.	
Årsredovisningen ska innehålla uppgift om den dag då den undertecknades.	

[1] Senaste lydelse 2009:702.

8 kap.

3 a §[2]

Handlingar som avses i 3 § får överföras elektroniskt till registreringsmyndigheten.

Ett bevis om fastställelse enligt 3 § 1 eller 2 får undertecknas med en elektronisk *signatur*.	Ett bevis om fastställelse enligt 3 § 1 eller 2 får undertecknas med en elektronisk *underskrift*.

Regeringen eller den myndighet som regeringen bestämmer meddelar närmare föreskrifter om

1. elektronisk överföring till registreringsmyndigheten av sådana handlingar som avses i 3 §,
2. bestyrkande av att en elektronisk kopia överensstämmer med originalet, och

3. den elektroniska *signaturen* enligt andra stycket.	3. den elektroniska *underskriften* enligt andra stycket.

Denna lag träder i kraft den 1 juli 2016.

[2] Senaste lydelse 2008:89.

2.11 Förslag till lag om ändring i lagen (1995:1559) om årsredovisning i kreditinstitut och värdepappersbolag

Härigenom föreskrivs att 8 kap. 5 a § lagen (1995:1559) om årsredovisning i kreditinstitut och värdepappersbolag ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
8 kap.	
5 a §[1]	
Handlingar som avses i 5 § får överföras elektroniskt till registreringsmyndigheten.	
Ett bevis om fastställelse enligt 5 § andra stycket får undertecknas med en elektronisk *signatur*.	Ett bevis om fastställelse enligt 5 § andra stycket får undertecknas med en elektronisk *underskrift*.
Regeringen eller den myndighet som regeringen bestämmer meddelar närmare föreskrifter om	
1. elektronisk överföring till registreringsmyndigheten av sådana handlingar som avses i 5 §,	
2. bestyrkande av att en elektronisk kopia överensstämmer med originalet, och	
3. den elektroniska *signaturen* enligt andra stycket.	3. den elektroniska *underskriften* enligt andra stycket.

Denna lag träder i kraft den 1 juli 2016.

[1] Senaste lydelse 2007:1461.

2.12 Förslag till lag om ändring i lagen (1995:1560) om årsredovisning i försäkringsföretag

Härigenom föreskrivs att 8 kap. 5 a § lagen (1995:1560) om årsredovisning i försäkringsföretag ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
8 kap.	
5 a §[1]	
Handlingar som avses i 5 § får överföras elektroniskt till registreringsmyndigheten.	
Ett bevis om fastställelse enligt 5 § andra stycket får undertecknas med en elektronisk *signatur*.	Ett bevis om fastställelse enligt 5 § andra stycket får undertecknas med en elektronisk *underskrift*.
Regeringen eller den myndighet som regeringen bestämmer meddelar närmare föreskrifter om	
1. elektronisk överföring till registreringsmyndigheten av sådana handlingar som avses i 5 §,	
2. bestyrkande av att en elektronisk kopia överensstämmer med originalet, och	
3. den elektroniska *signaturen* enligt andra stycket.	3. den elektroniska *underskriften* enligt andra stycket.

Denna lag träder i kraft den 1 juli 2016.

[1] Senaste lydelse 2007:1462.

2.13 Förslag till lag om ändring i lagen (1995:1570) om medlemsbanker

Härigenom föreskrivs att 1 kap. 7 § lagen (1995:1570) om medlemsbanker ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
1 kap.	
7 §[1]	
En handling enligt denna lag som ska vara undertecknad får, om något annat inte anges, undertecknas med avancerad elektronisk *signatur enligt lagen (2000:832) om kvalificerade elektroniska signaturer*.	En handling enligt denna lag som ska vara undertecknad får, om något annat inte anges, undertecknas med *en sådan* avancerad elektronisk *underskrift som avses i artikel 3 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, i den ursprungliga lydelsen*.

Denna lag träder i kraft den 1 juli 2016.

[1] Senaste lydelse 2007:1464.

2.14 Förslag till lag om ändring i revisionslagen (1999:1079)

Härigenom föreskrivs att 2 a § och rubriken närmast före 2 a § revisionslagen (1999:1079) ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
Undertecknande med elektronisk *signatur*	**Undertecknande med elektronisk *underskrift***
2 a §[1]	
En handling enligt denna lag som ska vara undertecknad får undertecknas med avancerad elektronisk *signatur enligt lagen (2000:832) om kvalificerade elektroniska signaturer*.	En handling enligt denna lag som ska vara undertecknad får undertecknas med *en sådan* avancerad elektronisk *underskrift som avses i artikel 3 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, i den ursprungliga lydelsen*.

Denna lag träder i kraft den 1 juli 2016.

[1] Senaste lydelse 2008:91.

2.15 Förslag till lag om ändring i lagen (2002:93) om kooperativ hyresrätt

Härigenom föreskrivs i fråga om lagen (2002:93) om kooperativ hyresrätt[1] att rubriken närmast före 1 kap. 6 § ska lyda ”Undertecknande med elektronisk underskrift”.

Denna lag träder i kraft den 1 juli 2016.

[1] Senaste lydelse av rubriken närmast före 1 kap. 6 § 2008:85.

2.16 Förslag till lag om ändring i lagen (2004:1199) om handel med utsläppsrätter

Härigenom föreskrivs att 4 kap. 5 § lagen (2004:1199) om handel med utsläppsrätter ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
4 kap.	
5 §[1]	
En ansökan om att öppna ett konto eller en ansökan om registrering i unionsregistret ska vara egenhändigt undertecknad av sökanden eller dennes ombud. En sådan ansökan får *signeras* och överföras elektroniskt.	En ansökan om att öppna ett konto eller en ansökan om registrering i unionsregistret ska vara egenhändigt undertecknad av sökanden eller dennes ombud. En sådan ansökan får *undertecknas* och överföras elektroniskt.

Denna lag träder i kraft den 1 juli 2016.

[1] Senaste lydelse 2011:1103.

2.17 Förslag till lag om ändring i aktiebolagslagen (2005:551)

Härigenom föreskrivs att 1 kap. 13 § och rubriken närmast före 1 kap. 13 § aktiebolagslagen (2005:551) ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
Undertecknande med elektronisk *signatur*	**Undertecknande med elektronisk *underskrift***
	1 kap.
	13 §[1]
En handling enligt denna lag som *skall* vara undertecknad får, om något annat inte anges, undertecknas med avancerad elektronisk *signatur enligt lagen (2000:832) om kvalificerade elektroniska signaturer*.	En handling enligt denna lag som *ska* vara undertecknad får, om något annat inte anges, undertecknas med *en sådan* avancerad elektronisk *underskrift som avses i artikel 3 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, i den ursprungliga lydelsen.*

Denna lag träder i kraft den 1 juli 2016.

[1] Senaste lydelse 2006:486.

2.18 Förslag till lag om ändring i lagen (2007:1091) om offentlig upphandling[1]

Härigenom föreskrivs att 2 kap. 10 § och 9 kap. 3 § lagen (2007:1091) om offentlig upphandling ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
2 kap.	
10 §[2]	
Med kontrakt avses ett skriftligt avtal med ekonomiska villkor som	
1. sluts mellan en eller flera upphandlande myndigheter och en eller flera leverantörer,	
2. avser utförande av byggentreprenad, leverans av varor eller tillhandahållande av tjänster, och	
3. undertecknas av parterna eller *signeras* av dem med en elektronisk *signatur*.	3. undertecknas av parterna eller *undertecknas* av dem med en elektronisk *underskrift*.
9 kap.	
3 §[3]	
Information om de specifikationer som är nödvändiga för elektronisk inlämning av anbudsansökningar och anbud, inbegripet kryptering, *skall* finnas tillgänglig för alla berörda parter.	Information om de specifikationer som är nödvändiga för elektronisk inlämning av anbudsansökningar och anbud, inbegripet kryptering, *ska* finnas tillgänglig för alla berörda parter.
En upphandlande myndighet får kräva att elektroniska anbud *skall* vara försedda med en avancerad elektronisk *signatur enligt lagen (2000:832) om kvalificerade elektroniska signaturer*.	En upphandlande myndighet får kräva att elektroniska anbud *ska* vara försedda med en *sådan* avancerad elektronisk *underskrift som avses i artikel 3 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, i den ursprungliga lydelsen*.
En upphandlande myndighet *skall* ha sådan utrustning att den elektroniskt kan ta emot anbudsan-	En upphandlande myndighet *ska* ha sådan utrustning att den elektroniskt kan ta emot anbudsansök-

[1] Ny lag om offentlig upphandling som ska träda i kraft den 1 april 2016 föreslagen i Ds 2014:25.
[2] Ingen motsvarighet till punkt 3 i förslaget till 1 kap. 9 § i den nya LOU, se Ds 2014:25 s. 18 och 298 f.
[3] En motsvarighet till andra stycket finns i förslaget till 12 kap. 9 § i den nya lagen, se Ds 2014:25 s. 80.

sökningar, anbud, ritningar och planer på ett säkert sätt. Utrustningen *skall* vara försedd med sådana säkerhetsanordningar att vissa uppgifter går att få fram, att bara behöriga personer *skall* få tillgång till uppgifterna och att det *skall* gå att spåra om någon obehörig har tagit del av uppgifterna.

ningar, anbud, ritningar och planer på ett säkert sätt. Utrustningen *ska* vara försedd med sådana säkerhetsanordningar att vissa uppgifter går att få fram, att bara behöriga personer *ska* få tillgång till uppgifterna och att det *ska* gå att spåra om någon obehörig har tagit del av uppgifterna.

Regeringen meddelar närmare föreskrifter om säkerhetsanordningarna.

Denna lag träder i kraft den 1 juli 2016.

2.19 Förslag till lag om ändring lagen (2007:1092) om upphandling inom områdena vatten, energi, transporter och posttjänster[1]

Härigenom föreskrivs att 2 kap. 10 § och 9 kap. 3 § lagen (2007:1092) om upphandling inom områdena vatten, energi, transporter och posttjänster ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
2 kap.	
10 §[2]	
Med kontrakt avses ett skriftligt avtal med ekonomiska villkor som	
1. sluts mellan en eller flera upphandlande myndigheter och en eller flera leverantörer,	
2. avser utförande av byggentreprenad, leverans av varor eller tillhandahållande av tjänster, och	
3. undertecknas av parterna eller *signeras* av dem med en elektronisk *signatur*.	3. undertecknas av parterna eller *undertecknas* av dem med en elektronisk *underskrift*.
9 kap.	
3 §[3]	
Information om de specifikationer som är nödvändiga för elektronisk inlämning av anbudsansökningar och anbud, inbegripet kryptering, *skall* finnas tillgänglig för alla berörda parter.	Information om de specifikationer som är nödvändiga för elektronisk inlämning av anbudsansökningar och anbud, inbegripet kryptering, *ska* finnas tillgänglig för alla berörda parter.
En upphandlande enhet får kräva att elektroniska anbud *skall* vara försedda med en avancerad elektronisk *signatur enligt lagen (2000:832) om kvalificerade elektroniska signaturer*.	En upphandlande enhet får kräva att elektroniska anbud *ska* vara försedda med en *sådan* avancerad elektronisk *underskrift som avses i artikel 3 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, i den ursprungliga lydelsen*.

[1] Ny lag om upphandling inom försörjningssektorerna som ska träda i kraft den 1 april 2016 föreslagen i Ds 2014:25.
[2] Ingen motsvarighet till punkt 3 i förslaget till 1 kap. 8 § i den nya lagen, se Ds 2014:25 s. 136 och 298 f.
[3] En motsvarighet till andra stycket finns i förslaget till 12 kap. 9 § i den nya lagen, se Ds 2014:25 s. 198.

En upphandlande enhet *skall* ha sådan utrustning att den elektroniskt kan ta emot anbudsansökningar, anbud, ritningar och planer på ett säkert sätt. Utrustningen *skall* vara försedd med sådana säkerhetsanordningar att vissa uppgifter går att få fram, att bara behöriga personer *skall* få tillgång till uppgifterna och att det *skall* gå att spåra om någon obehörig har tagit del av uppgifterna.	En upphandlande enhet *ska* ha sådan utrustning att den elektroniskt kan ta emot anbudsansökningar, anbud, ritningar och planer på ett säkert sätt. Utrustningen *ska* vara försedd med sådana säkerhetsanordningar att vissa uppgifter går att få fram, att bara behöriga personer *ska* få tillgång till uppgifterna och att det *ska* gå att spåra om någon obehörig har tagit del av uppgifterna.

Regeringen meddelar närmare föreskrifter om säkerhetsanordningarna.

Denna lag träder i kraft den 1 juli 2016.

2.20 Förslag till lag om ändring i lagen (2008:962) om valfrihetssystem

Härigenom föreskrivs att 2 kap. 2 § lagen (2008:962) om valfrihetssystem ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
2 kap.	
2 §	
Med kontrakt avses ett skriftligt avtal med ekonomiska villkor som	
1. sluts mellan en eller flera upphandlande myndigheter och en eller flera leverantörer,	
2. avser tillhandahållandet av tjänster, och	
3. undertecknas av parterna eller *signeras* av dem med en elektronisk *signatur*.	3. undertecknas av parterna eller *undertecknas* av dem med en elektronisk *underskrift*.
Kontraktet kan även innehålla andra villkor än ekonomiska.	

Denna lag träder i kraft den 1 juli 2016.

2.21 Förslag till lag om ändring i konsumentkreditlagen (2010:1846)

Härigenom föreskrivs att 43 § konsumentkreditlagen (2010:1846) ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
43 §[1]	
Kreditgivaren får hos Kronofogdemyndigheten söka handräckning för att återta varan under förutsättning att det rörande kreditköpet i en handling eller i någon annan läsbar och varaktig form som är tillgänglig för köparen har dokumenterats uppgifter om förbehållet om återtaganderätt, kontantpriset, kreditbeloppet, kreditavtalets löptid, kreditfordran och tidpunkterna för betalning. Dokumentet ska ha undertecknats av köparen eller signerats av denne med en sådan avancerad elektronisk *signatur* som avses i *2 § lagen (2000:832) om kvalificerade elektroniska signaturer*.	Kreditgivaren får hos Kronofogdemyndigheten söka handräckning för att återta varan under förutsättning att det rörande kreditköpet i en handling eller i någon annan läsbar och varaktig form som är tillgänglig för köparen har dokumenterats uppgifter om förbehållet om återtaganderätt, kontantpriset, kreditbeloppet, kreditavtalets löptid, kreditfordran och tidpunkterna för betalning. Dokumentet ska ha undertecknats av köparen eller signerats av denne med en sådan avancerad elektronisk *underskrift* som avses i *artikel 3 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, i den ursprungliga lydelsen*.

En ansökan om handräckning ska göras skriftligen. Det ska anges i ansökan hur stor del av kreditfordran som är obetald. Om kreditgivaren gör anspråk på dröjsmålsränta, ska det också uppges i ansökan vad kreditgivaren fordrar i den delen. En styrkt kopia av det dokument som anges i första stycket ska fogas till ansökan.

Denna lag träder i kraft den 1 juli 2016.

[1] Senaste lydelse 2012:69.

2.22 Förslag till lag om ändring i försäkringsrörelselagen (2010:2043)

Härigenom föreskrivs att 12 kap. 4 § försäkringsrörelselagen (2010:2043) ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
12 kap.	
4 §	
Bestämmelserna i 1 kap. 4–7 §§ lagen (1987:667) om ekonomiska föreningar om moderförening, dotterföretag, koncern och avancerad elektronisk *signatur* ska gälla för ömsesidiga försäkringsbolag.	Bestämmelserna i 1 kap. 4–7 §§ lagen (1987:667) om ekonomiska föreningar om moderförening, dotterföretag, koncern och avancerad elektronisk *underskrift* ska gälla för ömsesidiga försäkringsbolag.

Denna lag träder i kraft den 1 juli 2016.

2.23 Förslag till lag om ändring i lagen (2011:1029) om upphandling på försvars- och säkerhetsområdet

Härigenom föreskrivs att 2 kap. 14 § och 10 kap. 3 § lagen (2011:1029) om upphandling på försvars- och säkerhetsområdet ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
2 kap.	
14 §	
Med kontrakt avses ett skriftligt avtal med ekonomiska villkor som	
1. sluts mellan en eller flera upphandlande myndigheter eller enheter och en eller flera leverantörer,	
2. avser utförande av byggentreprenad, leverans av varor eller tillhandahållande av tjänster, och	
3. undertecknas av parterna eller *signeras* av dem med en elektronisk *signatur*.	3. undertecknas av parterna eller *undertecknas* av dem med en elektronisk *underskrift*.
10 kap.	
3 §	
Information om de specifikationer som är nödvändiga för elektronisk inlämning av anbudsansökningar och anbud, inbegripet kryptering, ska finnas tillgänglig för alla berörda parter.	
En upphandlande myndighet eller enhet får kräva att elektroniska anbud ska vara försedda med en avancerad elektronisk *signatur enligt lagen (2000:832) om kvalificerade elektroniska signaturer*.	En upphandlande myndighet eller enhet får kräva att elektroniska anbud ska vara försedda med en *sådan* avancerad elektronisk *underskrift som avses i artikel 3 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, i den ursprungliga lydelsen*.
En upphandlande myndighet eller enhet ska ha sådan utrustning att den elektroniskt kan ta emot anbudsansökningar, anbud, ritningar och planer på ett säkert sätt. Utrustningen ska vara försedd med sådana säkerhetsanordningar att vissa uppgifter går att få fram, att bara behöriga personer ska få tillgång till uppgifterna och att det ska gå att spåra om någon obehörig har tagit del av uppgifterna.	
Regeringen meddelar närmare föreskrifter om säkerhetsanordningarna.	

Denna lag träder i kraft den 1 juli 2016.

2.24 Lag om ändring i lagen (2014:105) om insyn i finansieringen av partier

Härigenom föreskrivs att 11 § lagen (2014:105) om insyn i finansieringen av partier ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
11 §	
En intäktsredovisning eller en anmälan enligt 10 § andra stycket ska skrivas under av den som är behörig företrädare för partiet på central nivå.	
Om en handling som avses i första stycket upprättas elektroniskt, ska den undertecknas med en avancerad elektronisk *signatur enligt lagen (2000:832) om kvalificerade elektroniska signaturer*.	Om en handling som avses i första stycket upprättas elektroniskt, ska den undertecknas med en *sådan* avancerad elektronisk *underskrift som avses i artikel 3 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, i den ursprungliga lydelsen*.

Denna lag träder i kraft den 1 juli 2016.

3 Ärendet

Europaparlamentet och rådet har antagit förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG (i fortsättningen benämnd EU-förordningen om elektronisk identifiering). Förordningens materiella delar ska börja tillämpas den 1 juli 2016. Förordningstexten finns i *bilaga 1*.

Under förhandlingarna upprättades och överlämnades en faktapromemoria till riksdagen (2011/12:FPM162).

I denna promemoria, som har utarbetats i Regeringskansliet, föreslås en ny lag med kompletterande bestämmelser till EU-förordningen om elektronisk identifiering. Genom förordningen upphävs Europaparlamentets och rådets direktiv 1999/93/EG av den 13 december 1999 om ett gemenskapsramverk för elektroniska signaturer. Direktivet har genomförts genom lagen (2000:832) om kvalificerade elektroniska signaturer. I promemorian föreslås att signaturlagen upphävs. Det lämnas också förslag till de följdändringar som detta föranleder.

4 Utgångspunkter

Elektronisk identifiering och elektronisk underskrift

Vår namnteckning är i det dagliga livet ofta nödvändig för att genomföra olika transaktioner i affärslivet, i förhållande till myndigheter och i privatlivet. I takt med att vi utför fler och fler transaktioner elektroniskt ökar behovet av elektroniska ersättare för våra namnteckningar. Det måste finnas säkra metoder för att identifiera privatpersoner och företag, och för att underteckna elektroniska handlingar, t.ex. ansökningar. Elektronisk identifiering och elektronisk underskrift är därför viktiga förutsättningar för att medborgare ska kunna använda digitala tjänster.

En elektronisk underskrift är uppgifter i elektronisk form som används för att kontrollera att innehållet i en elektronisk handling kommer från den som har undertecknat handlingen. En avancerad elektronisk underskrift är en elektronisk underskrift på vilken det ställs höga krav på säkerhet och kryptering. Det finns också kvalificerade elektroniska underskrifter med mycket höga sådana krav.

För det som numera, såsom i EU-förordningen om elektronisk identifiering, benämns elektronisk underskrift användes tidigare termen elektronisk signatur, bl.a. i lagen (2000:832) om kvalificerade elektroniska signaturer. Termen elektronisk signatur kommer från det s.k. signaturdirektivet 1999/93/EG. Med tiden har man dock kommit att allt mer ersätta den termen med termen elektronisk underskrift. Båda dessa termer har dock samma innebörd och de används synonymt i denna promemoria.

En e-legitimation är en elektronisk identitetshandling som kan användas för att identifiera innehavaren på elektronisk väg. E-legitimationen kan användas av enskilda och företrädare för företag eller myndigheter vid åtkomst till olika typer av e-tjänster. Den används också i andra

sammanhang, som vid informationsutbyte mellan myndigheter och internt i organisationer.

E-legitimationer ska vara enkla och trygga för användare och villkoren för offentlig sektor att använda tjänsterna ska vara enkla, förutsägbara och kostnadseffektiva. På så sätt kan e-legitimationer stödja utveckling av e-förvaltning och även underlätta användning av e-tjänster i samhället.

Sverige var tidigt ute med tjänster för elektronisk identifiering på internet och nådde snabbt en hög användning av e-legitimationer. I dag finns det mer än 7 miljoner e-legitimationer utfärdade i Sverige, vilket innebär att en stor andel av befolkningen använder eller har tillgång till e-legitimationer. Internationellt sett är detta en hög siffra. Under 2012 användes e-legitimationer för transaktioner i offentlig sektors e-tjänster ca 65 miljoner gånger. Användningen ökar snabbt. Motsvarande siffra för 2014 har beräknats till 98 miljoner, vilket alltså är en ökning med 50 procent på två år.

Elektronisk kommunikation och handel främjas av det finns tillgång till elektroniska underskrifter och andra s.k. betrodda tjänster, dvs. tjänster som gör det möjligt att skapa, kontrollera och validera t.ex. elektroniska underskrifter, elektroniska stämplar samt tjänster för rekommenderade leveranser, dvs. tjänster för elektronisk överföring av uppgifter mellan tredje män och vilka tillhandahåller bevis om de överförda uppgifternas hantering och skyddar dem mot risken för förlust, stöld, skada och otillåtna ändringar, och certifikat med anknytning till dessa tjänster. Kvalificerade elektroniska underskrifter kan också underlätta kontakten när invånare i Europeiska unionen behöver komma i kontakt med myndigheter i andra medlemsländer än där de är bosatta.

E-legitimationer i dag

De e-legitimationer som för närvarande används i den offentliga förvaltningens e-tjänster kan utfärdas antingen som en fil som innehavaren kan lagra på hårddisk (mjuk lagring) eller i form av en fysisk bärare (hård lagring), exempelvis ett s.k. smart kort. E-legitimationen består av en privat och en publik krypteringsnyckel med tillhörande elektroniskt certifikat. Den publika nyckeln finns i certifikatet och den privata nyckeln finns hos användaren. Det elektroniska certifikatet är en informationsstruktur som innehåller uppgifter som utfärdaren har valt att koppla till e-legitimationen, såsom närmare uppgifter om innehavaren, certifikatets unika nummer, vem som är utfärdare och den publika krypteringsnyckeln. Certifikatet är signerat av den som har utfärdat e-legitimationen.

Dagens e-legitimationer gör det möjligt för användaren att dels identifiera sig vid inloggning och liknande i e-tjänster, dels förse uppgifter med en elektronisk motsvarighet till en underskrift, dvs. en elektronisk underskrift.

För att ett system med e-legitimationer ska fungera krävs att samtliga tillhandahållare av e-tjänster uppfattar det som tillförlitligt. Detta säkerställs genom att det i avtal mellan tillhandahållare av e-tjänster, tillhandahållare av e-legitimationen och innehavare av e-legitimationer fastställs vilka regler var och en ska följa.

Svensk e-legitimation

Sedan 2011 har E-legitimationsnämnden regeringens uppdrag att stödja och samordna den offentliga sektorns behov av säkra metoder för elektronisk identifiering och signering. Nämndens uppdrag bygger på att den offentliga sektorn ska kunna använda konkurrerande marknadslösningar på e-legitimationsområdet. För att möta behovet har E-legitimationsnämnden utformat en infrastruktur för e-legitimationer, benämnd Svensk e-legitimation. Svensk e-legitimation ska göra det enkelt och säkert för medborgare och anställda att använda e-tjänster i offentlig förvaltning och privat sektor. Infrastrukturen är kopplad till tillämpning av valfrihetssystem, som ger den enskilde rätt att välja leverantör av e-legitimation bland de leverantörer som E-legitimationsnämnden har godkänt, se vidare avsnitt 6.

Den infrastruktur för elektronisk identifiering, en s.k. identitetsfederation, som E-legitimationsnämnden tillhandahåller består av ett regelverk som nämnden har tagit fram och som bl.a. innehåller bestämmelser om tillitsnivåer för e-legitimationer, servicenivåer för federationens tjänster, skadeståndsbestämmelser och avtalsreglerad möjlighet för nämnden att utföra kontroll och vid behov stänga av tjänster eller aktörer. Federationen innehåller även vissa interna tjänster som krävs för att systemet ska fungera. Myndigheter har möjlighet att avropa underskriftstjänster utifrån en kravspecifikation som E-legitimationsnämnden har tagit fram tillsammans med Kammarkollegiet.

I praktiken fungerar det så att myndigheter ger E-legitimationsnämnden i uppdrag att administrera sina valfrihetssystem. För myndigheternas räkning annonserar sedan E-legitimationsnämnden efter tjänster för elektronisk identifiering. De leverantörer som ansöker om att få delta och som uppfyller kraven ska godkännas av nämnden. Avtal tecknas därefter mellan myndigheten och leverantören genom nämndens försorg.

Det avtal som offentlig sektor använder i dag för att tillhandahålla tjänster för elektronisk identifiering löper ut den 1 juli 2016. Det kommer att ersättas av Svensk e-legitimation och E-legitimationsnämnden arbetar för närvarande med att ansluta myndigheter och leverantörer till den nya infrastrukturen.

Gränsöverskridande e-legitimationer och betrodda tjänster

Regeringens mål på området är att digitala tjänster ska vara enkla och säkra att använda. Det ska vara tryggt att använda statsförvaltningens digitala tjänster och det ska vara lätt för användaren att göra rätt. Rutinerna för identifiering och underskrifter i samband med användning av digitala tjänster bör fungera på ett enkelt sätt för användaren, oavsett om denna befinner sig i Sverige eller i något annat EU-land. Rutinerna måste dessutom bidra till en god säkerhetsnivå.

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. Hinder som identifierats handlar om fragmentering av den digitala marknaden, brist på interoperabilitet och ökande itbrottslighet. Det är därför viktigt att undanröja hindren för medborgarnas

möjligheter att utöva sina rättigheter och utnyttja fördelarna med en digital inre marknad och gränsöverskridande digitala tjänster.

I de flesta fall kan medborgare inte använda sina medel för elektronisk identifiering för att identifiera sig i andra medlemsstater inom EU därför att de nationella systemen för elektronisk identifiering inte erkänns 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. Exempelvis är ömsesidigt erkännande av elektronisk identifiering och autentisering en förutsättning för att gränsöverskridande sjukvård ska kunna bli verklighet för EU:s befolkning. Om t.ex. någon söker vård i en annan medlemsstat inom EU måste dennes patientjournal vara tillgänglig i behandlingslandet. Detta förutsätter robusta, säkra och tillförlitliga ramar för elektronisk identifiering.

För att möjliggöra säker åtkomst till gränsöverskridande digitala tjänster behöver dagens hinder för den gränsöverskridande användningen av elektronisk identifiering undanröjas. EU-förordningen om elektronisk identifiering syftar till att åstadkomma detta genom att dels fastställa villkor för att bygga förtroende för medlemsstaternas system för elektronisk identifiering på ett sätt som inte ingriper i nationella elektroniska identitetshanteringssystem och tillhörande infrastrukturer, dels genom att upprätta ett allmänt regelverk för användningen av betrodda tjänster i gränsöverskridande kontakter.

5 EU-förordningen om elektronisk identifiering

Inledande anmärkningar

I den svenska översättningen av EU-förordningen finns vissa tvetydigheter. I artikel 30 i förordningen behandlas certifiering av anordningar för skapande av kvalificerade elektroniska underskrifter. På andra ställen i förordningen anges dock att själva anordningen för att skapa en kvalificerad elektronisk underskrift eller stämpel ska vara kvalificerad, se t.ex. artikel 3 och 39 samt bilaga 2 och 3. I förordningen i övrigt görs skillnad mellan kvalificerade och icke-kvalificerade tjänster men inte mellan kvalificerade och icke-kvalificerade anordningar. I de engelska och franska språkversionerna används samma uttryckssätt på samtliga ställen (*qualified electronic signature creation device* och *qualified electronic seal creation device* respektive *dispositif de création de signature électronique qualifié* och *dispositif de création de cachet électronique qualifié*). Promemorian kommer därför att utgå från att det även i artikel 3 och 39 samt bilaga 2 och 3 är anordningar för skapande av kvalificerade elektroniska underskrifter respektive anordningar för skapande av kvalificerade elektroniska stämplar som avses.

Förordningens syfte och den inre marknaden (art. 1 och 4)

EU-förordningen om elektronisk identifiering syftar till att öka förtroendet för elektroniska transaktioner på den inre marknaden genom att tillhandahålla en gemensam grund för ett säkert elektroniskt samspel mellan företag, medborgare och offentliga myndigheter. Därigenom ska effektiviteten öka hos offentliga och privata e-tjänster samt i elektronisk affärsverksamhet och e-handel i unionen. Målet är att uppnå en tillräckligt hög nivå av säkerhet när det gäller medel för elektronisk identifiering och betrodda tjänster.

I förordningen slås principen om en inre marknad fast. Den som tillhandahåller betrodda tjänster i en medlemsstat får inte hindras att tillhandahålla sådana tjänster i en annan medlemsstat av skäl som omfattas av förordningen. Produkter och betrodda tjänster som överensstämmer med förordningen ska omfattas av fri rörlighet på den inre marknaden. Genom ömsesidigt erkännande av medel för elektronisk identifiering ska tillhandahållandet av tjänster över gränserna på den inre marknaden underlättas.

Tillämpningsområdet (art. 2)

Förordningen är tillämplig på system för elektronisk identifiering som en medlemsstat har anmält och på tillhandahållare av betrodda tjänster som är etablerade i unionen.

I förordningen anges under vilka villkor medlemsstater ska erkänna medel för elektronisk identifiering som omfattas av ett system för elektronisk identifiering som har anmälts av en annan medlemsstat. Det finns också bestämmelser om betrodda tjänster. Slutligen innehåller förordningen en rättslig ram för elektroniska underskrifter, elektroniska stämplar, elektroniska tidsstämplingar, elektroniska tjänster för rekommenderade leveranser, autentisering av webbplatser och för elektroniska dokument.

Förordningen gäller inte tillhandahållande av betrodda tjänster som till följd av nationell lagstiftning eller avtal mellan en avgränsad krets deltagare endast används inom slutna system. Den 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.

Elektronisk identifiering

Ömsesidigt erkännande (art. 6)

När det krävs användning av medel för elektronisk identifiering och autentisering för att få åtkomst till en tjänst som tillhandahålls av ett offentligt organ via internet, ska medel för elektronisk identifiering som har utfärdats i en annan medlemsstat erkännas för gränsöverskridande autentisering i den tjänsten. Detta förutsätter dock att medlet för elektronisk identifiering är utfärdat inom ramen för ett system för elektronisk identifiering som har anmälts av en medlemsstat och förts upp på en särskild förteckning som Europeiska kommissionen ska offentliggöra. Vidare ska medlet för elektronisk identifiering ha en säkerhetsnivå som är lika hög som eller högre än den säkerhetsnivå som krävs för åtkomst till internettjänsten och tjänsten ska kräva användning av säkerhetsnivån väsentlig

eller hög. Medlemsstaterna får dock även erkänna medel för elektronisk identifiering som motsvarar säkerhetsnivån låg.

Anmälan av system för elektronisk identifiering (art. 7 och 9)

System för elektronisk identifiering ska anmälas till kommissionen enligt ett särskilt förfarande. Kommissionen ska offentliggöra och löpande uppdatera en förteckning över anmälda system. Om det inträffar något som påverkar tillförlitligheten i systemets gränsöverskridande autentisering och problemet inte åtgärdas inom viss tid kan det leda till att systemet för elektronisk identifiering dras tillbaka.

Anmälan får ske om medlet för elektronisk identifiering inom systemet är utfärdat av, eller på uppdrag av, den anmälande medlemsstaten eller om det är utfärdat oberoende av den anmälande medlemsstaten men erkänt av denna. Medlet 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. Systemet för elektronisk identifiering och det medel för elektronisk identifiering som har utfärdats inom ramen för det ska uppfylla kraven för åtminstone en av de säkerhetsnivåer som anges i en genomförandeakt som ska beslutas av kommissionen. Vidare finns det krav som syftar till att säkerställa att medlet för elektronisk identifiering tilldelas rätt person. Den anmälande medlemsstaten ska dessutom se till att gränsöverskridande autentisering kan ske via internet. Offentliga organ ska ha kostnadsfri tillgång till sådan gränsöverskridande autentisering.

Säkerhetsnivåer (art. 8)

I de anmälda systemen ska säkerhetsnivåerna låg, väsentlig eller hög ha specificerats för de medel för elektronisk identifiering som utfärdas. För de olika säkerhetsnivåerna gäller vissa angivna kriterier som kommer att preciseras av kommissionen i genomförandeakter.

Säkerhetsincidenter (art. 10)

Om ett anmält system eller en autentisering utsätts för intrång eller delvis äventyras på ett sätt som påverkar tillförlitligheten i systemet ska medlemsstaten utan dröjsmål tillfälligt upphäva eller återkalla autentiseringen eller de berörda delarna av systemet och informera kommissionen och andra medlemsstater om detta. Om bristerna inte åtgärdas kan det ytterst leda till att det anmälda systemet måste dras tillbaka.

Ansvar (art. 11)

Såväl den anmälande medlemsstaten som den part som har utfärdat medel för elektronisk identifiering och den part som har hand om autentiseringsförfarandet kan bli skadeståndsansvariga om de inte uppfyller sina skyldigheter enligt förordningen. Skadeståndsbestämmelserna ska tillämpas i enlighet med nationell rätt.

Samarbete och interoperabilitet (art. 12)

I förordningen finns bestämmelser som syftar till att anmälda system ska fungera tillsammans med varandra. För det ändamålet ska det fastställas

en s.k. interoperabilitetsram som ska ha som mål att vara teknikneutral och inte diskriminera mellan olika nationella tekniska lösningar för elektronisk identifiering samt i möjlig mån följa europeiska och internationella standarder. Vidare finns det krav på integritetsskydd och på hur personuppgifter behandlas.

Medlemsstaterna ska samarbeta med varandra främst genom utbyte av information, erfarenhet och bästa praxis när det gäller system för elektronisk identifiering, särskilt i fråga om tekniska krav när det gäller interoperabilitet och säkerhetsnivåer.

Betrodda tjänster

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 eller certifikat med anknytning till dessa tjänster.

Ansvar (art. 13)

Tillhandahållare av betrodda tjänster är skadeståndsskyldiga om de avsiktligt eller på grund av oaktsamhet inte uppfyller kraven i förordningen. Bevisbördan när det gäller avsikten eller oaktsamheten hos en icke-kvalificerad tillhandahållare av betrodda tjänster ska ligga hos den fysiska eller juridiska person som åsamkats skada. När det gäller kvalificerade tillhandahållare av betrodda tjänster ska däremot dessa ansvara för skada såvida de inte bevisar att skadan har uppstått utan avsikt eller oaktsamhet hos denne.

Tillhandahållare av betrodda tjänster som i förväg informerar sina kunder om de begränsningar som gäller för användningen av deras tjänster ansvarar inte för skador som uppstår om dessa begränsningar överskrids.

Skadeståndsbestämmelserna ska tillämpas i enlighet med nationell rätt.

Sanktioner (art. 16)

Medlemsstaterna ska fastställa bestämmelser om de sanktioner som ska tillämpas vid överträdelser av förordningen. Sanktionerna ska vara effektiva, proportionella och avskräckande.

Tillsyn (art. 17 och 18)

Varje medlemsstat ska utse ett tillsynsorgan (i fortsättningen benämnt tillsynsmyndigheten) som ska ha de befogenheter och resurser som krävs för att kunna fullgöra sina uppgifter.

Tillsynsmyndigheten ska utöva tillsyn över att kvalificerade tillhandahållare av betrodda tjänster och de kvalificerade betrodda tjänster som de tillhandahåller uppfyller kraven i förordningen. Efter anmälan om att icke-kvalificerade tillhandahållare av betrodda tjänster eller de betrodda tjänster som de tillhandahåller inte uppfyller kraven i förordningen ska tillsynsmyndigheten vid behov även vidta åtgärder avseende dessa.

Tillsynsmyndigheten ska senast den 31 mars varje år överlämna en rapport till kommissionen om det föregående kalenderårets tillsynsverksamhet.

Tillsynsmyndigheterna i medlemsstaterna ska samarbeta med varandra i syfte att utbyta god praxis.

Säkerhetskrav (art. 19)

Tillhandahållare av betrodda tjänster ska vidta lämpliga tekniska och organisatoriska åtgärder för att hantera riskerna för säkerheten hos de betrodda tjänster som de tillhandahåller. Säkerhetsnivån ska, med tillämpning av den senaste tekniska utvecklingen, stå i proportion till risken. Tillsynsmyndigheten ska snabbt underrättas om mer allvarliga integritetsincidenter. Vid risk för negativ påverkan för fysiska eller juridiska personer ska även dessa underrättas. I vissa fall ska även allmänheten och andra medlemsstater underrättas.

Kvalificerade betrodda tjänster (art. 20–24)

Den som vill tillhandahålla kvalificerade betrodda tjänster ska anmäla detta till tillsynsmyndigheten och samtidigt lämna in en rapport med en överensstämmelsebedömning som har utfärdats av ett ackrediterat organ för bedömning av överensstämmelse. Tillsynsmyndigheten ska kontrollera om tillhandahållaren och dennes betrodda tjänster uppfyller förordningens krav. Om så är fallet ska myndigheten bevilja tillhandahållaren status som kvalificerad och se till att tillhandahållaren förs upp på en förteckning över kvalificerade tillhandahållare av betrodda tjänster. När tillhandahållaren förts upp på förteckningen får tjänsterna börja tillhandahållas.

Kvalificerade tillhandahållare av betrodda tjänster ska minst en gång vartannat år och på egen bekostnad granskas av ett ackrediterat organ för bedömning av överensstämmelse. Granskningen syftar till att kontrollera att förordningens krav uppfylls. En granskningsrapport ska överlämnas till tillsynsmyndigheten. Tillsynsmyndigheten kan också själv när som helst göra en granskning eller begära att ett ackrediterat organ för bedömning av överensstämmelse granskar verksamheten. Om brister påvisas och dessa inte åtgärdas kan det leda till att tillhandahållaren eller dennes betrodda tjänster blir av med sin status som kvalificerad.

Förteckningen över betrodda tjänstetillhandahållare ska vara offentlig och innehålla uppgifter om kvalificerade tillhandahållare av betrodda tjänster och om de kvalificerade betrodda tjänster som dessa tillhandahåller. En elektroniskt undertecknad eller förseglad version av förteckningen ska också offentliggöras i en form som lämpar sig för automatiserad behandling. Kommissionen ska göra medlemsstaternas förteckningar tillgängliga för allmänheten.

En kvalificerad tillhandahållare av betrodda tjänster får använda sig av en förtroendemärkning på EU-nivå för sina kvalificerade betrodda tjänster.

För kvalificerade tillhandahållare av betrodda tjänster gäller särskilda krav på kontroll av identiteten hos den till vilken ett kvalificerat certifikat utfärdas, på personalens utbildning och kunskaper, på ekonomin, på information om villkor för användning av tjänsten, på teknisk säkerhet

och tillförlitlighet hos system, på tillförlitliga system för lagring av och tillgång till uppgifter samt kontroll av uppgifternas äkthet, på registrering och tillhandahållande av uppgifter som har utfärdats och tagits emot, på löpande planering för att kunna garantera tjänstens kontinuitet i fall av verksamhetens upphörande och på att, då det är fråga om kvalificerade tillhandahållare av betrodda tjänster som utfärdar kvalificerade certifikat, upprätta och uppdatera en certifikatdatabas.

Återkallelse av ett kvalificerat certifikat ska registreras i certifikatdatabasen och offentliggöras inom 24 timmar. Återkallelsen ska gälla från offentliggörandet.

Elektroniska underskrifter (art. 25–34)

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. En kvalificerad elektronisk underskrift ska ha samma rättsliga verkan som en handskriven underskrift.

En kvalificerad elektronisk underskrift som är baserad på ett kvalificerat certifikat som har utfärdats i en medlemsstat ska erkännas som en kvalificerad elektronisk underskrift i alla andra medlemsstater.

För en avancerad elektronisk underskrift gäller ett antal krav. Den ska vara unikt knuten till undertecknaren, undertecknaren ska kunna identifieras genom den, 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 och 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.

Om en medlemsstat kräver en avancerad elektronisk underskrift, eller en avancerad elektronisk underskrift som är baserad på ett kvalificerat certifikat, för användningen av en e-tjänst hos ett offentligt organ ska medlemsstaten erkänna underskrifter i de format som anges i genomförandeakter som kommissionen ska besluta.

För gränsöverskridande användning av nättjänster som erbjuds av ett offentligt organ får det inte krävas en elektronisk underskrift med en högre säkerhetsnivå än den som gäller för kvalificerade elektroniska underskrifter.

Kvalificerade certifikat för elektroniska underskrifter ska uppfylla vissa ytterligare krav när det gäller certifikatens innehåll och utformning samt information om certifikaten. Kommissionen får genom genomförandeakter fastställa referensnummer till standarder för kvalificerade certifikat för elektroniska underskrifter. Ett certifikat som uppfyller sådana standarder ska förutsättas överensstämma med kraven för kvalificerade certifikat.

Medlemsstaterna får fastställa nationella bestämmelser för tillfälligt upphävande av ett kvalificerat certifikat för elektroniska underskrifter. Medan ett certifikat är tillfälligt upphävt så ska det vara ogiltigt. Upphävandetiden ska tydligt anges i certifikatdatabasen och certifikatets status som upphävt ska under den tiden framgå i den tjänst som tillhandahåller information om certifikatets status.

En kvalificerad elektronisk underskrift är en avancerad elektronisk underskrift som är skapad med hjälp av en anordning för skapande av kvalificerade elektroniska underskrifter och som är baserad på ett kvalificerat certifikat för elektroniska underskrifter. För anordningar för skapande av kvalificerade elektroniska underskrifter gäller extra höga säkerhetskrav. Överensstämmelsen med dessa krav ska certifieras av lämpliga offentliga eller privata organ som utses av medlemsstaterna. Kommissionen får genom genomförandeakter fastställa referensnummer till standarder för sådana anordningar. Anordningar som uppfyller en sådan standard ska förutsättas uppfylla förordningens krav. Certifieringen ska bygga på ett förfarande för säkerhetsutvärdering som utförts i enlighet med en standard för säkerhetsbedömning av it-produkter som finns med i en förteckning som kommissionen ska upprätta.

Medlemsstaterna ska informera kommissionen om anordningar för skapande av kvalificerade elektroniska underskrifter som har certifierats och om anordningar som inte längre är certifierade. Kommissionen ska på grundval av denna information upprätta, offentliggöra och underhålla en förteckning över certifierade anordningar för skapande av kvalificerade elektroniska underskrifter.

Förordningen innehåller vidare krav på valideringsförfarandet för kvalificerade elektroniska underskrifter och på tjänster för bevarande av sådana underskrifter.

Elektroniska stämplar (art. 35–40)

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

En elektronisk stämpel får inte förvägras rättslig verkan eller giltighet som bevis vid rättsliga förfaranden enbart på grund av att stämpeln har elektronisk form eller att den inte uppfyller kraven för en kvalificerad elektronisk stämpel. En kvalificerad elektronisk stämpel ska omfattas av en presumtion om integritet hos de uppgifter som stämpeln är kopplad till och om att uppgifterna har korrekt ursprung.

En kvalificerad elektronisk stämpel som är baserad på ett kvalificerat certifikat som har utfärdats i en medlemsstat ska erkännas som en kvalificerad elektronisk stämpel i alla andra medlemsstater.

En avancerad elektronisk stämpel ska vara knuten uteslutande till skaparen av stämpeln och skaparen ska kunna identifieras genom den. Stämpeln ska vara skapad 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 och den ska vara kopplad till de uppgifter som den avser på ett sådant sätt att alla efterföljande ändringar av uppgifterna kan upptäckas.

Om en medlemsstat kräver en avancerad elektronisk stämpel, eller en sådan stämpel baserad på ett kvalificerat certifikat, för användningen av en nättjänst hos ett offentligt organ ska medlemsstaten erkänna stämplar i åtminstone de format som kommissionen anger i kommande genomförandeakter.

För gränsöverskridande användning av nättjänster som erbjuds av ett offentligt organ får det inte krävas elektroniska stämplar med högre säkerhetsnivå än den som gäller för kvalificerade elektroniska stämplar.

Kommissionen får genom genomförandeakter fastställa referensnummer till standarder för avancerade elektroniska stämplar. Stämplar som uppfyller sådana standarder ska förutsättas överensstämma med kraven på avancerade elektroniska stämplar i förordningen.

Kvalificerade certifikat för elektroniska stämplar ska uppfylla vissa ytterligare krav när det gäller innehåll, utformning och information. Certifikat som uppfyller sådana standarder som kommissionen har fastställt referensnummer till i genomförandeakter ska förutsättas överensstämma med kraven för kvalificerade certifikat.

Ett kvalificerat certifikat för en elektronisk stämpel som återkallas efter den ursprungliga aktiveringen ska förlora sin giltighet i och med återkallelsen.

Medlemsstaterna får fastställa nationella bestämmelser för tillfälligt upphävande av kvalificerade certifikat för elektroniska stämplar. Tillfälligt upphävda certifikat ska vara ogiltiga under upphävandetiden. Vidare ska upphävandetiden tydligt anges i certifikatdatabasen och certifikatets status som upphävt ska under denna tid framgå genom den tjänst som tillhandahåller information om certifikatets status.

Vidare finns regler om anordningar för skapande av kvalificerade elektroniska stämplar, om certifiering av sådana anordningar samt om offentliggörandet av en förteckning över vilka anordningar som har certifierats. Dessa regler motsvarar dem som gäller för kvalificerade elektroniska underskrifter. Även i fråga om validering och bevarande av kvalificerade elektroniska stämplar gäller samma regler som för kvalificerade elektroniska underskrifter.

Elektroniska tidsstämplingar (art. 41 och 42)

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.

En elektronisk tidsstämpling ska inte förvägras rättslig verkan eller giltighet som bevis vid rättsliga förfaranden enbart på grund av att den är i elektronisk form eller inte uppfyller kraven för en kvalificerad elektronisk tidsmärkning. En kvalificerad elektronisk tidsstämpling ska omfattas av en presumtion om att tidsangivelsen är korrekt och att integriteten är bevarad hos de uppgifter som datumet och tiden är kopplade till. En kvalificerad elektronisk tidsstämpling som utfärdats i en medlemsstat ska erkännas som en kvalificerad elektronisk tidsstämpling i alla medlemsstater.

För en kvalificerad elektronisk tidsstämpling gäller särskilda krav på att tidsangivelsen ska kunna bindas till uppgifter så att möjligheten att uppgifterna ändras utan att det går att upptäcka rimligtvis kan uteslutas, på att tidsangivelsen är grundad på en korrekt tidskälla och på att den är undertecknad med en avancerad elektronisk underskrift eller förseglad med en avancerad elektronisk stämpel från en kvalificerad tillhandahållare av betrodda tjänster eller genom en likvärdig metod.

Kommissionen får genom genomförandeakter fastställa referensnummer till standarder för att binda datum och tidpunkt till uppgifter och för

korrekta tidskällor. När sådana standarder följs ska det förutsättas att kraven i förordningen är uppfyllda.

Elektroniska tjänster för rekommenderade leveranser (art. 43 och 44)

En elektronisk tjänst för rekommenderad leverans 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.

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 för en kvalificerad elektronisk tjänst för rekommenderade leveranser.

Uppgifter som sänds och tas emot genom en kvalificerad elektronisk tjänst för rekommenderade leveranser ska omfattas av en presumtion om uppgifternas integritet, om att uppgifterna kommer från den identifierade avsändaren, tas emot av den identifierade adressaten samt om riktigheten i tidsangivelsen för avsändande respektive mottagande av uppgifterna som anges i tjänsten.

Kvalificerade elektroniska tjänster för rekommenderade leveranser ska uppfylla särskilda krav på vem som tillhandahåller dem, på säkerställande av avsändarens identitet innan uppgifterna levereras och på vilka åtgärder som ska vidtas för att utesluta 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 avsändaren och adressaten och datum samt tidpunkten för avsändande, mottagande och eventuella ändringar av uppgifter måste anges genom en kvalificerad elektronisk tidsstämpling.

Autentisering av webbplatser (art. 45)

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.

I förordningen finns vissa krav som kvalificerade certifikat för autentisering av webbplatser ska uppfylla.

Elektroniska dokument (art. 46)

Med elektroniska dokument avses ljud- och bildinspelningar och audiovisuella inspelningar samt annat innehåll som är lagrat i elektronisk form.

Elektroniska dokument får inte förvägras rättslig verkan eller giltighet som bevis vid rättsliga förfaranden enbart på grund av att de har elektronisk form.

Signaturdirektivet (art. 50 och 51)

Signaturdirektivet ska upphöra att gälla den 1 juli 2016.

Förordningen innehåller vissa övergångsbestämmelser när det gäller säkra anordningar för skapande av signaturer som överensstämmer med kraven i direktivet och kvalificerade certifikat som har utfärdats för fysis-

ka personer enligt direktivet, liksom för tillhandahållare av certifieringstjänster som utfärdar certifikat enligt direktivet och som vill bli kvalificerade tillhandahållare av betrodda tjänster enligt förordningen.

6 Nuvarande reglering

I svensk rätt saknas i stor utsträckning särskilda bestämmelser om elektronisk identifiering, betrodda tjänster, elektroniska stämplar, elektroniska tidsstämplingar, elektroniska tjänster för rekommenderade leveranser, autentisering av webbplatser och elektroniska dokument.

I fråga om elektroniska underskrifter finns bestämmelser i lagen (2000:832) om kvalificerade elektroniska signaturer (signaturlagen), som har tillkommit i syfte att genomföra signaturdirektivet. Det finns också i ett antal författningar bestämmelser om att handlingar som ska vara undertecknade får undertecknas med avancerade elektroniska signaturer enligt signaturlagen. Vidare förekommer det författningsbestämmelser som endast allmänt hänvisar till elektroniska signaturer utan angivande av att signaturen ska vara av en viss kvalitet.

När det gäller elektronisk identifiering finns viss författningsreglering i lagen (2013:311) om valfrihetssystem i fråga om tjänster för elektronisk identifiering.

Elektronisk identifiering

Det saknas författningsreglering som specifikt rör krav på medel för elektronisk identifiering eller på hur elektronisk identifiering ska gå till. Den offentliga förvaltningens behov av tjänster för elektronisk identifiering och underskrift har i stället tillgodosetts genom upphandling av gemensamma ramavtal. Det senaste ramavtalet (eID 2008) gällde till och med utgången av juni 2012. Avrop som gjordes innan dess kan gälla under fyra år.

Den 1 juli 2013 trädde lagen (2013:311) om valfrihetssystem i fråga om tjänster för elektronisk identifiering i kraft. Tillämpning av lagen är ett alternativ till upphandling enligt lagen (2007:1091) om offentlig upphandling. Lagen gäller när en upphandlande myndighet har beslutat att tillämpa valfrihetssystem i fråga om tjänster för elektronisk identifiering av enskilda i myndighetens elektroniska tjänster, har anslutit sig till ett system för säker elektronisk identifiering som tillhandahålls av E-legitimationsnämnden och uppdragit åt nämnden att i den upphandlande myndighetens namn administrera valfrihetssystemet.

Valfrihetssystem enligt lagen innebär att den enskilde har rätt att välja den leverantör som ska utföra tjänsten och som en upphandlande myndighet har godkänt och tecknat kontrakt med. En förutsättning för att kontrakt ska kunna tecknas är att leverantören uppfyller de krav som har fastställts i ett förfrågningsunderlag.

Lagen om valfrihetssystem i fråga om tjänster för elektronisk identifiering innehåller endast allmänna bestämmelser om annonsering och förfrågningsunderlag, ansökan, uteslutning av sökande, godkännande av

sökande och ingående av kontrakt, information, rättsmedel och tillsyn. Regleringen av de krav som ställs på medlen för elektronisk identifiering och på hur den elektroniska identifieringen ska gå till finns alltså inte i lagen utan framgår av det förfrågningsunderlag som ska finnas.

Elektroniska underskrifter

Signaturlagen

Signaturlagen innehåller bestämmelser om säkra anordningar för signaturframställning, om kvalificerade certifikat för elektroniska signaturer och om utfärdande av sådana certifikat.

Med en elektronisk signatur avses data i elektronisk form som är fogade till eller logiskt knutna till andra elektroniska data och som används för att kontrollera att innehållet härrör från den som framstår som utställare och att det inte har förvanskats. Lagen skiljer mellan avancerade och kvalificerade elektroniska signaturer. En avancerad elektronisk signatur är knuten uteslutande till en undertecknare, gör det möjligt att identifiera undertecknaren, är skapad med hjälpmedel som endast undertecknaren kontrollerar och är knuten till andra elektroniska data på ett sådant sätt att förvanskningar av dessa data kan upptäckas. En kvalificerad elektronisk signatur är en avancerad elektronisk signatur som är baserad på ett kvalificerat certifikat och som är skapad av en säker anordning för signaturframställning.

I signaturlagen anges vilka krav som säkra anordningar för signaturframställning ska uppfylla (3–5 §§). Kraven på anordningarna ska anses uppfyllda för maskin- eller programvara som överensstämmer med sådana standarder för produkter för elektroniska signaturer som Europeiska kommissionen har fastställt och offentliggjort referensnummer till i Europeiska unionens officiella tidning.

Vidare anges i lagen att ett certifikat endast får kallas kvalificerat om det är utfärdat för viss tid av en certifikatutfärdare som uppfyller angivna krav och om det innehåller vissa angivna uppgifter (6 § första stycket). Det ställs också upp ett antal krav på hur den som utfärdar kvalificerade certifikat ska bedriva sin verksamhet (9–11 §§).

Innan en certifikatutfärdare ingår avtal om att utfärda ett kvalificerat certifikat ska certifikatutfärdaren skriftligen och på ett lättbegripligt språk informera motparten om begränsningar och andra villkor för användning av certifikatet, om frivillig ackreditering eller certifiering och om förfaranden för klagomål och avgörande av tvister (12 §).

En certifikatutfärdare som utfärdar kvalificerade certifikat till allmänheten ska ersätta den skada som åsamkats den som förlitat sig på certifikatet, om skadan uppkommit genom att certifikatutfärdaren inte har uppfyllt kraven i 6 § första stycket eller 10 § eller om certifikatet vid utfärdandet innehöll felaktiga uppgifter. En certifikatutfärdare som kan visa att skadan inte har orsakats av vårdslöshet hos utfärdaren själv undgår dock ersättningsskyldighet. Certifikatutfärdaren är inte heller ersättningsskyldig för en skada som härrör från att ett kvalificerat certifikat använts i strid med begränsningar som gäller användningsområde eller transaktionsbelopp och som tydligt angetts i certifikatet (14 §).

I signaturlagen anges också att om det i lag eller annan författning ställs krav på egenhändig underskrift eller motsvarande och om det är

tillåtet att uppfylla kravet med elektroniska medel, ska en kvalificerad elektronisk signatur anses uppfylla kravet (17 §). Vid kommunikation med eller mellan myndigheter kan dock användningen av elektroniska signaturer vara förenad med ytterligare krav.

Post- och telestyrelsen (PTS) är tillsynsmyndighet enligt signaturlagen. Den som avser att utfärda kvalificerade certifikat till allmänheten ska anmäla det till PTS. I dagsläget har tre utfärdare gjort en sådan anmälan.

Övrig lagstiftning

Lagbestämmelser som innebär att handlingar som ska vara undertecknade får undertecknas med avancerade elektroniska signaturer enligt signaturlagen finns i

– 45 kap. 4 § rättegångsbalken,
– 111 kap. 5 § socialförsäkringsbalken,
– 11 § lagen (1978:599) om avbetalningsköp mellan näringsidkare m.fl.,
– 1 kap. 4 § sparbankslagen (1987:619),
– 1 kap. 7 § lagen (1987:667) om ekonomiska föreningar,
– 1 kap. 9 § stiftelselagen (1994:1220),
– 2 kap. 7 § årsredovisningslagen (1995:1554),
– 1 kap. 7 § lagen (1995:1570) om medlemsbanker,
– 2 a § revisionslagen (1999:1079),
– 1 kap. 13 § aktiebolagslagen (2005:551),
– 9 kap. 3 § lagen (2007:1091) om offentlig upphandling,
– 9 kap. 3 § lagen (2007:1092) om upphandling inom områdena vatten, energi, transporter och posttjänster,
– 43 § konsumentkreditlagen (2010:1846), och
– 10 kap. 3 § lagen (2011:1029) om upphandling på försvars- och säkerhetsområdet.

Lagbestämmelser som endast allmänt hänvisar till elektroniska signaturer utan angivande av att signaturen ska vara av en viss kvalitet finns i

– 1 kap. 9 § bostadsrättslagen (1991:614),
– 8 kap. 3 a § årsredovisningslagen (1995:1554),
– 8 kap. 5 a § lagen (1995:1559) om årsredovisning i kreditinstitut och värdepappersbolag,
– 8 kap. 5 a § lagen (1995:1560) om årsredovisning i försäkringsföretag,
– 1 kap. 6 § lagen (2002:93) om kooperativ hyresrätt,
– 2 kap. 10 § lagen (2007:1091) om offentlig upphandling,
– 2 kap. 10 § lagen (2007:1092) om upphandling inom områdena vatten, energi, transporter och posttjänster,
– 2 kap. 2 § lagen (2008:962) om valfrihetssystem,
– 111 kap. 1 och 6 §§ socialförsäkringsbalken,
– 12 kap. 4 § försäkringsrörelselagen (2010:2043),
– 2 kap. 14 § lagen (2011:1029) om upphandling på försvars- och säkerhetsområdet, och
– 11 § lagen (2014:105) om finansiering av partier.

Det saknas lagstiftning som innebär att handlingar ska vara undertecknade med kvalificerade elektroniska signaturer.

7 Kompletterande bestämmelser till EU-förordningen

7.1 En ny lag införs

Förslag: De nationella bestämmelser som behövs för att komplettera EU-förordningen ska samlas i en ny lag med kompletterande bestämmelser till EU-förordningen om elektronisk identifiering.

Skälen för förslaget: En EU-förordning är bindande i sin helhet och direkt tillämplig i varje medlemsstat. En sådan rättsakt varken ska eller får genomföras i eller omvandlas till nationell rätt. Sverige får alltså inte vidta några särskilda åtgärder för att införliva de materiella bestämmelserna i EU-förordningen om elektronisk identifiering med nationell rätt. Det är endast då svensk rätt kan anses strida mot förordningen, då förordningen föreskriver en skyldighet eller möjlighet att vidta lagstiftningsåtgärder på det nationella planet eller då det behövs andra nationella åtgärder till stöd för förordningens syfte som ändringar i svensk rätt aktualiseras.

EU-förordningen om elektronisk identifiering förutsätter att medlemsstaterna vidtar vissa nationella åtgärder, t.ex. att utse tillsynsorgan (i fortsättningen benämnt tillsynsmyndighet) och att införa bestämmelser om effektiva, proportionella och avskräckande sanktioner för överträdelser av förordningen. Förordningen kräver i vissa avseenden kompletterande lagstiftning medan den i andra delar ger medlemsstaterna möjlighet att vidta åtgärder, se vidare följande avsnitt.

Som redovisats i avsnitt 6 finns det i signaturlagen vissa lagbestämmelser på området. Den lagen har dock tillkommit för att genomföra signaturdirektivet och den täcker endast en del av det område som EU-förordningen omfattar. Enligt artikel 50 i EU-förordningen upphör signaturdirektivet att gälla den 1 juli 2016, se avsnitt 3. Det föreslås därför i avsnitt 8.1 att signaturlagen ska upphävas. Eftersom det inte i någon annan lag finns bestämmelser som reglerar något av de ämnen som EU-förordningen omfattar bör de lagbestämmelser som är nödvändiga till följd av EU-förordningen samlas i en ny lag med kompletterande bestämmelser till EU-förordningen om elektronisk identifiering.

7.2 Granskning av kvalificerade tillhandahållare av betrodda tjänster

Förslag: I lagen ska det anges att bestämmelser om ackreditering av sådana organ för bedömning av överensstämmelse som ska granska kvalificerade tillhandahållare av betrodda tjänster finns i förordning (EG) nr 765/2008 och i lagen (2011:791) om ackreditering och teknisk kontroll. Regeringen eller den myndighet som regeringen bestämmer ska få meddela föreskrifter om krav för ackreditering av sådana organ, om rapportering av bedömningar av överensstämmelse och om hur bedömningar av överensstämmelse ska göras.

Bedömning: Tillsynsmyndigheten bör meddela de föreskrifter som behövs.

Skälen för förslaget och bedömningen: Enligt artikel 20 jämfört med artikel 2.18 i EU-förordningen om elektronisk identifiering ska kvalificerade tillhandahållare av betrodda tjänster minst en gång vartannat år granskas av ett organ för bedömning av överensstämmelse som är ackrediterat enligt Europaparlamentets och rådets förordning (EG) nr 765/2008. Vidare har tillsynsmyndigheten möjlighet att när som helst begära att en sådan granskning utförs. Granskningen syftar till att kontrollera att tjänstetillhandahållarna och deras betrodda tjänster uppfyller förordningens krav och den ska utmynna i en rapport med en bedömning av överensstämmelse som ska överlämnas till tillsynsmyndigheten.

I artikel 20 anges också att Europeiska kommissionen genom genomförandeakter får fastställa referensnummer till standarder för ackreditering av organ för bedömning av överensstämmelse, för rapporter om sådana bedömningar och för granskningsregler som ska följas vid bedömningarna.

Ackreditering enligt förordning (EG) nr 765/2008 innebär att ett nationellt ackrediteringsorgan förklarar att ett organ för bedömning av överensstämmelse uppfyller kraven i harmoniserade standarder och, i förekommande fall, ytterligare krav. I Sverige är Styrelsen för ackreditering och teknisk kontroll (Swedac) nationellt ackrediteringsorgan. Ett organ som vill bli ackrediterat måste lämna en ansökan till Swedac som prövar och bedömer om organet uppfyller de krav som ställs i förordning (EG) nr 765/2008, lagen (2011:791) om ackreditering och teknisk kontroll med tillhörande förordning samt föreskrifter som Swedac har meddelat. Organet måste också uppfylla de sektorsspecifika myndighetsföreskrifter eller andra krav som organet ska arbeta i enlighet med. Ackreditering beviljas i form av ett ackrediteringsintyg som gäller för viss tid eller tills vidare och som innehåller de villkor som gäller för ackrediteringen.

Det följer av EU-förordningen om elektronisk identifiering att ackreditering av organ för bedömning av överensstämmelse ska ske enligt förordning (EG) nr 765/2008. Kompletterande bestämmelser till den förordningen finns i lagen (2011:791) om ackreditering och teknisk kontroll. Lagen gäller i princip all ackreditering som Swedac utför, såväl sådan som är föreskriven i förordning (EG) nr 765/2008 som sådan som sker på annan grund. I och med att EU-förordningen om elektronisk identifiering anger att organen för bedömning av överensstämmelse ska vara ackredi-

terade enligt förordning (EG) nr 765/2008 finns det därför inget behov av att i den nya lagen ange att ackreditering ska ske på det sättet. Däremot bör det i den nya lagen införas en upplysningsbestämmelse om var det finns bestämmelser om ackreditering.

EU-förordningen om elektronisk identifiering innehåller inte några bestämmelser om hur ackrediteringen ska gå till, t.ex. när det gäller vilken kontrollform som ska användas, eller vilka krav som organen för bedömning av överensstämmelse ska uppfylla. Det saknas också bestämmelser om rapporteringen av bedömningar av överensstämmelse och om hur sådana bedömningar ska göras.

EU-förordningen syftar till en harmonisering av regler för betrodda tjänster och betrodda tjänster ska omfattas av fri rörlighet på den inre marknaden. För att kunna uppnå detta måste de krav som ställs på ackrediterade organ för bedömning av överensstämmelse och de regler som ska gälla för dessas verksamhet vara så enhetliga som möjligt inom unionen.

Som angetts ovan får kommissionen anta genomförandeakter som fastställer referensnummer till standarder som gäller ackreditering av organ för bedömning av överensstämmelse, rapporter om överensstämmelsebedömning och granskningsregler som organen för bedömning av överensstämmelse ska följa vid bedömningarna. Det är inte obligatoriskt för kommissionen att anta sådana genomförandeakter och det är i dagsläget oklart huruvida genomförandeakter kommer att finnas på plats den 1 juli 2016 när EU-förordningen ska börja tillämpas. I den mån det då saknas EU-rättslig reglering måste det införas nationell reglering i stället. Det kan också finnas behov av nationell reglering även om kommissionen utnyttjar möjligheten att anta genomförandeakter, antingen i form av kompletterande bestämmelser till genomförandeakterna eller närmare föreskrifter i vissa avseenden som inte omfattas av genomförandeakter. En sådan reglering blir med nödvändighet av teknisk och detaljerad natur och lämpar sig därför mindre väl att läggas fast i lag. Det bör i stället anges i lagen att regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om ackreditering av organ för bedömning av överensstämmelse, om rapportering av rapporter om bedömning av överensstämmelse och om hur bedömningar av överensstämmelse ska göras.

För att inte harmoniseringssträvandet ska äventyras är det viktigt att de föreskrifter som kan komma att behövas i så stor utsträckning som möjligt tar hänsyn till internationellt standardiseringsarbete.

Det finns ingen myndighet som för närvarande har i uppdrag att meddela de föreskrifter som kan aktualiseras. Det framstår som naturligt att den myndighet som utses till tillsynsmyndighet också får i uppdrag att meddela dessa föreskrifter. Frågan om val av tillsynsmyndighet behandlas nedan i avsnitt 7.8.3.

7.3 Certifiering av anordningar för skapande av kvalificerade elektroniska underskrifter m.m.

Förslag: Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om certifiering av anordningar för skapande av kvalificerade elektroniska underskrifter och anordningar för skapande av kvalificerade elektroniska stämplar.

Bedömning: Tillsynsmyndigheten bör meddela de föreskrifter som behövs.

Sveriges certifieringsorgan för it-säkerhet vid Försvarets materielverk bör utses till certifieringsorgan för anordningar för skapande av kvalificerade elektroniska underskrifter och för anordningar för skapande av kvalificerade elektroniska stämplar.

Skälen för förslaget och bedömningen: Enligt artikel 30 och 39 i EU-förordningen om elektronisk identifiering ska medlemsstaterna utse lämpliga offentliga eller privata organ som certifierar att anordningar för skapande av kvalificerade elektroniska underskrifter och anordningar för skapande av kvalificerade elektroniska stämplar överensstämmer med förordningens krav på sådana anordningar. Certifiering av sådana anordningar innebär att de har bedömts uppfylla särskilda krav som ställs i standarder eller andra normerande dokument.

Certifieringen ska bygga på ett förfarande för säkerhetsutvärdering som har utförts i enlighet med en standard för säkerhetsutvärdering av informationsteknikprodukter som finns med i en särskild förteckning som Europeiska kommissionen ska upprätta genom genomförandeakter. Det anges inte i förordningen inom vilken tid kommissionen ska anta sådana genomförandeakter. Vid avsaknad av sådana standarder eller medan en säkerhetsutvärdering pågår får enligt förordningen ett annat förfarande användas, om det omfattar jämförbara säkerhetsnivåer och kommissionen underrättas om förfarandet.

Bestämmelserna i EU-förordningen innebär att det blir obligatoriskt med certifiering av anordningar för skapande av kvalificerade elektroniska underskrifter och anordningar för skapande av kvalificerade elektroniska stämplar. Förutom att det anges i förordningen att certifiering ska ske och att den ska bygga på standarder för säkerhetsutvärdering som kommissionen anger i genomförandeakter saknas reglering av certifieringsförfarandet. Mot denna bakgrund kan det finnas behov av nationella föreskrifter om certifiering, dels i den mån genomförandeakter saknas eller behöver kompletteras, t.ex. med regler om förfarandet för säkerhetsutvärderingen, dels i fråga om vilket förfarande som ska användas medan en säkerhetsutvärdering pågår. Dessa tekniska och detaljerade föreskrifter behöver inte framgå av lagen. I stället bör det anges i lagen att regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om certifiering av anordningar för skapande av kvalificerade elektroniska underskrifter och anordningar för skapande av kvalificerade elektroniska stämplar.

Det finns ingen myndighet som för närvarande har i uppdrag att meddela de föreskrifter som kan aktualiseras. I likhet med vad som föreslagits i föregående avsnitt framstår det som naturligt att den myndighet

som utses till tillsynsmyndighet också får i uppdrag att meddela dessa föreskrifter. Frågan om val av tillsynsmyndighet behandlas i avsnitt 7.8.3.

Vilken myndighet bör ansvara för certifieringen?

Av artikel 30 i EU-förordningen framgår att Europeiska kommissionen har befogenhet att i delegerade akter fastställa särskilda kriterier som certifieringsorganen ska uppfylla. Några delegerade akter har ännu inte antagits. Antagandet av sådana rättsakter kan, beroende på de krav som ställs upp, påverka vilken myndighet som är mest lämpad att ansvara för certifieringen.

I skäl 55 till EU-förordningen anges att it-säkerhetscertifiering som bygger på internationella standarder såsom ISO 15408 och besläktade utvärderingsmetoder och arrangemang för ömsesidigt erkännande, är viktiga verktyg för att kontrollera säkerheten hos anordningar för skapande av kvalificerade elektroniska underskrifter och bör främjas. Det finns därför skäl att anta att den standarden kommer att föras upp på den förteckning som kommissionen ska upprätta enligt artikel 30 i förordningen.

I enlighet med 5 § förordningen (2007:854) med instruktion för Försvarets materielverk finns hos myndigheten ett särskilt certifieringsorgan, Sveriges certifieringsorgan för it-säkerhet (CSEC), som ska upprätta och driva en certifieringsordning för säkerhet i it-produkter och system. CSEC verkar som Sveriges nationella certifieringsorgan för it-säkerhet i produkter och system enligt standarden Common Criteria for Information Technology Security Evaluation (Common Criteria), som har beteckningen ISO/IEC 15408 och som används för kravställning och opartisk granskning av it-säkerhet. CSEC har blivit ackrediterat av Swedac för certifiering av it-säkerhet hos produkter, system och skyddsprofiler med stöd av ISO/IEC 15408, Common Criteria version 2.3 och Common Criteria version 3.1. CSEC tillämpar för närvarande också de standarder som Europeiska kommissionen har använt för att ställa krav på it-säkerhet och kryptering med stöd av signaturdirektivet. I nuläget framstår det därför som lämpligast att utse CSEC vid Försvarets materielverk att ansvara för certifiering av anordningar för skapande av kvalificerade elektroniska underskrifter och anordningar för skapande av kvalificerade elektroniska stämplar. Detta kan regleras i förordning.

7.4 Skadestånd

Bedömning: Det behövs inte några kompletterande bestämmelser till EU-förordningens bestämmelser om skadeståndsansvar.

Skälen för bedömningen: I artikel 13 i EU-förordningen finns bestämmelser om skadestånd. I punkt 1 anges att den som tillhandahåller betrodda tjänster ansvarar för skada som avsiktligt eller på grund av oaktsamhet åsamkas fysiska och juridiska personer genom att kraven i förordningen inte uppfylls. Om det är en icke-kvalificerad tillhandahållare av betrodda tjänster ska den skadelidande ha bevisbördan för att det föreligger avsikt eller oaktsamhet. I fråga om kvalificerade tillhandahållare

av betrodda tjänster ska avsikt eller oaktsamhet anses föreligga såvida inte tjänstetillhandahållaren kan visa motsatsen.

I punkt 2 finns en särskild begränsningsregel. En tjänstetillhandahållare som i förväg informerar sina kunder om att det finns begränsningar i användningen av tjänsterna, ansvarar bara för skada som uppstår vid användning inom dessa begränsningar.

I punkt 3 anges att skadeståndsansvaret ska tillämpas i enlighet med nationella bestämmelser om skadeståndsansvar. Enligt skäl 37 till förordningen innebär detta att nationella bestämmelser om t.ex. definitionen av skada, avsikt, oaktsamhet eller relevanta procedurregler inte påverkas.

Den skada som åsamkas i de fall som anges i EU-förordningen utgörs normalt av ren förmögenhetsskada, dvs. ekonomisk skada som uppkommer utan samband med en person- eller sakskada, se 1 kap. 2 § skadeståndslagen (1972:207). Skadeståndsrätten skiljer mellan skador som uppkommer i avtalsförhållanden och skador som uppkommer utanför avtalsförhållanden, s.k. utomobligatoriska förhållanden. Skadeståndslagen innehåller en särskild bestämmelse om ersättning för ren förmögenhetsskada i utomobligatoriska förhållanden. Enligt 2 kap. 2 § i den lagen ska den som vållar ren förmögenhetsskada genom brott ersätta skadan.

Bestämmelserna i skadeståndslagen tillämpas inte om annat är föreskrivet, se 1 kap. 1 § i den lagen. Det behövs därför inte några kompletterande bestämmelser om skadeståndsansvaret i sig med anledning av de skadeståndsrättsliga bestämmelserna i artikel 13.1 och 13.2 i EU-förordningen.

När det gäller skadeståndsrättsliga frågor i övrigt följer av artikel 13.3 att nationella bestämmelser ska gälla. Vid bedömningen av de skadeståndsrättsliga frågor som kan uppkomma kommer således skadeståndslagen och allmänna skadeståndsrättsliga principer att gälla. Hur dessa principer ska tillämpas på skador i nu aktuella fall får, som på andra områden inom skadeståndsrätten, bli en uppgift för rättstillämpningen att avgöra. Inte heller i dessa avseenden behövs därför några kompletterande bestämmelser.

7.5 Rättslig verkan av elektroniska underskrifter m.m.

Bedömning: Det behövs inte några lagändringar med anledning av EU-förordningens bestämmelser om rättslig verkan eller giltighet som bevis av elektroniska underskrifter, elektroniska stämplar, elektroniska tidsstämplingar, elektroniska dokument eller uppgifter som sänds och tas emot genom elektroniska tjänster för rekommenderade leveranser.

Skälen för bedömningen: Enligt artikel 25.1 i förordningen om elektronisk identifiering får en elektronisk underskrift 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. Motsvarande regel i fråga om elektroniska stämplar finns i artikel 35.1, i fråga om elektroniska tids-

stämplingar i artikel 41.1 och i fråga om uppgifter som sänds och tas emot genom en elektronisk tjänst för rekommenderade leveranser i artikel 43.1. Vidare anges i artikel 46 att ett elektroniskt dokument inte får förvägras rättslig verkan eller giltighet som bevis vid rättsliga förfaranden enbart på grund av att det har elektronisk form.

En kvalificerad elektronisk underskrift ska enligt artikel 25.2 ha motsvarande rättsliga verkan som en egenhändig underskrift. I artikel 35.2 anges att en kvalificerad elektronisk stämpel ska medföra att de uppgifter som stämpeln är kopplad till omfattas av en presumtion om integritet, dvs. att uppgifterna är äkta och riktiga, och om att uppgifterna har korrekt ursprung. I artikel 41.2 anges att en kvalificerad elektronisk tidsstämpling ska omfattas av en presumtion om att det datum och den tid som den anger är korrekta och om att de uppgifter som datumet och tiden är kopplade till är äkta och korrekta. Enligt artikel 43.2 ska uppgifter som sänds och tas emot genom en kvalificerad tjänst för rekommenderade leveranser omfattas av en presumtion om äktheten och riktigheten av uppgifterna, om att avsändaren har skickat uppgifterna, att adressaten har tagit emot dem samt om datumet och tidpunkten för avsändandet och mottagandet som anges i den kvalificerade elektroniska tjänsten för rekommenderade leveranser är riktigt.

Utöver vad som anges i förordningen gäller nationell rätt i fråga om vilken rättsverkan betrodda tjänster ska ha och om verkan av olika bevis, se skäl 22 och 49 till förordningen.

I svensk rätt gäller principerna om fri bevisföring och fri bevisvärdering. Av detta följer att en domare ska ta hänsyn till varje omständighet som kan vara ägnad att påverka bedömningen av sakfrågorna. Det finns alltså i princip inte någon begränsning av bevisningsmöjligheterna med hänsyn till en viss upplysningskällas beskaffenhet. Det följer också att en domare fritt ska värdera bevisningens styrka. Det är dock möjligt att göra undantag från principen om fri bevisvärdering, se t.ex. 35 kap. 1 § andra stycket rättegångsbalken. De ovan redovisade presumtionerna i artikel 35.2, 41.2 och 43.2 i EU-förordningen utgör sådana undantag.

I övrigt saknas det i svensk rätt bestämmelser som begränsar möjligheterna att åberopa eller beakta elektroniska underskrifter, elektroniska stämplar, elektroniska tidsstämplingar, elektroniska dokument eller uppgifter som sänds och tas emot genom elektroniska tjänster för rekommenderade leveranser, eller som i övrigt begränsar dessas rättsliga verkan.

Det finns inte heller några regler i svensk rätt som kan sägas förvägra elektroniska underskrifter, elektroniska stämplar, elektroniska tidsstämplingar, elektroniska dokument eller uppgifter som sänds och tas emot genom elektroniska tjänster för rekommenderade leveranser rättslig verkan över huvud taget. Det kan visserligen finnas formkrav för rättshandlingar som utesluter elektronisk kommunikation. Sådana formkrav är dock uttryckligen tillåtna enligt artikel 2.3 i EU-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. Såvitt avser elektroniska underskrifter bedömdes i förarbetena till signaturlagen att i sak motsvarande bestämmelser i artikel 1, 5.1 och 5.2 i signaturdirektivet inte krävde några genomförandeåtgärder (prop. 1999/2000:117 s. 57). Det finns inte skäl att nu göra en annan bedömning vare sig det gäller elektroniska

underskrifter, elektroniska stämplar, elektroniska tidsstämplingar, elektroniska dokument eller uppgifter som sänds och tas emot genom elektroniska tjänster för rekommenderade leveranser.

Kravet i artikel 25.2 om att en kvalificerad elektronisk underskrift ska ha motsvarande rättsliga verkan som en handskriven underskrift överensstämmer i sak med vilken verkan medlemsstaterna ska säkerställa att kvalificerade elektroniska signaturer har enligt artikel 5.1 a i signaturdirektivet. I förarbetena till signaturlagen (prop. 1999/2000:117 s. 56 f och 77 f) gjordes bedömningen att bestämmelsen i signaturdirektivet inte innebär att medlemsstaterna måste godta kvalificerade elektroniska underskrifter i alla de fall där det finns krav på underskrift i nationell rätt eller unionsrätt. I stället måste direktivet uppfattas så att i den mån det över huvud taget är tillåtet att uppfylla ett formkrav på traditionell underskrift eller dylikt med elektroniska rutiner, så måste kvalificerade elektroniska signaturer alltid godtas. En bestämmelse med den innebörden togs därför in i 17 § signaturlagen.

Syftet med EU-förordningen om elektronisk identifiering är enligt artikel 1 bl.a. att uppnå en lämplig säkerhetsnivå för elektronisk identifiering genom att fastställa en rättslig ram för elektroniska underskrifter. EU-förordningen föreskriver inte att elektronisk kommunikation måste accepteras inom något rättsområde. 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 tolkas som så, att om det är tillåtet att uppfylla ett formkrav med elektroniska rutiner så måste kvalificerade elektroniska signaturer alltid godtas. Detta är i enlighet med den bedömning som ligger till grund för motsvarande reglering i 17 § signaturlagen.

I och med att EU-förordningen är direkt tillämplig behövs det sammanfattningsvis inte några lagändringar med anledning av dess bestämmelser om rättslig verkan eller giltighet som bevis av elektroniska underskrifter, elektroniska stämplar, elektroniska tidsstämplingar, elektroniska dokument eller uppgifter som sänds och tas emot genom elektroniska tjänster för rekommenderade leveranser.

7.6 Förteckningar över betrodda tjänsteleverantörer

Bedömning: Tillsynsmyndigheten bör föra en förteckning över kvalificerade tillhandahållare av betrodda tjänster och de kvalificerade betrodda tjänster som dessa tillhandahåller.

Skälen för bedömningen: Enligt artikel 22 i EU-förordningen om elektronisk identifiering ska varje medlemsstat upprätta, underhålla och offentliggöra en förteckning över kvalificerade tillhandahållare av betrodda tjänster och de kvalificerade betrodda tjänster som dessa tillhandahåller. Detta ska ske på ett sätt som lämpar sig för automatiserad behandling och förteckningen ska vara elektroniskt undertecknad eller förseglad. Enligt artikel 17.4 h ska tillsynsmyndigheten lämna information om beviljad status som kvalificerad tillhandahållare av betrodd tjänst, respek-

tive om statusen återkallas, till den som ansvarar för förteckningen om det är någon annan än tillsynsmyndigheten själv.

Liknande bestämmelser om en förteckning finns i artikel 8 i Europaparlamentets och rådets direktiv 2006/123/EG om tjänster på den inre marknaden (tjänstedirektivet). Med stöd av direktivet har Europeiska kommissionen fattat beslut (2009/767/EG) 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. I beslutet anges att medlemsstaterna ska inrätta, underhålla och offentliggöra en tillförlitlig förteckning över de tillhandahållare av certifikattjänster som utfärdar kvalificerade certifikat till allmänheten. För svensk del uppfylls kravet för närvarande genom att det i 18 § signaturlagen anges att tillsynsmyndigheten enligt den lagen ska föra en förteckning och publicera en lista över dem som utfärdar kvalificerade certifikat.

Av EU-förordningen om elektronisk identifiering framgår att kommissionen genom genomförandeakter ska fastställa format och tekniska specifikationer för förteckningen. Förteckningen enligt tjänstedirektivet och förteckningen enligt EU-förordningen fyller samma syfte och kommer av allt att döma att baseras på samma format och specifikation.

Den myndighet som utövar tillsyn över EU-förordningen om elektronisk identifiering är det organ som har tillgång till uppgifter om anmälda kvalificerade tillhandahållare av betrodda tjänster och de kvalificerade betrodda tjänster dessa tillhandahåller. Vidare är det tillsynsmyndigheten som har rätt att förändra statusen för en tillhandahållare av betrodda tjänster. Det är därför naturligast att tillsynsmyndigheten ansvarar för förteckningen.

Frågan om vilken myndighet som bör vara tillsynsmyndighet behandlas i avsnitt 7.8.3.

7.7 Tillfälligt upphävande av kvalificerade certifikat

Bedömning: Det bör inte införas bestämmelser om tillfälligt upphävande av kvalificerade certifikat.

Skälen för bedömningen: Enligt artikel 28.5 och 38.5 i EU-förordningen om elektronisk identifiering får medlemsstaterna fastställa nationella bestämmelser för tillfälligt upphävande av kvalificerade certifikat för elektroniska signaturer och kvalificerade certifikat för elektroniska stämplar. Detta får ske under förutsättning att certifikatet är ogiltigt under upphävandetiden, att upphävandetiden tydligt anges i certifikatdatabasen och att certifikatets status som upphävt under hela denna tid är synlig genom den tjänst som tillhandahåller information om certifikatets status.

Ett system med tillfälligt upphävande skulle möjliggöra återaktivering av borttappade certifikat och krypteringsnycklar om dessa hittas inom en kort tidsperiod.

I Sverige används för närvarande inte tillfälligt upphävande i certifikatbaserade betrodda tjänster. Certifikat med tillhörande krypteringsnycklar

upphävs i stället om de kommit på avvägar eller på annat sätt kompromet-terats och de kan inte få tillbaka sin status som giltiga. Detta innebär att den som har fått sitt certifikat spärrat måste skaffa ett nytt certifikat, på samma sätt som sker vid förlust av betal- eller kreditkort. Ett system där certifikat inte kan återaktiveras medför en något ökad säkerhet, efter-som det inte går att veta vad som har hänt med certifikat och krypterings-nycklar under det tillfälliga upphävandet. Värdet av att införa kom-pletterande bestämmelser om tillfälligt upphävande framstår därför som begränsad. I dagsläget finns det därför inte anledning att införa särskilda bestämmelser om detta.

7.8 Tillsyn

7.8.1 Tillsynsmyndighetens befogenheter

Förslag: En tillsynsmyndighet ska utöva tillsyn över efterlevnaden av EU-förordningen om elektronisk identifiering och rättsakter som har meddelats med stöd av förordningen samt över efterlevnaden av den nya lagen och föreskrifter som har meddelats med stöd av denna.

Tillsynsmyndigheten ska ha rätt att på begäran få de upplysningar och handlingar som behövs för tillsynen och ha rätt att få tillträde till områden, lokaler och andra utrymmen, förutom bostäder, där verk-samhet bedrivs. Tillsynsmyndigheten ska få meddela de förelägganden och förbud som behövs för tillsynen. Förelägganden och förbud ska få förenas med vite.

Skälen för förslaget: Enligt artikel 16 i EU-förordningen om elektro-nisk identifiering är medlemsstaterna skyldiga att fastställa regler om de sanktioner som ska tillämpas vid överträdelser av förordningen. Sanktio-nerna ska vara effektiva, proportionella och avskräckande.

Enligt artikel 17.1 i förordningen ska medlemsstaterna utse ett tillsyns-organ (tillsynsmyndighet).

Tillsynsmyndighetens roll framgår av artikel 17.3. När det gäller kva-lificerade tillhandahållare av betrodda tjänster ska tillsynen gå ut på att genom såväl förebyggande verksamhet som kontroller i efterhand se till att tjänstetillhandahållarna och deras tjänster uppfyller förordningens krav. När det gäller icke-kvalificerade tillhandahållare av betrodda tjäns-ter ska tillsynsmyndigheten agera när någon påstår att en tjänstetillhanda-hållare inte uppfyller kraven.

Tillsynsmyndighetens uppgifter preciseras i artikel 17.4. Där anges att tillsynsmyndigheten ska samarbeta på olika sätt med andra tillsynsmyn-digheter, analysera rapporter om överensstämmelsebedömning, lämna in-formation till Europeiska kommissionen, bedriva granskningsverksamhet samt bevilja status som kvalificerad tillhandahållare av betrodda tjänster (punkt a–h). Tillsynen ska bestå dels i att kontrollera att kvalificerade tillhandahållare av betrodda tjänster som upphör med sin verksamhet föl-jer bestämmelserna om planering för detta och om hur information i så-dana fall ska hållas tillgänglig (punkt i), dels i att ålägga tillhandahållare av betrodda tjänster som inte uppfyller kraven i förordningen att vidta rättelse (punkt j).

Såvitt avser kvalificerade elektroniska signaturer gäller enligt nuvarande regler i 19 § signaturlagen att tillsynsmyndigheten har rätt att på begäran få de upplysningar och handlingar som behövs för tillsynen och få tillträde till områden, lokaler och andra utrymmen, utom bostäder, där det bedrivs verksamhet som står under tillsyn. Vid behov har myndigheten rätt att få biträde av kronofogdemyndigheten för denna tillsyn. Enligt 20 § första stycket i lagen får tillsynsmyndigheten meddela de förelägganden och förbud som behövs för efterlevnaden av lagen eller av föreskrifter som meddelats med stöd av lagen. Förelägganden och förbud får enligt 21 § förenas med vite.

Det är en uppgift för tillsynsmyndigheten att utforma en lämplig tillsynsverksamhet med utgångspunkt från de uppgifter som framgår av EU-förordningen. En grundläggande förutsättning för en fungerande tillsyn är att tillsynsmyndighetens initiativ och beslut är väl underbyggda. Det är därför viktigt att tillsynsmyndigheten kan få tillgång till de upplysningar och handlingar som bedöms nödvändiga för tillsynen samt vid behov kan få tillträde där verksamhet som omfattas av EU-förordningen bedrivs. Därigenom säkerställs också att en effektiv tillsynsverksamhet kan upprätthållas.

När tillsynsmyndigheten upptäcker brister i en verksamhet bör den kunna utfärda de förelägganden eller förbud som behövs för att rättelse ska ske. Mot bakgrund av EU-förordningens krav på att det ska finnas effektiva, proportionella och avskräckande sanktioner bör förelägganden och förbud kunna förenas med vite. Det innebär att tillsynsmyndigheten ytterst kan meddela ett vitessanktionerat förbud för en tjänstetillhandahållare att fortsätta med sin verksamhet. Att härutöver införa bestämmelser om straff eller om sanktionsavgifter framstår däremot inte som nödvändigt.

Sammanfattningsvis innebär detta att tillsynsmyndighetens befogenheter enligt den nya lagen bör överensstämma med vad som i dag gäller för tillsynsmyndighetens befogenheter enligt 19 §, 20 § första stycket och 21 § signaturlagen. Dessa bestämmelser bör således i sak föras över till den nya lagen.

Frågan om vilken myndighet som bör vara tillsynsmyndighet behandlas i avsnitt 8.

7.8.2 Infrastruktur för betrodda tjänster

Bedömning: Tillsynsmyndigheten bör inte inrätta någon infrastruktur för betrodda tjänster.

Skälen för bedömningen: EU-förordningen om elektronisk identifiering bygger på att tillit till betrodda tjänster skapas genom att tillsynsmyndigheter upprättar, offentliggör och löpande uppdaterar en förteckning över tillhandahållare av betrodda tjänster och där tjänstetillhandahållarnas status framkommer, se artikel 22 i förordningen. Om en tjänstetillhandahållare eller en betrodd tjänst tas bort eller förlorar sin status som kvalificerad tillhandahållare uppdateras statusen i förteckningen.

Enligt artikel 17.5 i EU-förordningen om elektronisk identifiering får medlemsstaterna kräva att tillsynsmyndigheten ska inrätta, underhålla

och uppdatera en infrastruktur för betrodda tjänster. Den ordningen innebär att tillsynsmyndigheten, som ett komplement till att ändra tjänstetillhandahållares status i förteckningen, även kan spärra dessas certifikat för tillhandahållande av betrodda tjänster. I en sådan ordning byggs tilliten till tjänsterna normalt upp genom en modell där det finns en kryptografisk koppling mellan tillsynsmyndigheten och tjänstetillhandahållaren som kan kontrolleras av dem som förlitar sig på certifikaten. Detta innebär, till skillnad från systemet med en förteckning enligt artikel 22 i förordningen, där den som har förlorat sin status som kvalificerad tillhandahållare av betrodda tjänster kan återfå den, att om tillsynsmyndigheten spärrar ett utfärdarcertifikat så blir alla certifikat som utfärdats under detta ogiltiga. I en sådan situation måste ett nytt utfärdarcertifikat utfärdas eller undertecknas av tillsynsmyndigheten och alla den tjänstetillhandahållarens kunder måste skaffa nya certifikat. Detta kan visserligen medföra en säkerhetsfördel i ett akutläge i och med att tjänstetillhandahållarens och alla dennes kunders certifikat spärras direkt. Motsvarande funktion kan dock uppnås genom att en tjänstetillhandahållare snabbt tas bort från förteckningen enligt artikel 22 i EU-förordningen och därmed inte längre är betrodd.

Modellen med att tillsynsmyndigheten har en särskild infrastruktur för betrodda tjänster används inte i Sverige i dag. Frågan om inrättandet av en sådan s.k. toppnod berördes i förarbetena till signaturlagen, se prop. 1999/2000:117 s. 61. Regeringen bedömde då att signaturdirektivets regel om förbud mot förhandstillstånd innebar att man inte kunde kräva att alla certifikatutfärdare skulle ansluta sig till en toppnod för att få sina öppna nycklar signerade. Regeringen konstaterade också att ett sådant krav skulle innebära att en certifikatutfärdare inte kan verka på marknaden utan att ansluta sig till toppnoden, vilket är att jämställa med ett krav på förhandstillstånd. Ett sådant krav skulle vidare innebära att certifikatutfärdaren måste anpassa sina tekniska lösningar till toppnoden för att kunna verka i dess underliggande struktur. Detta ansågs strida mot direktivets strävan mot teknikneutralitet, dvs. att direktivets krav ska kunna uppfyllas på flera olika sätt med hjälp av olika typer av teknik.

Bestämmelsen i artikel 17.5 tar främst hänsyn till de länder som har etablerat en sådan infrastruktur sedan tidigare och ger dem en möjlighet att fortsätta med sin modell. En sådan infrastruktur är dock beroende av höga tillgänglighetskrav med bl.a. jourtjänstgöring dygnet runt. Den skulle därmed bli kostsam att bygga upp. Dessutom skulle det innebära att alla befintliga utfärdares certifikat och strukturer för betrodda tjänster skulle behöva bytas ut mot certifikat som är utfärdade eller undertecknade av tillsynsmyndigheten, vilket också är förenat med betydande olägenheter och kostnader. Inrättandet av en sådan infrastruktur skulle totalt sett medföra begränsade fördelar jämfört med att enbart använda förteckning som ska föras enligt artikel 22 i EU-förordningen. Fördelarna står inte i proportion till de kostnader som uppbyggnaden av en ny infrastruktur skulle medföra. En sådan infrastruktur bör därför inte inrättas.

7.8.3 Val av tillsynsmyndighet

Bedömning: E-legitimationsnämnden bör utses till tillsynsmyndighet.

Skälen för bedömningen

Tillsynsmyndighetens uppdrag

Som framgår av avsnitt 7.8.1 ska medlemsstaterna enligt artikel 17.1 i EU-förordningen om elektronisk identifiering utse ett tillsynsorgan (tillsynsmyndighet).

Härutöver görs i denna promemoria bedömningen att tillsynsmyndigheten även bör fullgöra vissa andra uppgifter.

I avsnitt 7.2 görs bedömningen att tillsynsmyndigheten bör meddela föreskrifter om krav för ackreditering av organ för bedömning av överensstämmelse, om rapportering av bedömningar av överensstämmelse och om hur sådana bedömningar ska göras.

I avsnitt 7.3 görs bedömningen att regeringen eller den myndighet som regeringen bestämmer bör meddela föreskrifter om certifiering av anordningar för skapande av kvalificerade elektroniska underskrifter och anordningar för skapande av kvalificerade elektroniska stämplar.

I avsnitt 7.6 görs bedömningen att tillsynsmyndigheten bör föra en förteckning över kvalificerade tillhandahållare av betrodda tjänster och de kvalificerade betrodda tjänster som dessa tillhandahåller.

Uppdraget bör samlas hos en myndighet

Det svenska marknaden för tjänster som omfattas av EU-förordningen är i dagsläget liten och rättsområdet är begränsat. Uppgiften att vara tillsynsmyndighet, att meddela föreskrifter och att föra en förteckning enligt vad som nyss beskrivits kommer därför att vara av begränsad omfattning. Den bör därför läggas på en befintlig myndighet.

Elektronisk identifiering, elektronisk underskrift och andra betrodda tjänster är centrala delar i den gemensamma infrastruktur som utgör grunden i digitaliseringen av samhället. Den svenska marknaden för sådana tjänster är liten i dagsläget. Marknaden kan dock förväntas öka på sikt, inte minst mot bakgrund av tillkomsten av EU-förordningen.

I och med att det är ett litet rättsområde med få marknadsaktörer finns det en risk för fragmentering om ansvaret för olika delar är spritt bland flera myndigheter. Utgångspunkten bör i stället vara att utvecklingen inom området bör bedrivas sammanhållet och på lång sikt av en enda myndighet så att denna kan upprätthålla kompetens på området. Genom att samla frågorna hos en aktör minskar också risken för att frågor faller mellan stolarna eller hanteras dubbelt. Därmed minskar även regeringens behov av att detaljerat styra olika myndigheters verksamheter inom området.

Det finns flera tänkbara myndigheter för uppdraget att vara tillsynsmyndighet: E-legitimationsnämnden, Försvarets materielverk (FMV), Myndigheten för samhällsskydd och beredskap (MSB), Post- och telestyrelsen (PTS), och Styrelsen för ackreditering och teknisk kontroll (Swedac).

E-legitimationsnämnden

E-legitimationsnämnden har i uppdrag att stödja och samordna den offentliga sektorns behov av säkra metoder för elektronisk identifiering och signering. I detta arbete ingår att efter överenskommelse med upphandlande myndigheter tillhandahålla system för säker elektronisk identifiering enligt lagen (2013:311) om valfrihetssystem i fråga om tjänster för elektronisk identifiering och att administrera sådana valfrihetssystem. E-legitimationsnämnden tillhandahåller en infrastruktur för elektronisk identifiering, en så kallad identitetsfederation för svensk offentlig sektor. Denna består av det regelverk som nämnden har tagit fram och som bl.a. innehåller bestämmelser om tillitsnivåer för e-legitimationer, servicenivåer för i federationen ingående tjänster, skadeståndsbestämmelser och avtalsreglerad möjlighet för E-legitimationsnämnden att utföra kontroll och vid behov stänga av tjänster eller aktörer. Federationen innehåller även vissa centrala tjänster, som metadatatjänst och anvisningstjänst.

E-legitimationsnämnden har ett upparbetat nära samarbete med många myndigheter som levererar service till medborgarna via e-tjänster.

FMV

FMV ansvarar för Sveriges Certifieringsorgan för it-säkerhet (CSEC). Detta organ verkar som Sveriges nationella certifieringsorgan för it-säkerhet enligt den internationella standarden ISO/IEC 15408, även kallad Common Criteria. Standarden används för kravställning och opartisk granskning av it-säkerhetsprodukter. CSEC tillämpar för närvarande också de standarder som Europeiska kommissionen har använt för att ställa krav på it-säkerhet och kryptering med stöd av signaturdirektivet.

MSB

MSB har i uppdrag att utveckla samhällets förmåga att förebygga och hantera olyckor och kriser. MSB har därför bl.a. i uppgift att samordna arbetet med samhällets informationssäkerhet genom att stödja förebyggande åtgärder och att arbeta med att främja ett systematiskt långsiktigt arbete med informationssäkerhet på alla nivåer i samhället.

MSB har ansvar på en övergripande nivå när det gäller statliga myndigheters informationssäkerhet.

PTS

PTS är central förvaltningsmyndighet med ett samlat ansvar inom postområdet och området för elektronisk kommunikation. Myndigheten har bl.a. till uppgift att främja tillgången till säkra och effektiva elektroniska kommunikationer, vilket även omfattar att se till att samhällsomfattande tjänster finns tillgängliga, och att främja tillgången till ett brett urval av elektroniska kommunikationstjänster.

PTS har också till uppgift att 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.

PTS är en utpräglad tillstånds- och tillsynsmyndighet med verksamhet inom flera områden. PTS utövar för närvarande tillsyn över utfärdare av kvalificerade certifikat till allmänheten enligt signaturlagen. PTS är också tillsynsmyndighet enligt lagen (2003:389) om elektronisk kommunikation, lagen (2000:121) om radio- och teleterminalutrustning och lagen (2006:24) om toppdomäner för Sverige på Internet.

Swedac

Swedac är central förvaltningsmyndighet för teknisk kontroll och mätteknik. Swedac ackrediterar certifieringsorgan som i sin tur kan certifiera certifikatutfärdare i enlighet med lagen (2011:791) om ackreditering och teknisk kontroll.

Swedac arbetar inom många områden med att ackreditera certifieringsorgan, kontrollorgan och laboratorier som i sin tur kontrollerar, provar, bedömer och verifierar alltifrån ledningssystem och hissar till medicinska laboratorier och växthusgaser. Swedac tar också fram regler för exempelvis vågar, ädelmetallarbeten, färdigförpackade varor, elmätare och bensinpumpar som handlare och tillverkare ska följa. Swedac har lång erfarenhet av såväl egen bedömning av tekniska system som bedömning av andra organ. Swedac är också engagerat i vidareutveckling av de europeiska systement för ömsesidigt godtagande av provning och kontroll. Däremot är myndigheten inte inblandad i framtagande av sakområdesspecifika krav på t.ex. kompetensbedömning av organ eller för bedömning av överensstämmelse. Sådana krav tas i stället fram av myndigheter inom respektive område.

Val av myndighet

PTS har varit tillsynsmyndighet enligt signaturlagen sedan den 1 januari 2001 då lagen infördes. I förarbetena till lagen diskuterades vilken myndighet som var bäst lämpad för tillsynsuppdraget. Att PTS kom att få uppdraget hängde i hög grad samman med att det vid den tidpunkten var fråga om en ny verksamhet som inte omfattades av den tillsyn som fanns inom förvaltningen och att ingen annan myndighet ansågs bättre lämpad (se Ds 1999:73 s. 93 f och prop. 1999/2000:117 s. 64 f).

Det kan konstateras att PTS under ett flertal år har byggt både juridisk och teknisk kompetens inom området för elektroniska signaturer. Dagens tillsyn och anknytande uppgifter utgör dock endast en mycket liten del av myndighetens verksamhet och arbetet är främst inriktat mot marknadens aktörer. Det framstår också till sin art som något perifert i förhållande till myndighetens övriga verksamhet.

Vidare kommer tillsynsmyndighetens verksamhet enligt EU-förordningen om elektronisk identifiering att omfatta ett större område och fler betrodda tjänster än signaturlagen. Ingen myndighet utövar för närvarande tillsyn över dessa tillkommande tjänster på det sätt som förutsätts i EU-förordningen.

Det finns numera även en annan myndighet med kompetens inom EU-förordningens tillämpningsområde. Sedan 2011 har E-legitimationsnämnden regeringens uppdrag att stödja och samordna den offentliga sektorns behov av säkra metoder för elektronisk identifiering och under-

skrift. Nämnden tillhandahåller en infrastruktur för elektronisk identifiering, en så kallad identitetsfederation för svensk offentlig sektor.

Nämndens uppdrag faller väl in under EU-förordningens tillämpningsområde. Nämnden har ett upparbetat nära samarbete med många myndigheter som levererar service till medborgarna via e-tjänster. Det arbete som krävs enligt EU-förordningen och anknytande rättsakter kan bygga vidare på dessa nätverk. Nämndens verksamhet är av sådan art att det skulle vara förhållandevis enkelt att bygga upp den kompetens som krävs även inom övriga områden som täcks av EU-förordningen. De kontakter som PTS har i dag med marknadens aktörer bedöms kunna tas över av E-legitimationsnämnden utan att verksamheten påverkas i någon större omfattning.

Den samlade bedömningen är att målet att utvecklingen inom området bör bedrivas sammanhållet och på lång sikt av en enda myndighet tillgodoses bäst om myndighetsansvaret samlas hos E-legitimationsnämnden. Därigenom kan kompetens på lång sikt byggas upp inom hela området och frågorna få den kontinuitet som krävs för en fortsatt framgångsrik utveckling av området.

Mot den nu angivna bakgrunden framstår E-legitimationsnämnden som mest lämpad för uppgiften att vara tillsynsmyndighet. Därmed bör nämnden också meddela föreskrifter om krav för ackreditering av organ för bedömning av överensstämmelse, om rapportering av bedömningar av överensstämmelse och om hur bedömningar av överensstämmelse ska göras, liksom om certifiering av anordningar för skapande av kvalificerade elektroniska underskrifter och anordningar för skapande av kvalificerade elektroniska stämplar, samt föra förteckningen över kvalificerade tillhandahållare av betrodda tjänster och de kvalificerade betrodda tjänster som dessa tillhandahåller.

7.9 Gränsöverskridande elektronisk identifiering

En av de viktigaste förutsättningarna för effektiva och framgångsrika digitala tjänster är att det finns väl fungerande tjänster för elektronisk identifiering och elektronisk underskrift. Med hjälp av en e-legitimation kan en användare av elektroniska tjänster både bevisa sin identitet och med elektronisk signatur bekräfta lämnade uppgifter. I de flesta fall kan dock medborgare i dag inte använda medel för elektronisk identifiering för att autentisera sig i en annan medlemsstat.

Ett av målen med EU-förordningen är att undanröja hinder för gränsöverskridande användning av medel för elektronisk identifiering som används i medlemsstaterna inom EU. Detta ska ske genom ömsesidigt erkännande av medel för elektronisk identifiering. En förutsättning för det ömsesidiga erkännandet är att medlet har utfärdats inom ramen för ett nationellt system för elektronisk identifiering som uppfyller vissa villkor och som har anmälts till Europeiska kommissionen enligt ett särskilt förfarande. Villkoren för vilka medel för elektronisk identifiering som måste erkännas och hur systemen för elektronisk identifiering ska anmälas anges dels i EU-förordningen, dels i kommande rättsakter i form av genomförandeakter som meddelas med stöd av EU-förordningen.

Genom förordningen kommer ömsesidigt erkända medel för elektronisk identifiering 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. Utländska personer kommer att på ett tillförlitligt sätt kunna använda sitt lands godkända e-legitimationer vid användning av svenska tjänster, givet att det finns ett regelverk som garanterar säkerhetsnivå och ansvar.

Offentlig sektor har lanserat en lång rad digitala tjänster under det senaste årtiondet och samverkan mellan myndigheter har ökat. Det finns dock mer att göra för att underlätta för dem som använder digitala tjänster. Digitala tjänster i offentlig sektor bör utformas på ett sådant sätt att alla människor kan ta del av dem utifrån olika förutsättningar och behov. Det gäller t.ex. funktionsnedsättningar av syn, hörsel och kognitiva förmågor. En viktig målsättning bör vara att utvecklingen av digitala tjänster bidrar till att kvinnor respektive män är nöjda och nyttjar tjänsterna i likvärdig utsträckning. Utvecklingen av digitala tjänster bör vara behovsdriven, baseras på nytta och genomföras i samverkan med användarna. Utformningen av tjänsterna bör utgå ifrån användarens livssituation eller verksamhetsprocess.

Det ska vara tryggt att använda digitala tjänster i offentlig sektor. Rutinerna för identifiering och underskrifter i samband med användning av digitala tjänster bör fungera på ett enkelt sätt för användaren, oavsett om denna befinner sig i Sverige eller i någon annan medlemsstat. Rutinerna måste dessutom bidra till en god säkerhetsnivå.

Regeringens ambition är att offentlig sektor ska erbjuda fler och bättre digitala tjänster som kan nyttjas av användare. För många av de nuvarande och framtida tjänsterna krävs e-legitimation. Privatpersoners och företags användning av och förtroende för e-legitimation är avgörande i den pågående digitaliseringen av samhället. Regeringen har också uttalat att det är angeläget att varje medlemsland, inklusive Sverige, bidrar till att underlätta gränsöverskridande elektronisk identifiering (prop. 2014/15:1, utg.omr. 22, s. 150 f).

De e-legitimationer som används i Sverige i dag tillhandahålls av marknaden och inte av staten eller på uppdrag av staten. Det finns ingen skyldighet för en medlemsstat att anmäla något nationellt system för elektronisk identifiering enligt EU-förordningen. Däremot är ett anmält system en förutsättning för att svenska e-legitimationer ska erkännas i övriga medlemsstater inom EU. De möjligheter som EU-förordningen erbjuder i denna del väcker frågor som inte har kunnat behandlas inom ramen för denna promemoria, utan frågorna behöver analyseras i särskild ordning.

Vidare innebär EU-förordningen att Sverige är skyldigt att erkänna utländska personers användning av e-legitimationer som har utfärdats inom ett system för elektronisk identifiering som en annan medlemsstat har anmält. Hur detta ska gå till i praktiken är ett annat område som kräver ytterligare analys.

Regeringen har lämnat ett uppdrag till E-legitimationsnämnden och Post- och telestyrelsen att löpande följa och analysera konsekvenserna av de genomförandeakter som utarbetas som en följd av EU-förordningen (dnr N2015/2620/EF).

I vissa fall är det obligatoriskt för Europeiska kommissionen att anta genomförandeakter. I andra öppnar EU-förordningen endast för en möjlighet att anta genomförandeakter. I de två myndigheternas uppdrag ingår också att analysera och redovisa vilka konsekvenser det får om sådana icke-obligatoriska genomförandeakter inte antas.

Inom ramen för samma uppdrag ska E-legitimationsnämnden även utreda och föreslå hur en lösning för gränsöverskridande elektronisk identifiering och underskrift kan utformas och erbjudas svenska intressenter i olika situationer, t.ex. privat, i tjänsten, om man är bosatt utomlands eller ett företag, en myndighet eller annan organisation med gränsöverskridande verksamhet.

8 Följdändringar

8.1 Upphävande av lagen om kvalificerade elektroniska signaturer

Förslag: Lagen om kvalificerade elektroniska signaturer upphävs.

Skälen för förslaget: Lagen (2000:832) om kvalificerade elektroniska signaturer (signaturlagen) har kommit till för att genomföra Europaparlamentets och rådets direktiv 1999/93/EG om ett gemenskapsramverk för elektroniska signaturer (signaturdirektivet) i svensk rätt.

Genom EU-förordningen om elektronisk identifiering stärks och utvidgas det regelverk som finns i signaturdirektivet. Enligt artikel 50 i EU-förordningen ska signaturdirektivet upphöra att gälla den 1 juli 2016. Efter den tidpunkten finns det således inte något EU-rättsligt krav på att ha kvar bestämmelserna i signaturlagen.

I signaturlagen finns materiella bestämmelser om säkra anordningar för signaturframställning, om kvalificerade certifikat och utfärdande av sådana certifikat, om skadestånd, om behandling av personuppgifter och om verkan av kvalificerade elektroniska signaturer när ett författningsreglerat krav på egenhändig underskrift får uppfyllas med elektroniska medel. Samtliga dessa områden är reglerade i EU-förordningen, som är bindande och direkt tillämplig i Sverige. Det finns därmed inte längre något behov av signaturlagens reglering. Lagen bör därför upphävas.

8.2 Följdändringar i andra lagar

Förslag: Hänvisningar i lag till avancerade elektroniska signaturer enligt lagen om kvalificerade elektroniska signaturer ersätts av hänvisningar till avancerade elektroniska underskrifter enligt EU-förordningen om elektronisk identifiering. Lagbestämmelser som direkt eller indirekt endast allmänt hänvisar till elektroniska signaturer, utan angivande av att signaturen ska vara av en viss kvalitet, ändras på så sätt att hänvisningen avser elektroniska underskrifter.

Skälen för förslaget: I signaturlagen finns bestämmelser om avancerade och kvalificerade elektroniska signaturer.

Enligt 2 § signaturlagen ska en avancerad elektronisk signatur

a) vara knuten uteslutande till en undertecknare,

b) göra det möjligt att identifiera undertecknaren,

c) vara skapad med hjälpmedel som endast undertecknaren kontrollerar, och

d) vara knuten till andra elektroniska data på ett sådant sätt att förvanskningar av dessa data kan upptäckas.

I EU-förordningen om elektronisk identifiering har termen elektronisk signatur ersatts av termen elektronisk underskrift. Av artikel 3 i EU-förordningen följer att en avancerad elektronisk underskrift ska uppfylla följande krav:

a) den ska vara unikt knuten 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, och

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.

Den sakliga skillnaden mellan uttrycket avancerad elektronisk signatur i signaturlagen och uttrycket avancerad elektronisk underskrift i EU-förordningen är mycket litet. Hänvisningar i lag till avancerade elektroniska signaturer enligt signaturlagen bör därför ersättas med hänvisningar till avancerade elektroniska underskrifter enligt EU-förordningen.

De hänvisningar till avancerade elektroniska signaturer som bör ändras på det angivna sättet finns i:

– 45 kap. 4 § rättegångsbalken,

– 111 kap. 5 § socialförsäkringsbalken,

– 11 § lagen (1978:599) om avbetalningsköp mellan näringsidkare m.fl.,

– 1 kap. 4 § sparbankslagen (1987:619),

– 1 kap. 7 § lagen (1987:667) om ekonomiska föreningar,

– 1 kap. 9 § stiftelselagen (1994:1220),

– 2 kap. 7 § årsredovisningslagen (1995:1554),

– 1 kap. 7 § lagen (1995:1570) om medlemsbanker,

– 2 a § revisionslagen (1999:1079),

– 1 kap. 13 § aktiebolagslagen (2005:551),

– 9 kap. 3 § lagen (2007:1091) om offentlig upphandling[1],

– 9 kap. 3 § lagen (2007:1092) om upphandling inom områdena vatten, energi, transporter och posttjänster[2],

[1] I 12 kap. 9 § i den nya lag om offentlig upphandling som i Ds 2014:25 föreslås ersätta lagen (2007:1091) om offentlig upphandling från och med den 1 april 2016, finns en motsvarighet till denna hänvisning.

[2] I 12 kap. 9 § i den nya lag om upphandling inom försörjningssektorerna som i Ds 2014:25 föreslås ersätta lagen (2007:1092) om offentlig upphandling inom områdena vatten, energi, transporter och posttjänster från och med den 1 april 2016, finns en motsvarighet till denna hänvisning.

– 43 § konsumentkreditlagen (2010:1846),
– 10 kap. 3 § lagen (2011:1029) om upphandling på försvars- och säkerhetsområdet, och
– 11 § lagen (2014:105) om finansiering av partier.

En hänvisning till signaturlagen som bör justeras på motsvarande sätt finns också i det förslag till ny lag om koncessioner som har lämnats i SOU 2014:69.

Det finns i dagsläget inga lagbestämmelser som kräver att kvalificerade elektroniska signaturer ska användas.

Lagbestämmelser som direkt eller indirekt endast allmänt hänvisar till elektroniska signaturer utan angivande av att signaturen ska vara av en viss kvalitet behöver endast ändras på så sätt att hänvisningen avser elektroniska underskrifter, i enlighet med EU-förordningens terminologi. Sådana hänvisningar finns i:

– 111 kap. 1 och 6 §§ socialförsäkringsbalken,
– 1 kap. 9 § bostadsrättslagen (1991:614),
– 8 kap. 3 a § årsredovisningslagen (1995:1554),
– 8 kap. 5 a § lagen (1995:1559) om årsredovisning i kreditinstitut och värdepappersbolag,
– 8 kap. 5 a § lagen (1995:1560) om årsredovisning i försäkringsföretag,
– 1 kap. 6 § lagen (2002:93) om kooperativ hyresrätt,
– 4 kap. 5 § lagen (2004:1199) om handel med utsläppsrätter,
– 2 kap. 10 § lagen (2007:1091) om offentlig upphandling[3],
– 2 kap. 10 § lagen (2007:1092) om upphandling inom områdena vatten, energi, transporter och posttjänster[4],
– 2 kap. 2 § lagen (2008:962) om valfrihetssystem,
– 12 kap. 4 § försäkringsrörelselagen (2010:2043), och
– 2 kap. 14 § lagen (2011:1029) om upphandling på försvars- och säkerhetsområdet.

Det saknas hänvisningar i lag till elektroniska stämplar, elektroniska tidsstämplingar, elektroniska tjänster för rekommenderade leveranser och kvalificerade certifikat för autentisering av webbplatser. Det finns därmed inget behov av följdändringar med anledning av EU-förordningens bestämmelser i dessa delar.

[3] I den nya lag om offentlig upphandling som i Ds 2014:25 föreslås ersätta lagen (2007:1091) om offentlig upphandling från och med den 1 april 2016, finns ingen motsvarighet till denna hänvisning.

[4] I den nya lag om upphandling inom försörjningssektorerna som i Ds 2014:25 föreslås ersätta lagen (2007:1092) om offentlig upphandling inom områdena vatten, energi, transporter och posttjänster från och med den 1 april 2016, finns ingen motsvarighet till denna hänvisning.

9 Avgifter

Förslag: Regeringen eller, efter regeringens bemyndigande, tillsynsmyndigheten får meddela föreskrifter om skyldighet för tillhandahållare av betrodda tjänster att betala avgift för tillsynsmyndighetens verksamhet enligt denna lag och enligt föreskrifter som har meddelats med stöd av lagen samt enligt EU-förordningen om elektronisk identifiering och rättsakter som har meddelats med stöd av den förordningen.

Skälen för förslaget: Enligt 22 § signaturlagen får regeringen eller, efter regeringens bemyndigande, tillsynsmyndigheten meddela föreskrifter om skyldighet för certifikatutfärdare som utfärdar kvalificerade certifikat till allmänheten att betala avgift för tillsynsmyndighetens verksamhet enligt lagen. I förarbetena till signaturlagen uttalades att det framstod som mest naturligt att låta tillsynsmyndighetens verksamhet finansieras genom avgiftsuttag från dem som berörs av verksamheten och för vilka den i vissa avseenden får anses vara till nytta (prop. 1999/2000:117 s. 66). Frågan om och i vilken omfattning det är lämpligt att ta ut avgifter överlämnades åt regeringen att avgöra.

Ett avgiftssystem har införts. Av 10 § förordningen (2003:767) om finansiering av Post- och telestyrelsens verksamhet jämfört med 17 § Post- och telestyrelsens föreskrifter (PTSFS 2013:6) om avgifter följer att certifikatutfärdare som utfärdar kvalificerade certifikat till allmänheten ska betala en årlig avgift om 5 000 kr.

I EU-förordningen om elektronisk identifiering utökas tillsynsmyndighetens uppdrag till att avse tillsyn över alla betrodda tjänster, såväl kvalificerade som icke-kvalificerade. Det framstår som lämpligt att även fortsättningsvis bibehålla den ordning som gällt sedan signaturlagens tillkomst att tillsynsmyndighetens verksamhet ska vara avgiftsfinansierad av dem som berörs av verksamheten. I den nya lagen bör det därför föras in en motsvarighet till 22 § signaturlagen. Mot bakgrund av EU-förordningens vidare tillämpningsområde bör dock avgiftsskyldigheten utvidgas från att gälla certifikatutfärdare som utfärdar kvalificerade certifikat till allmänheten till att gälla alla tillhandahållare av betrodda tjänster. Dessutom bör den gälla tillsynsmyndighetens verksamhet enligt den nya lagen och föreskrifter som har meddelats med stöd av lagen samt enligt EU-förordningen om elektronisk identifiering och rättsakter som har meddelats med stöd av den förordningen. Närmare detaljer om avgiftssystemets utformning kan meddelas av regeringen med stöd av bemyndigandet.

10 Överklagande

Förslag: Tillsynsmyndighetens beslut enligt den nya lagen får överklagas till allmän förvaltningsdomstol. Prövningstillstånd ska krävas vid överklagande till kammarrätten. Tillsynsmyndigheten får bestämma att ett beslut ska gälla omedelbart.

Skälen för förslaget: Enligt artikel 17.4 j i EU-förordningen om elektronisk identifiering ska tillsynsmyndigheten kunna ålägga tillhandahållare av betrodda tjänster att vidta rättelse om kraven i förordningen inte följs. Med anledning av detta föreslås i avsnitt 7.9.1 att tillsynsmyndigheten ska kunna besluta om förelägganden och förbud, i förekommande fall i förening med vite. Dessa tillsynsbeslut måste kunna överklagas.

Även i övrigt följer av EU-förordningen att tillsynsmyndigheten ska fatta vissa beslut som måste kunna överklagas. Det rör t.ex. beslut enligt artikel 19.2 fjärde stycket att informera om integritetsincidenter, beslut enligt artikel 20.3 att återkalla någons status som kvalificerad tillhandahållare av betrodda tjänster och beslut att inte bevilja någon status som kvalificerad tillhandahållare av betrodda tjänster enligt artikel 21.2.

Tillsynsmyndighetens befogenheter enligt den nya lagen överensstämmer med dem som tillsynsmyndigheten i dag har enligt signaturlagen. Enligt 23 § signaturlagen får tillsynsmyndighetens beslut enligt den lagen överklagas till allmän förvaltningsdomstol. Vidare krävs prövningstillstånd vid överklagande till kammarrätten. Tillsynsmyndigheten får också bestämma att beslut enligt lagen ska gälla omedelbart.

Det framstår som lämpligt att samma ordning som gäller för överklagande enligt signaturlagen ska gälla även enligt den nya lagen. De tillsynsbeslut som tillsynsmyndigheten meddelar bör därför få överklagas till allmän förvaltningsdomstol, med krav på prövningstillstånd vid överklagande till kammarrätten. I avsnitt 7.8.3 görs bedömningen att E-legitimationsnämnden bör vara tillsynsmyndighet. Enligt 14 § lagen (1971:289) om allmänna förvaltningsdomstolar kommer därmed överklaganden av nämndens beslut att prövas av Förvaltningsrätten i Stockholm.

Antalet elektroniska transaktioner ökar stadigt i dagens samhälle. Med hänsyn till betrodda tjänsters centrala roll i skapandet och bibehållandet av tillit mellan parterna i sådana transaktioner kan det vara av avgörande betydelse att ingripa skyndsamt när brister i betrodda tjänster uppmärksammas. Det bör därför även fortsättningsvis finnas möjlighet för tillsynsmyndigheten att bestämma att dess beslut ska gälla omedelbart.

11 Ikraftträdande- och övergångsbestämmelser

Förslag: Den nya lagen med kompletterande bestämmelser till förordningen om elektronisk identifiering och följdändringarna ska träda i kraft den 1 juli 2016, då lagen om kvalificerade elektroniska signaturer ska upphöra att gälla.

Bestämmelserna om skadestånd i lagen om kvalificerade elektroniska signaturer bör fortsätta att gälla i fråga om skada som har åsamkats före upphävandet av den lagen.

Skälen för förslaget: Av artikel 52 i EU-förordningen om elektronisk identifiering följer att förordningen, i de delar som omfattas av denna promemoria, ska börja tillämpas den 1 juli 2016. Den nya lagen med kompletterande bestämmelser till förordningen om elektronisk identifiering liksom nödvändiga följdändringar bör därför träda i kraft den dagen. Samtidigt bör lagen (2000:832) om kvalificerade elektroniska signaturer (signaturlagen), upphöra att gälla.

I artikel 51 i EU-förordningen finns vissa övergångsbestämmelser med anledning av att signaturdirektivet upphävs. Där anges att säkra anordningar för skapande av underskrifter, vilkas överensstämmelse har fastställts i enlighet med artikel 3.4 i signaturdirektivet, ska anses som kvalificerade anordningar för skapande av elektroniska underskrifter enligt EU-förordningen. Vidare anges att kvalificerade certifikat som har utfärdats för fysiska personer enligt signaturdirektivet ska anses som kvalificerade certifikat för elektroniska signaturer enligt EU-förordningen till dess att de löper ut. Det finns också bestämmelser om att den som utfärdar certifikat enligt signaturdirektivet har möjlighet att behålla sin status som kvalificerad tillhandahållare på grundval av en rapport om bedömning av överensstämmelse, om rapporten lämnas till tillsynsmyndigheten senast den 1 juli 2017.

I de nu angivna delarna kommer EU-förordningens bestämmelser att vara direkt tillämpliga. Det finns alltså inte något behov av kompletterande övergångsbestämmelser i dessa delar.

Inte heller i övrigt finns det behov av övergångsreglering i anslutning till signaturlagens bestämmelser om säkra anordningar för signaturframställning, kvalificerade certifikat, utfärdande av kvalificerade certifikat, behandling av personuppgifter, kvalificerade elektroniska signaturer och avgifter.

I 14 § signaturlagen finns bestämmelser om att den som utfärdar kvalificerade certifikat till allmänheten under vissa förutsättningar ska ersätta den skada som åsamkats den som har förlitat sig på certifikatet. I 15 § anges att avtalsvillkor som i jämförelse med 14 § är till nackdel för den som förlitar sig på certifikatet är utan verkan mot denne. Dessa bestämmelser bör även fortsättningsvis gälla för skada som åsamkats före upphävandet av signaturlagen. Det bör införas en särskild övergångsbestämmelse om detta.

När det gäller tillsynsåtgärder följer av allmänna principer att förelägganden och förbud som har meddelats med stöd av signaturlagen fortsätter att gälla efter upphävandet av den lagen. Det behövs alltså inte

någon särskild övergångsbestämmelse i den delen. Inte heller i övrigt finns det behov av ytterligare övergångsbestämmelser.

12 Konsekvenser

Syftet med den nya EU-förordningen 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 digitala tjänster samt i elektronisk affärsverksamhet och e-handel inom EU.

EU-förordningens regler är bindande och direkt tillämpliga. De nya bestämmelser som införs syftar till att komplettera EU-förordningens bestämmelser så att den kan få fullt genomslag. Förslagen har utformats med utgångspunkt från att de förhållanden som redan har bidragit till att öka förtroendet för elektroniska transaktioner genom den lag (2000:832) om kvalificerade elektroniska signaturer (signaturlagen) som infördes i enlighet med signaturdirektivet ska tas till vara.

Införandet av lagen i sig innebär inga åligganden för kommuner och landsting, och därmed inte några ekonomiska åtaganden för den kommunala och landstingskommunala sektorn.

Antalet tillhandahållare av kvalificerade betrodda tjänster är begränsat och bedöms vara begränsat även i fortsättningen. Antalet tillhandahållare av icke kvalificerade betrodda tjänster är mer svårbedömt både vad gäller hur många som är etablerade i Sverige och hur marknaden kan komma att utvecklas. Bedömningen är att det i dagsläget finns ca 15–30 sådana tillhandahållare.

Det finns för närvarande en mycket begränsad eller ingen nationell efterfrågan på kvalificerade elektroniska underskrifter. Det finns däremot ett behov av sådana tjänster för gränsöverskridande användning. Det är därför viktigt att det finns tillhandahållare av kvalificerade betrodda tjänster på den svenska marknaden så att svenska företag kan köpa tjänster för att, t.ex. kunna lämna anbud i offentlig upphandling och signera elektroniska fakturor till de medlemsländer där det ställs formkrav på att kvalificerade betrodda tjänster används för sådana förfaranden. Behovet av andra kvalificerade betrodda tjänster än underskrift och stämplar är svårbedömt.

Marknadens aktörer kan komma att påverkas av föreskrifter om krav för ackreditering och föreskrifter om certifiering av anordningar för skapande av kvalificerade elektroniska underskrifter och anordningar för skapande av kvalificerade elektroniska stämplar, i den mån dessa inte överensstämmer med befintliga ordningar på området.

E-legitimationsnämnden föreslås vara tillsynsmyndighet och ha föreskriftsrätt på området. Utgångspunkten är att nämndens uppgifter ska finansieras med avgifter, i likhet med vad som gällt för Post- och telestyrelsens verksamhet som tillsynsmyndighet enligt signaturlagen. Uppgifterna består i arbete med tillsynsramverk, föreskrifter och processer, t.ex. avseende incidentrapportering. En mindre del kommer att

kunna täckas av ökade avgifter, dels pga. att alla tillhandahållare av betrodda tjänster bör omfattas av avgiftssystemet, dels genom en viss höjning av avgiftens storlek jämfört med vad som tidigare har gällt. I övrigt behöver de tillkommande kostnaderna hos E-legitimationsnämnden finansieras med ökade anslagsmedel från och med 2016.

Sveriges certifieringsorgan för it-säkerhet (CSEC) vid Försvarets materielverk bedöms bli certifieringsorgan för anordningar för skapande av kvalificerade elektroniska underskrifter och för anordningar för skapande av kvalificerade elektroniska signaturer. CSEC:s arbete med att driva en nationell certifieringsordning för säkerhet i it-produkter och system är anslagsfinansierad, medan själva certifieringen av it-produkter är avgiftsfinansierad. Kostnaderna för det tillkommande arbetet bedöms bli blygsamma och förväntas rymmas inom ramen för redan tilldelat anslag för denna verksamhet och avgifter för tillkommande certifieringar. Behovet av eventuell utökning av anslaget kommer att följas upp.

Styrelsen för ackreditering och teknisk kontroll (Swedac) är nationellt ackrediteringsorgan. Ett organ som vill bli ackrediterat måste lämna in en ansökan till Swedac som prövar och bedömer om organet uppfyller de krav som ställs i förordning (EG) nr 765/2008, lagen (2011:791) om ackreditering och teknisk kontroll med tillhörande förordning samt föreskrifter som Swedac har meddelat. Ackrediteringsverksamheten vid Swedac finansieras av kundernas avgifter, som ska täcka samtliga kostnader för ackrediteringen.

Lagen innehåller bestämmelser om att tillsynsmyndighetens beslut får överklagas till allmän förvaltningsdomstol. Särskilt med hänsyn till att antalet leverantörer är begränsat väntas reglerna få så begränsad tillämpning att någon ytterligare måltillströmning av betydelse till de allmänna förvaltningsdomstolarna inte är att vänta. Arbetet bör rymmas inom befintliga ekonomiska ramar.

13 Författningskommentar

13.1 Förslaget till lag med kompletterande bestämmelser till EU-förordningen om elektronisk identifiering

Inledande bestämmelser

1 § Denna lag kompletterar 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 (EU-förordningen om elektronisk identifiering).

Termer och uttryck i lagen har samma betydelse som i EU-förordningen om elektronisk identifiering.

Av *första stycket* framgår att syftet med lagen är att komplettera EU-förordningen om elektronisk identifiering.

I *andra stycket* klargörs att termer och uttryck i lagen har samma betydelse som i EU-förordningen. En lista med definitioner finns i artikel 3 i EU-förordningen.

Granskning av kvalificerade tillhandahållare av betrodda tjänster

2 § Bestämmelser om ackreditering av sådana organ för bedömning av överensstämmelse som i enlighet med artikel 20 i EU-förordningen om elektronisk identifiering ska granska kvalificerade tillhandahållare av betrodda tjänster, finns i förordning (EG) nr 765/2008 om krav för ackreditering och marknadskontroll i samband med saluföring av produkter och upphävande av förordning (EEG) nr 229/93 och i lagen (2011:791) om ackreditering och teknisk kontroll.

Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om

1. krav för ackreditering av organ för bedömning av överensstämmelse,
2. rapportering av bedömningar av överensstämmelse, och
3. hur bedömningar av överensstämmelse ska göras.

Övervägandena finns i avsnitt 7.2.

Av artikel 20.1 och 2 i EU-förordningen följer att kvalificerade tillhandahållare av betrodda tjänster minst vartannat år, och därutöver på tillsynsmyndighetens begäran, ska granskas av ett ackrediterat organ för bedömning av överensstämmelse. Ackreditering ska ske enligt förordning (EG) nr 765/2008. Bestämmelsen i *första stycket* innehåller en upplysning om att ackreditering ska ske enligt förordning (EG) nr 765/2008 och lagen (2011:791) om ackreditering och teknisk kontroll, som kompletterar den förordningen.

Enligt artikel 20.4 i EU-förordningen har Europeiska kommissionen möjlighet att genom genomförandeakter fastställa referensnummer till standarder för ackreditering av organ för bedömning av överensstämmelse, rapportering av bedömningar av överensstämmelse och hur bedömningar av överensstämmelse ska göras. Med stöd av bestämmelsen i *andra stycket* blir det möjligt att meddela nödvändiga föreskrifter i den mån kommissionen inte utnyttjar sitt mandat att meddela genomförande-

akter och att meddela de eventuellt kompletterande föreskrifter som kan behövas för det fall mandatet utnyttjas. I 33 § lagen (2011:791) om ackreditering och teknisk kontroll finns bestämmelser om att regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om själva ackrediteringen. Bemyndigandet i punkt 1 har därför utformats på så sätt att det möjliggör kompletterande föreskrifter om krav för att organen ska ackrediteras.

Certifiering av anordningar

3 § Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om certifiering av anordningar för skapande av kvalificerade elektroniska underskrifter och anordningar för skapande av kvalificerade elektroniska stämplar.

Övervägandena finns i avsnitt 7.3.

Med stöd av paragrafen blir det möjligt att meddela de nationella föreskrifter om certifiering som kan behövas för att komplettera artikel 30 och 39 i EU-förordningen om elektronisk identifiering och de genomförandeakter som Europeiska kommissionen får anta enligt dessa bestämmelser, t.ex. om certifieringsförfarandet och om vilket förfarande som enligt artikel 30.3 b i förordningen får användas medan det pågår en sådan säkerhetsutvärdering som avses i led a i samma förordningsbestämmelse.

Tillsyn

4 § Den myndighet som regeringen bestämmer (tillsynsmyndigheten) ska

1. fullgöra tillsynsorganets uppgifter enligt EU-förordningen om elektronisk identifiering och rättsakter som har meddelats med stöd av den förordningen, och
2. utöva tillsyn över denna lag och föreskrifter som har meddelats med stöd av lagen.

Övervägandena finns i avsnitt 7.8.1.

Medlemsstaterna ska enligt artikel 17 i EU-förordningen utse en tillsynsmyndighet. Tillsynsmyndighetens uppgifter enligt *första punkten* framgår i huvudsak av artikel 17.3, 4 och 6 i EU-förordningen.

Med stöd av *andra punkten* utövar tillsynsmyndigheten även tillsyn över lagen och föreskrifter som har meddelas med stöd av lagen.

5 § Tillsynsmyndigheten har rätt att på begäran få de upplysningar och handlingar som behövs för tillsynen.

Tillsynsmyndigheten har också rätt att få tillträde till områden, lokaler och andra utrymmen där verksamhet som står under tillsyn bedrivs. Denna tillträdesrätt omfattar inte bostäder.

Tillsynsmyndigheten har rätt att få verkställighet hos Kronofogdemyndigheten av beslut som avser åtgärder enligt första och andra styckena. Då gäller bestämmelserna i utsökningsbalken om verkställighet av förpliktelser som inte avser betalningsskyldighet eller avhysning.

Övervägandena finns i avsnitt 7.8.1.

I paragrafen anges vilka befogenheter som tillsynsmyndigheten har. Paragrafen motsvarar i sak 19 § lagen (2000:832) om kvalificerade elek-

troniska signaturer. I likhet med vad som angavs i förarbetena till den lagen (prop. 1999/2000:117 s. 80) bör uppgifter som huvudregel kunna hämtas in formlöst vid kontakter mellan tillsynsmyndigheten och aktörerna på marknaden. Normalt sett torde tillsynsmyndigheten också kunna få det underlag som behövs för tillsynen genom sådana kontakter som anges i *första stycket*. I vissa fall kan det dock vara befogat att med stöd av *andra stycket* få tillträde till platser där verksamhet bedrivs, t.ex. för olika kontroller.

Med stöd av 6 § har tillsynsmyndigheten möjlighet att förelägga någon att lämna uppgifter eller att lämna tillträde till platser där verksamhet bedrivs och att förena förelägganden med vite. I sista hand kan tillsynsmyndigheten få verkställighet hos Kronofogdemyndigheten, se *tredje stycket*. I sådant fall kan bl.a. bestämmelserna om tvång i 2 kap. 17 § utsökningsbalken komma att tillämpas.

6 § Tillsynsmyndigheten får meddela de förelägganden och förbud som behövs för efterlevnaden av

1. EU-förordningen om elektronisk identifiering och rättsakter som har meddelats med stöd av den förordningen, och
2. denna lag och föreskrifter som har meddelats med stöd av lagen.

Förelägganden och förbud får förenas med vite.

Övervägandena finns i avsnitt 7.8.1.

Genom paragrafen, som kompletterar artikel 17.4 j i EU-förordningen om elektronisk identifiering, ges tillsynsmyndigheten möjlighet att vidta de åtgärder som är nödvändiga för att säkerställa att förordningen om elektronisk identifiering följs. Befogenheterna motsvarar dem som tillsynsmyndigheten har enligt 20 § första stycket lagen (2000:832) om kvalificerade elektroniska signaturer.

Tillsynsmyndigheten får själv bestämma när ett föreläggande ska förenas med vite. Det normala torde dock vara att myndigheten först försöker få till stånd en frivillig rättelse.

Paragrafen gör det också möjligt för tillsynsmyndigheten att förelägga någon att lämna upplysningar eller handlingar enligt 5 § första stycket eller att lämna tillträde enligt 5 § andra stycket.

Bestämmelserna om förbud och om vite kompletterar bestämmelsen om sanktioner i artikel 20 i EU-förordningen.

Avgifter

7 § Regeringen eller, efter regeringens bemyndigande, tillsynsmyndigheten får meddela föreskrifter om skyldighet för tillhandahållare av betrodda tjänster att betala avgift för tillsynsmyndighetens verksamhet enligt denna lag.

Övervägandena finns i avsnitt 9.

Paragrafen gör det möjligt att införa ett avgiftssystem för att finansiera tillsynsmyndighetens verksamhet. Paragrafen är uppbyggd på motsvarande sätt som 22 § lagen om kvalificerade elektroniska signaturer men omfattar fler tjänster.

Överklagande

8 § Tillsynsmyndighetens beslut enligt EU-förordningen om elektronisk identifiering och rättsakter som har meddelats med stöd av den förordningen, samt enligt denna lag och föreskrifter som har meddelats med stöd av lagen, får överklagas hos allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

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

Övervägandena finns i avsnitt 10.

I *första och andra styckena* regleras rätten att överklaga tillsynsmyndighetens beslut. Ordningen för överklagande är densamma som enligt 23 § första och andra styckena lagen om kvalificerade elektroniska signaturer.

Bestämmelsen i *tredje stycket* motsvarar 23 § tredje stycket lagen om kvalificerade elektroniska signaturer. Bestämmelsen torde framför allt komma att tillämpas när det krävs skyndsamma åtgärder för att undvika skada.

Ikraftträdande- och övergångsbestämmelser

1. Denna lag träder i kraft den 1 juli 2016.

2. Genom lagen upphävs lagen (2000:832) om kvalificerade elektroniska signaturer.

3. Bestämmelserna om skadestånd i 14 och 15 §§ i den upphävda lagen ska fortsätta att gälla i fråga om skada som har åsamkats före upphävandet.

Övervägandena finns i avsnitt 8.1 och 11.

Dagen för ikraftträdande i *punkt 1* överensstämmer med den dag då de materiella bestämmelserna i EU-förordningen om elektronisk identifiering ska börja tillämpas, se artikel 52.2 i förordningen. Enligt *punkt 2* upphävs samtidigt lagen (2000:832) om kvalificerade elektroniska signaturer. I *punkt 3* anges att den upphävda lagens bestämmelser om skadestånd ska fortsätta att gälla i fråga om skada som åsamkats före upphävandet. I fråga om skada som åsamkas efter denna tidpunkt gäller bestämmelserna i artikel 13 i EU-förordningen, se vidare avsnitt 7.4.

Härutöver finns i artikel 51 i EU-förordningen vissa direkt tillämpliga övergångsbestämmelser.

13.2 Övriga lagförslag

Lagarna följdändras med anledning av att lagen (2000:832) om kvalificerade elektroniska signaturer upphävs. Övervägandena finns i avsnitt 8.2.

Hänvisningar till avancerade elektroniska signaturer enligt 2 § lagen om kvalificerade elektroniska signaturer ersätts med hänvisningar till avancerade elektroniska underskrifter enligt artikel 3 i EU-förordningen om elektronisk identifiering. Dessutom justeras vissa hänvisningar språkligt så att samtliga hänvisningar får en enhetlig utformning.

Bestämmelser som endast allmänt hänvisar till elektroniska signaturer utan att ange att signaturen ska vara av en viss kvalitet, ändras så att hänvisningarna avser elektroniska underskrifter, i enlighet med den nya terminologin i EU-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

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 nätverksport 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.