Den Europæiske Unions
Tidende

L 235

58. årgang

Dansk udgave

Retsforskrifter

9. september 2015

Indhold

(1) EØS-relevant tekst

DA

De akter, hvis titel er trykt med magre typer, er løbende retsakter inden for landbrugspolitikken og har normalt en begrænset gyldighedsperiode.

Titlen på alle øvrige akter er trykt med fede typer efter en asterisk.

[1] EØS-relevant tekst

II

(Ikke-lovgivningsmæssige retsakter)

FORORDNINGER

KOMMISSIONENS GENNEMFØRELSESFORORDNING (EU) 2015/1501

af 8. september 2015

om interoperabilitetsrammen i henhold til artikel 12, stk. 8, i Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked

(EØS-relevant tekst)

EUROPA-KOMMISSIONEN HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde,

under henvisning til Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF ([1]), særlig artikel 12, stk. 8, og

ud fra følgende betragtninger:

(1) Det fremgår af artikel 12, stk. 2, i forordning (EU) nr. 910/2014, at der bør indføres en interoperabilitetsramme med henblik på at sikre interoperabilitet mellem nationale elektroniske identifikationsordninger anmeldt i henhold til forordningens artikel 9, stk. 1.

(2) Knudepunkter spiller en central rolle i sammenkoblingen af medlemsstaternes elektroniske identifikationsordninger. Deres bidrag forklares i dokumentationen til Connecting Europe-faciliteten, som blev indført ved Europa-Parlamentets og Rådets forordning (EU) nr. 1316/2013 ([2]), herunder »eIDAS-knudepunktets« funktioner og komponenter.

(3) Hvis en medlemsstat eller Kommissionen leverer software, som skal muliggøre autentifikation til et knudepunkt, der drives i en anden medlemsstat, kan den part, der leverer og opdaterer softwaren i autentifikationsmekanismen, aftale med den part, der hoster softwaren, hvordan driften af autentifikationsmekanismen skal forvaltes. En sådan aftale bør ikke pålægge den part, der står for hosting, urimelige tekniske krav eller omkostninger (herunder til support, forpligtelser, hosting og andre omkostninger).

(4) I det omfang gennemførelsen af interoperabilitetsrammen kræver det, kan Kommissionen i samarbejde med medlemsstaterne udarbejde yderligere tekniske specifikationer, som giver flere oplysninger om tekniske krav, jf. denne forordning, navnlig i forlængelse af udtalelser fra samarbejdsnetværket, jf. artikel 14, litra d), i Kommissionens gennemførelsesafgørelse (EU) 2015/296 ([3]). Sådanne specifikationer bør udarbejdes som en del af digitaltjenesteinfrastrukturerne i forordning (EU) nr. 1316/2013, som fastsætter midlerne til den praktiske implementering af et modul for elektronisk identifikation.

([1]) EUT L 257 af 28.8.2014, s. 73.

([2]) Europa-Parlamentets og Rådets forordning (EU) nr. 1316/2013 af 11. december 2013 om oprettelse af Connecting Europe-faciliteten, om ændring af forordning (EU) nr. 913/2010 og om ophævelse af forordning (EF) nr. 680/2007 og (EF) nr. 67/2010 (EUT L 348 af 20.12.2013, s. 129).

([3]) Kommissionens gennemførelsesafgørelse (EU) 2015/296 af 24. februar 2015 om fastlæggelse af de proceduremæssige ordninger for samarbejde mellem medlemsstaterne om elektronisk identifikation i henhold til artikel 12, stk. 7, i Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked (EUT L 53 af 25.2.2015, s. 14).

(5) De tekniske krav i denne forordning bør finde anvendelse på trods af eventuelle ændringer af de tekniske specifikationer, som eventuelt udarbejdes i henhold til artikel 12 i denne forordning.

(6) Der er i udstrakt grad blevet taget hensyn til pilotprojektet i stor skala, STORK, herunder specifikationer udarbejdet i forbindelse hermed, og principperne og begreberne i den europæiske interoperabilitetsramme for europæiske offentlige tjenester i forbindelse med udarbejdelsen af bestemmelserne for interoperabilitetsrammen, som er fastsat i denne forordning.

(7) Der er i udstrakt grad blevet taget hensyn til resultaterne af samarbejdet mellem medlemsstaterne.

(8) Foranstaltningerne i denne forordning er i overensstemmelse med udtalelsen fra det udvalg, der er nedsat ved artikel 48 i forordning (EU) nr. 910/2014 —

VEDTAGET DENNE FORORDNING:

Artikel 1

Genstand

Denne forordning fastlægger de tekniske og operationelle krav til interoperabilitetsrammen med henblik på at sikre interoperabiliteten af de elektroniske identifikationsordninger, som medlemsstaterne anmelder til Kommissionen.

Disse krav omfatter:

a) tekniske minimumskrav for sikringsniveauerne og kortlægning af nationale sikringsniveauer for anmeldte elektroniske identifikationsmidler udstedt i overensstemmelse med anmeldte identifikationsordninger i henhold til artikel 8 i forordning (EU) nr. 910/2014, som fastsat i artikel 3 og 4

b) tekniske minimumskrav for interoperabilitet, som fastsat i artikel 5 og 8

c) det minimum af personidentifikationsdata, der entydigt repræsenterer en fysisk eller juridisk person, som fastsat i artikel 11 og i bilaget

d) fælles operationelle sikkerhedsstandarder, som fastsat i artikel 6, 7, 9 og 10

e) tvistbilæggelsesordninger, som fastsat i artikel 13.

Artikel 2

Definitioner

I denne forordning forstås ved:

1) »knudepunkt«: et forbindelsespunkt, som er en del af den elektroniske identifikationsinteroperabilitetsarkitektur, som indgår i grænseoverskridende autentifikation af personer, og som er i stand til at genkende, behandle eller videregive oplysninger til andre knudepunkter ved at give en medlemsstats nationale identifikationsinfrastruktur mulighed for at kommunikere med en anden medlemsstats nationale elektroniske identifikationsinfrastruktur

2) »knudepunktsoperatør«: enhed, som er ansvarlig for at sikre, at knudepunktet fungerer korrekt og sikkert som forbindelsespunkt.

Artikel 3

Tekniske minimumskrav for sikringsniveauer

De tekniske minimumskrav for sikringsniveauerne er som fastsat i Kommissionens gennemførelsesforordning (EU) 2015/1502 ([1]).

Artikel 4

Kortlægning af nationale sikringsniveauer

Kortlægningen af nationale sikringsniveauer for anmeldte elektroniske identifikationsordninger følger kravene i Kommissionens gennemførelsesforordning (EU) 2015/1502. Resultaterne af kortlægningen anmeldes til Kommissionen ved hjælp af anmeldelsesformularen i Kommissionens gennemførelsesafgørelse (EU) 2015/1505 ([2]).

Artikel 5

Knudepunkter

1. Et knudepunkt i én medlemsstat kan opnå forbindelse til knudepunkter i andre medlemsstater.

2. Knudepunkterne kan skelne mellem offentlige myndigheder og andre modtagerparter ved hjælp af tekniske midler.

3. En medlemsstats implementering af de tekniske krav i denne forordning pålægger ikke andre medlemsstater urimelige tekniske krav eller omkostninger, for at de kan fungere sammen med den implementering, som førstnævnte medlemsstat har indført.

Artikel 6

Datasikkerhed og fortrolighed

1. Beskyttelse af datasikkerhed og fortrolighed i forbindelse med dataudveksling og vedligeholdelse af dataintegritet mellem knudepunkterne sikres ved hjælp af de bedste tilgængelige tekniske løsninger og beskyttelsespraksis.

2. Knudepunkterne lagrer ingen personlige data med undtagelse af dem, der er nødvendige til det i artikel 9, stk. 3, beskrevne formål.

Artikel 7

Dataintegritet og kommunikationens ægthed

Kommunikation mellem knudepunkter sikrer datas integritet og ægthed, samt at alle anmodninger og svar er ægte og ikke er blevet manipuleret. Med henblik herpå bruger knudepunkterne løsninger, som med succes er blevet anvendt til grænseoverskridende operationer.

([1]) Kommissionens gennemførelsesforordning (EU) 2015/1502 af 8. september 2015 om fastlæggelse af tekniske minimumsspecifikationer og procedurer for fastsættelse af sikringsniveauer for elektroniske identifikationsmidler i henhold til artikel 8, stk. 3, i Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked (se side 7 i denne EUT).

([2]) Kommissionens gennemførelsesafgørelse (EU) 2015/1505 af 8. september 2015 om fastlæggelse af tekniske specifikationer og formater for positivlister i henhold til artikel 22, stk. 5, i Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked (se side 26 i denne EUT).

Artikel 8

Kommunikationens format

Knudepunkter gør til syntaks brug af fælles beskedformater, der er baseret på standarder, som allerede er blevet anvendt i flere tilfælde mellem medlemsstater, og som har vist sig at virke i et operationelt miljø. Syntaksen giver mulighed for:

a) korrekt behandling af det minimum af personidentifikationsdata, der entydigt repræsenterer en fysisk eller juridisk person

b) korrekt behandling af det elektroniske identifikationsmiddels sikringsniveau

c) at skelne mellem offentlige myndigheder og modtagerparter

d) fleksibilitet til at opfylde kravene til yderligere attributter i forbindelse med identifikation.

Artikel 9

Forvaltning af sikkerhedsoplysninger og metadata

1. Knudepunktsoperatøren kommunikerer metadata vedrørende knudepunktets forvaltning på en standardiseret måde, hvor de kan behandles af en maskine, og på en sikker og pålidelig måde.

2. Som minimum kan de parametre, der er relevante for sikkerheden, indhentes automatisk.

3. Knudepunktsoperatøren lagrer data, som i tilfælde af en hændelse giver mulighed for at gendanne beskedudvekslingssekvensen med henblik på at fastslå, hvor og hvordan hændelsen fandt sted. Disse data lagres i den periode, der er angivet i national lovgivning, og består som minimum af følgende elementer:

a) identifikation af knudepunktet

b) identifikation af beskeden

c) dato og tidspunkt for beskeden.

Artikel 10

Informationssikring og sikkerhedsstandarder

1. Operatører af knudepunkter, hvor der foretages autentifikation, dokumenterer over for knudepunkter, der deltager i interoperabilitetsrammen, at knudepunktet opfylder kravene i standarden ISO/IEC 27001, enten i form af certificering eller en tilsvarende vurderingsmetode eller ved at opfylde kravene i national lovgivning.

2. Knudepunktsoperatøren udruller sikkerhedskritiske opdateringer uden unødig forsinkelse.

Artikel 11

Personidentifikationsdata

1. Det minimum af personidentifikationsdata, der entydigt repræsenterer en fysisk eller juridisk person, lever op til de krav, der fremgår af bilaget, når disse data anvendes på tværs af grænser.

2. Det minimum af personidentifikationsdata for en fysisk person, der repræsenterer en juridisk person, indeholder en kombination af de attributter, der er oplistet i bilaget for fysiske og juridiske personer, når de anvendes på tværs af grænser.

3. Data sendes som originale tegn og, hvor muligt, også omskrevet til latinske bogstaver.

Artikel 12

Tekniske specifikationer

1. Hvis gennemførelsesprocessen for interoperabilitetsrammen retfærdiggør det, kan det samarbejdsnetværk, som er oprettet ved gennemførelsesafgørelse (EU) 2015/296, vedtage udtalelser om behovet for at udvikle tekniske specifikationer i henhold til denne afgørelses artikel 14, litra d). Sådanne tekniske specifikationer indeholder yderligere detaljer om tekniske krav, som anført i denne forordning.

2. I henhold til den udtalelse, der henvises til i stk. 1, udvikler Kommissionen i samarbejde med medlemsstaterne de tekniske specifikationer som en del af digitaltjenesteinfrastrukturerne i forordning (EU) nr. 1316/2013.

3. Samarbejdsnetværket vedtager en udtalelse i henhold til artikel 14, litra d), i gennemførelsesafgørelse (EU) 2015/296, hvori det vurderer, om og i hvor høj grad de tekniske specifikationer, der er udviklet under stk. 2, stemmer overens med det behov, der blev klarlagt i den udtalelse, der henvises til i stk. 1, eller med kravene i denne forordning. Det kan anbefale, at medlemsstaterne tager hensyn til de tekniske specifikationer, når de implementerer interoperabilitetsrammen.

4. Kommissionen stiller en referenceimplementering til rådighed som eksempel på en fortolkning af de tekniske specifikationer. Medlemsstaterne kan anvende referenceimplementeringen eller bruge den som eksempel, når de tester andre implementeringer af tekniske specifikationer.

Artikel 13

Tvistbilæggelse

1. Eventuelle tvister om interoperabilitetsrammen løses om muligt af de pågældende medlemsstater gennem forhandling.

2. Hvis der ikke findes en løsning i overensstemmelse med stk. 1, har det samarbejdsnetværk, der er oprettet i henhold til artikel 12 i Kommissionens gennemførelsesafgørelse (EU) 2015/296, kompetence til at bilægge tvisten i henhold til dets forretningsorden.

Artikel 14

Ikrafttræden

Denne forordning træder i kraft på tyvendedagen efter offentliggørelsen i *Den Europæiske Unions Tidende*.

Denne forordning er bindende i alle enkeltheder og gælder umiddelbart i hver medlemsstat.

Udfærdiget i Bruxelles, den 8. september 2015.

På Kommissionens vegne

Jean-Claude JUNCKER

Formand

BILAG

Krav til det minimum af personidentifikationsdata, som entydigt repræsenterer en fysisk eller juridisk person som omhandlet i artikel 11

1. **Minimum af data fastsat for en fysisk person**

Det minimum af data, der er fastsat for en fysisk person, indeholder følgende obligatoriske oplysninger:

a) Nuværende efternavn(e)

b) Nuværende fornavn(e)

c) Fødselsdato

d) Et entydigt identifikationsnummer, som er tildelt af den afsendende medlemsstat i overensstemmelse med de tekniske specifikationer med henblik på grænseoverskridende identifikation, og som så vidt muligt består over tid.

Det minimum af data, der er fastsat for en fysisk person, kan indeholde en eller flere af følgende supplerende oplysninger:

a) Fornavn(e) og efternavn(e) ved fødslen

b) Fødested

c) Nuværende adresse

d) Køn.

2. **Minimum af data fastsat for en juridisk person**

Det minimum af data, der er fastsat for en juridisk person, indeholder følgende obligatoriske oplysninger:

a) Nuværende officielle navn

b) Et entydigt identifikationsnummer, som er tildelt af den afsendende medlemsstat i overensstemmelse med de tekniske specifikationer med henblik på grænseoverskridende identifikation, og som så vidt muligt består over tid.

Det minimum af data, der er fastsat for en juridisk person, kan indeholde en eller flere af følgende supplerende oplysninger:

a) Nuværende adresse

b) Momsregistreringsnummer

c) Skatteregistreringsnummer

d) Det identifikationsnummer, der henvises til i artikel 3, stk. 1, i Europa-Parlamentets og Rådets direktiv 2009/101/EF ([1])

e) Identifikatoren for juridiske enheder, som der henvises til i Kommissionens gennemførelsesforordning (EU) nr. 1247/2012 ([2])

f) EORI-nummer (registrerings- og identifikationsnummer for økonomiske operatører), som der henvises til i Kommissionens gennemførelsesforordning (EU) nr. 1352/2013 ([3])

g) Punktafgiftsnummeret i artikel 2, stk. 12, i Rådets forordning (EU) nr. 389/2012 ([4]).

([1]) Europa-Parlamentets og Rådets direktiv 2009/101/EF af 16. september 2009 om samordning af de garantier, som kræves i medlemsstaterne af de i traktatens artikel 48 nævnte selskaber til beskyttelse af såvel selskabsdeltagernes som tredjemands interesser, med det formål at gøre disse garantier lige byrdefulde (EUT L 258 af 1.10.2009, s. 11).

([2]) Kommissionens gennemførelsesforordning (EU) nr. 1247/2012 af 19. december 2012 om gennemførelsesmæssige tekniske standarder for formatet for og hyppigheden af handelsindberetninger til transaktionsregistre i henhold til Europa-Parlamentets og Rådets forordning (EU) nr. 648/2012 om OTC-derivater, centrale modparter og transaktionsregistre (EUT L 352 af 21.12.2012, s. 20).

([3]) Kommissionens gennemførelsesforordning (EU) nr. 1352/2013 af 4. december 2013 om fastlæggelse af de blanketter, der er foreskrevet i Europa-Parlamentets og Rådets forordning (EU) nr. 608/2013 om toldmyndighedernes håndhævelse af intellektuelle ejendomsrettigheder (EUT L 341 af 18.12.2013, s. 10).

([4]) Rådets forordning (EU) nr. 389/2012 af 2. maj 2012 om administrativt samarbejde på punktafgiftsområdet og om ophævelse af forordning (EF) nr. 2073/2004 (EUT L 121 af 8.5.2012, s. 1).

KOMMISSIONENS GENNEMFØRELSESFORORDNING (EU) 2015/1502

af 8. september 2015

om fastlæggelse af tekniske minimumsspecifikationer og procedurer for fastsættelse af sikringsniveauer for elektroniske identifikationsmidler i henhold til artikel 8, stk. 3, i Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked

(EØS-relevant tekst)

EUROPA-KOMMISSIONEN HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde,

under henvisning til Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF ([1]), særlig artikel 8, stk. 3, og

ud fra følgende betragtninger:

(1) Det fremgår af artikel 8 i forordning (EU) nr. 910/2014, at en elektronisk identifikationsordning, der er anmeldt i henhold til artikel 9, stk. 1, skal anføre sikringsniveauerne »lav«, »betydelig« og/eller »høj« for de elektroniske identifikationsmidler, der er udstedt under den pågældende ordning.

(2) Det er væsentligt at fastsætte de tekniske minimumsspecifikationer, minimumsstandarder og procedurer for at opnå en fælles forståelse af sikringsniveauernes detaljer og sikre interoperabilitet, når der skal foretages en sammenligning af de nationale sikringsniveauer for anmeldte elektroniske identifikationsordninger og sikringsniveauerne i artikel 8, jf. artikel 12, stk. 4, litra b), i forordning (EU) nr. 910/2014.

(3) Den internationale standard ISO/IEC 29115 betragtes i forbindelse med de minimumsspecifikationer og procedurer, der er fastsat i denne gennemførelsesforordning, som den vigtigste internationale standard inden for fastsættelse af sikringsniveauer for elektroniske identifikationsmidler. Forordning (EU) nr. 910/2014 adskiller sig imidlertid fra den internationale standard hvad angår kravene til godtgørelse og kontrol af identitet samt den måde, hvorpå der tages hensyn til forskellene i medlemsstaternes identitetsordninger og eksisterende værktøjer i EU med samme formål. Derfor bør bilaget, selv om det bygger på denne internationale standard, ikke henvise til det specifikke indhold i ISO/IEC 29115.

(4) Denne forordning er blevet udarbejdet på grundlag af en resultatorienteret tilgang, som anses for at være den bedst egnede, hvilket også afspejles i de definitioner, der anvendes til at beskrive de forskellige termer og begreber. De tager hensyn til målet med forordning (EU) nr. 910/2014 i forbindelse med fastsættelse af sikringsniveauer for elektroniske identifikationsmidler. Derfor bør pilotprojektet i stor skala STORK og de specifikationer, som er udviklet i forbindelse hermed, og definitionerne og begreberne i ISO/IEC 29115 i særdeleshed tages i betragtning, når der fastsættes minimumsspecifikationer og procedurer i denne gennemførelsesforordning.

(5) Autoritative kilder kan antage mange former, f.eks. registre, dokumenter eller organer, afhængig af hvilken kontekst et identitetsbevis skal kontrolleres i. Autoritative kilder kan variere fra medlemsstat til medlemsstat selv i en lignende kontekst.

(6) Kravene til godtgørelse og kontrol af identitet bør tage hensyn til forskellige systemer og forskellig praksis, samt sikre et tilstrækkelig højt sikringsniveau til at opbygge den nødvendige tillid. Derfor bør godkendelse af procedurer, som tidligere er blevet brugt til andre formål end udstedelse af elektroniske identifikationsmidler, gøres betinget af, at det bekræftes, at disse procedurer lever op til kravene for det tilsvarende sikringsniveau.

([1]) EUT L 257 af 28.8.2014, s. 73.

(7) Der anvendes typisk bestemte autentifikationsfaktorer, f.eks. delte hemmeligheder, fysiske enheder og fysiske kendetegn. Imidlertid bør der opfordres til at anvende et større antal autentifikationsfaktorer, navnlig fra forskellige kategorier af faktorer, for at øge sikkerheden i autentifikationsprocessen.

(8) Forordningen bør ikke påvirke juridiske personers repræsentationsret. Imidlertid bør det sikres i bilaget, at der er overensstemmelse mellem kravene til elektroniske identifikationsmidler for fysiske og juridiske personer.

(9) Vigtigheden af informationssikkerhed og service management-systemer bør anerkendes, såvel som vigtigheden af at anvende anerkendte metoder og de principper, der indgår i standarder som ISO/IEC 27000 og ISO/IEC 20000-serien.

(10) Der bør også tages hensyn til god praksis i forbindelse med medlemsstaternes sikringsniveauer.

(11) IT-sikkerhedscertificering baseret på internationale standarder er et vigtigt værktøj til at kontrollere, at produkter overholder kravene til sikkerhedsregler i denne gennemførelsesforordning.

(12) Det udvalg, der er omhandlet i artikel 48 i forordning (EU) nr. 910/2014, har ikke afgivet en udtalelse inden for den af formanden fastsatte frist —

VEDTAGET DENNE FORORDNING:

Artikel 1

1. Sikringsniveauerne »lav«, »betydelig« og »høj« for elektroniske identifikationsmidler, der udstedes under en anmeldt elektronisk identifikationsordning, defineres med henvisning til de minimumsspecifikationer og procedurer, der er fastsat i bilaget.

2. De specifikationer og procedurer, der er fastsat i bilaget, anvendes til at fastsætte sikringsniveauet for elektroniske identifikationsmidler, der er udstedt under en anmeldt elektronisk identifikationsordning, ved at finde frem til følgende elementers pålidelighed og kvalitet:

a) tilmelding, som fastsat i afsnit 2.1 i bilaget til denne forordning, jf. artikel 8, stk. 3, litra a), i forordning (EU) nr. 910/2014

b) håndtering af elektroniske identifikationsmidler, som fastsat i afsnit 2.2 i bilaget til denne forordning, jf. artikel 8, stk. 3, litra b) og f), i forordning (EU) nr. 910/2014

c) autentifikation, som fastsat i afsnit 2.3 i bilaget til denne forordning, jf. artikel 8, stk. 3, litra c), i forordning (EU) nr. 910/2014

d) håndtering og organisering, som fastsat i afsnit 2.4 i bilaget til denne forordning, jf. artikel 8, stk. 3, litra d) og e), i forordning (EU) nr. 910/2014.

3. Hvis et elektronisk identifikationsmiddel, som er udstedt under en anmeldt elektronisk identifikationsordning, opfylder krav henhørende under et højere sikringsniveau, antages det at opfylde de tilsvarende krav på et lavere sikringsniveau.

4. Medmindre andet fremgår af den relevante del af bilaget, skal alle elementer i bilaget for et sikringsniveau for et elektronisk identifikationsmiddel, som er udstedt under en anmeldt elektronisk identifikationsordning, være opfyldt, for at det kan anses for at opfylde det pågældende sikringsniveau.

Artikel 2

Denne forordning træder i kraft på tyvendedagen efter offentliggørelsen i *Den Europæiske Unions Tidende*.

Denne forordning er bindende i alle enkeltheder og gælder umiddelbart i hver medlemsstat.

Udfærdiget i Bruxelles, den 8. september 2015.

På Kommissionens vegne

Jean-Claude JUNCKER

Formand

BILAG

Tekniske specifikationer og procedurer til angivelse af sikringsniveauerne »lav«, »betydelig« og »høj« for elektroniske kommunikationsmidler udstedt under en anmeldt elektronisk identifikationsordning

1. Definitioner

I dette bilag forstås ved:

1) »autoritativ kilde«: enhver kilde, der uanset dens form kan anvendes til at opnå nøjagtige data, oplysninger og/eller beviser, der kan bruges til at fastslå en identitet

2) »autentifikationsfaktor«: en faktor, som kan bekræftes at være relateret til en person, og som falder inden for en af følgende kategorier:

   a) »indehaverbaseret autentifikationsfaktor«: en autentifikationsfaktor, som den kontrollerede skal bevise at være i besiddelse af

   b) »vidensbaseret autentifikationsfaktor«: en autentifikationsfaktor, som den kontrollerede skal bevise at have kendskab til

   c) »iboende autentifikationsfaktor«: en autentifikationsfaktor, der er baseret på et fysisk træk hos en fysisk person, og som den kontrollerede skal bevise at have

3) »dynamisk autentifikation«: en elektronisk proces, som anvender kryptografi eller andre teknikker til på forlangende at skabe et elektronisk bevis for, at den kontrollerede har adgang til eller er i besiddelse af identifikationsdata, og som ændres ved hver autentifikation mellem den, der søger adgang til systemet, og det system, der kontrollerer dennes identitet

4) »system til forvaltning af informationssikkerhed«: en række processer og procedurer, der har til formål at begrænse de risici, der knytter sig til informationssikkerhed, til et acceptabelt niveau.

2. Tekniske minimumsspecifikationer og procedurer

De elementer i de tekniske specifikationer og procedurer, som er fastsat i nærværende bilag, skal bruges til at fastslå, hvordan kravene og kriterierne i artikel 8 i forordning (EU) nr. 910/2014 finder anvendelse på elektroniske identifikationsmidler udstedt under en elektroniske identifikationsordning.

2.1. *Tilmelding*

2.1.1. Ansøgning og registrering

Sikringsniveau	Obligatoriske elementer
Lav	1. Det er sikret, at ansøgeren er bekendt med de betingelser og vilkår, som gælder for brugen af det elektroniske identifikationsmiddel. 2. Det er sikret, at ansøgeren er bekendt med de anbefalede sikkerhedsforanstaltninger, som har at gøre med brugen af det elektroniske identifikationsmiddel. 3. De data, som er relevante for godtgørelse og kontrol af identitet, er indsamlet.
Betydelig	Samme niveau som »lav«.
Høj	Samme niveau som »lav«.

2.1.2. Godtgørelse og kontrol af identitet (fysiske personer)

Sikringsniveau	Obligatoriske elementer
Lav	1. Det kan antages, at personen er i besiddelse af et bevis, som er anerkendt af den medlemsstat, hvor ansøgningen om det elektroniske identifikationsmiddel indgives, og som dokumenterer den påståede identitet. 2. Det kan antages, at beviset er ægte, eller at det eksisterer i henhold til en autoritativ kilde, og beviset skal se ud til at være gyldigt. 3. Det er kendt af en autoritativ kilde, at den påståede identitet eksisterer, og det kan antages, at den person, som gør krav på den pågældende identitet, er en og samme person.
Betydelig	Kravene til sikringsniveauet »lav« samt et af alternativerne i punkt 1-4 nedenfor skal være opfyldt: 1. Det er blevet kontrolleret, at personen er i besiddelse af et bevis, som er anerkendt af den medlemsstat, hvor ansøgningen om det elektroniske identifikationsmiddel indgives, og som dokumenterer den påståede identitet, og beviset er blevet kontrolleret for at fastslå, at det er ægte, eller det vides i henhold til en autoritativ kilde, at beviset eksisterer og er relateret til en fysisk person, og der er taget skridt til at nedbringe risikoen for, at den pågældende persons identitet ikke er den, den påstås at være, under hensyntagen til risikoen for at beviset kan være blevet tabt, stjålet, suspenderet, tilbagekaldt eller være udløbet, eller 2. Der er blevet fremvist et identitetsdokument i løbet af registreringsprocessen i den medlemsstat, hvor dokumentet blev udstedt, og dokumentet ser ud til at tilhøre den person, som fremlægger det, og der er taget skridt til at nedbringe risikoen for, at den pågældende persons identitet ikke er den, den påstås at være, under hensyntagen til risikoen for at dokumenterne kan være blevet tabt, stjålet, suspenderet, inddraget eller være udløbet, eller 3. Hvis procedurer, der tidligere er blevet brugt af en offentlig eller privat enhed i den pågældende medlemsstat til et andet formål end udstedelse af elektroniske identifikationsmidler på en måde, der svarer til den, der er fastsat i afsnit 2.1.2, sikrer, at sikringsniveauet »betydelig« er opfyldt, behøver den enhed, der er ansvarlig for registreringen, ikke at gentage de tidligere procedurer, forudsat at den tilsvarende sikring bekræftes af et overensstemmelsesvurderingsorgan, jf. artikel 2, stk. 13, i Europa-Parlamentets og Rådets forordning (EF) nr. 765/2008 ([1]), eller af et tilsvarende organ eller 4. Hvis elektroniske identifikationsmidler udstedes på grundlag af et gyldigt anmeldt elektronisk identifikationsmiddel med sikringsniveau »betydelig« eller »høj«, og der tages hensyn til eventuelle ændringer i personidentifikationsdata, kræves det ikke, at processerne for godtgørelse og kontrol af identitet gentages. Hvis det elektroniske identifikationsmiddel, der anvendes til at foretage kontrol, ikke er blevet anmeldt, skal sikringsniveauet »betydelig« eller »høj« bekræftes af et overensstemmelsesvurderingsorgan, jf. artikel 2, stk. 13, i forordning (EF) nr. 765/2008, eller af et tilsvarende organ.

Sikringsniveau	Obligatoriske elementer
Høj	Kravene i punkt 1 eller punkt 2 skal være opfyldt: 1. Kravene til sikringsniveauet »betydelig« samt et af alternativerne i punkt a)-c) nedenfor skal være opfyldt: a) Hvis det er blevet kontrolleret, at personen er i besiddelse af et fotografisk eller biometrisk identifikationsbevis, som er anerkendt af den medlemsstat, hvor ansøgningen om et elektronisk identifikationsmiddel er indgivet, og beviset dokumenterer den påståede identitet, kontrolleres beviset med henblik på at fastslå, at det er gyldigt i henhold til en autoritativ kilde og ansøgeren kan identificeres som havende den påståede identitet ved sammenligning af et eller flere af personens fysiske kendetegn med en autoritativ kilde eller b) Hvis procedurer, der tidligere er blevet brugt af en offentlig eller privat enhed i den pågældende medlemsstat til et andet formål end udstedelse af elektroniske identifikationsmidler på en måde, der svarer til den, der er fastsat i afsnit 2.1.2, sikrer, at sikringsniveauet »høj« er opfyldt, behøver den enhed, der er ansvarlig for registreringen, ikke at gentage de tidligere procedurer, forudsat at den tilsvarende sikring bekræftes af et overensstemmelsesvurderingsorgan, jf. artikel 2, stk. 13, i Europa-Parlamentets og Rådets forordning (EF) nr. 765/2008, eller af et tilsvarende organ og der tages skridt til at kontrollere, at resultaterne af tidligere procedurer fortsat er gyldige eller c. Hvis elektroniske identifikationsmidler udstedes på grundlag af et gyldigt anmeldt elektronisk identifikationsmiddel med sikringsniveauet »høj«, og der tages hensyn til eventuelle ændringer i personidentifikationsdata, kræves det ikke, at processerne for godtgørelse og kontrol af identitet gentages. Hvis det elektroniske identifikationsmiddel, der anvendes til at foretage kontrol, ikke er blevet anmeldt, skal sikringsniveauet »høj« bekræftes af et overensstemmelsesvurderingsorgan, jf. artikel 2, stk. 13, i forordning (EF) nr. 765/2008, eller af et tilsvarende organ. og der tages skridt til at kontrollere, at resultaterne af den foregående procedure for udstedelse af et anmeldt elektronisk identifikationsmiddel fortsat er gyldige. ELLER 2. Hvis ansøgeren ikke fremlægger et anerkendt fotografisk eller biometrisk identifikationsbevis, anvendes de samme procedurer for fremskaffelse af et anerkendt fotografisk eller biometrisk identifikationsbevis, som dem der anvendes i den pågældende medlemsstat af den enhed, der er ansvarlig for registrering.

([1]) Europa-Parlamentets og Rådets forordning (EF) nr. 765/2008 af 9. juli 2008 om kravene til akkreditering og markedsovervågning i forbindelse med markedsføring af produkter og om ophævelse af Rådets forordning (EØF) nr. 339/93 (EUT L 218 af 13.8.2008, s. 30).

2.1.3. Godtgørelse og kontrol af identitet (juridiske personer)

Sikringsniveau	Obligatoriske elementer
Lav	1. Den juridiske persons påståede identitet dokumenteres med et bevis, som er anerkendt af den medlemsstat, hvor ansøgningen om det elektroniske identifikationsmiddel indgives.

Sikringsniveau	Obligatoriske elementer
	2. Beviset fremstår gyldigt og kan antages at være ægte eller eksistere i henhold til en autoritativ kilde, hvis opførelsen af en juridisk person i den autoritative kilde er frivillig og er reguleret af en aftale mellem den juridiske person og den autoritative kilde. 3. Den juridiske person er ikke registreret af den autoritative kilde med en status, der afholder den juridiske person fra at agere som sådan.
Betydelig	Kravene til sikringsniveauet »lav« samt et af alternativerne i punkt 1-3 nedenfor skal være opfyldt: 1. Den juridiske persons påståede identitet dokumenteres med et bevis, som er anerkendt af den medlemsstat, hvor ansøgningen om det elektroniske identifikationsmiddel indgives, herunder den juridiske persons navn, retlige form og (eventuelt) registreringsnummer, og beviset kontrolleres for at fastslå, om det er ægte eller kendt af en autoritativ kilde, hvis opførelsen af den juridiske person i den autoritative kilde er påkrævet, for at den juridiske person kan være aktiv i sin branche og der er taget skridt til at nedbringe risikoen for, at den juridiske persons identitet ikke er den, som den påstås at være, under hensyntagen til risikoen for at dokumenterne kan være blevet tabt, stjålet, suspenderet, inddraget eller være udløbet, eller 2. Hvis de procedurer, der tidligere er blevet brugt af en offentlig eller privat enhed i den pågældende medlemsstat til et andet formål end udstedelse af elektroniske identifikationsmidler på en måde, der svarer til den, der er fastsat i afsnit 2.1.3, sikrer, at sikringsniveauet »betydelig« er opfyldt, behøver den enhed, der er ansvarlig for registreringen, ikke at gentage de tidligere procedurer, forudsat at den tilsvarende sikring bekræftes af et overensstemmelsesvurderingsorgan, jf. artikel 2, stk. 13, i forordning (EF) nr. 765/2008, eller af et tilsvarende organ eller 3. Hvis elektroniske identifikationsmidler udstedes på grundlag af et gyldigt anmeldt elektronisk identifikationsmiddel med sikringsniveauet »betydelig« eller »høj«, kræves det ikke, at processerne for godtgørelse og kontrol af identitet gentages. Hvis det elektroniske identifikationsmiddel, der anvendes til at foretage kontrol, ikke er blevet anmeldt, skal sikringsniveauet »betydelig« eller »høj« bekræftes af et overensstemmelsesvurderingsorgan, jf. artikel 2, stk. 13, i forordning (EF) nr. 765/2008, eller af et tilsvarende organ.
Høj	Kravene til sikringsniveauet »betydelig« samt et af alternativerne i punkt 1-3 nedenfor skal være opfyldt: 1. Den juridiske persons påståede identitet dokumenteres med et bevis, som er anerkendt af den medlemsstat, hvor ansøgningen om det elektroniske identifikationsmiddel indgives, herunder den juridiske persons navn, retlige form og mindst et entydigt identifikationsnummer, der repræsenterer den juridiske person, og som anvendes i nationale sammenhænge og beviset kontrolleres for at fastslå, at det er gyldigt i henhold til en autoritativ kilde, eller

Sikringsniveau	Obligatoriske elementer
	2. Hvis de procedurer, der tidligere er blevet brugt af en offentlig eller privat enhed i den pågældende medlemsstat til et andet formål end udstedelse af elektroniske identifikationsmidler på en måde, der svarer til den, der er fastsat i afsnit 2.1.3, sikrer, at sikringsniveauet »høj« er opfyldt, behøver den enhed, der er ansvarlig for registreringen, ikke at gentage de tidligere procedurer, forudsat at den tilsvarende sikring bekræftes af et overensstemmelsesvurderingsorgan, jf. artikel 2, stk. 13, i forordning (EF) nr. 765/2008, eller af et tilsvarende organ og der tages skridt til at kontrollere, at resultaterne af den foregående procedure fortsat er gyldige eller 3. Hvis elektroniske identifikationsmidler udstedes på grundlag af et gyldigt anmeldt elektronisk identifikationsmiddel med sikringsniveauet »høj«, kræves det ikke, at processerne for godtgørelse og kontrol af identitet gentages. Hvis det elektroniske identifikationsmiddel, der anvendes til at foretage kontrol, ikke er blevet anmeldt, skal sikringsniveauet »høj« bekræftes af et overensstemmelsesvurderingsorgan, jf. artikel 2, stk. 13, i forordning (EF) nr. 765/2008, eller af et tilsvarende organ. og der tages skridt til at kontrollere, at resultaterne af den foregående procedure for udstedelse af et anmeldt elektronisk identifikationsmiddel fortsat er gyldige.

2.1.4. Forbindelser mellem elektroniske identifikationsmidler for fysiske og juridiske personer

Følgende vilkår gælder for forbindelser mellem fysiske og juridiske personers elektroniske identifikationsmidler (»forbindelse«), hvis sådanne findes:

1) Det skal være muligt at suspendere og/eller ophæve en forbindelse. En forbindelses livscyklus (f.eks. aktivering, suspendering, fornyelse, ophævelse) skal forvaltes i henhold til nationalt anerkendte procedurer.

2) En fysisk person, hvis elektroniske identifikationsmiddel er forbundet til en juridisk persons elektroniske identifikationsmiddel, kan delegere brugen af forbindelsen til en anden fysisk person på grundlag af nationalt anerkendte procedurer. Imidlertid er det fortsat den delegerende fysiske person, der er ansvarlig.

3) Forbindelser skal oprettes på følgende måde:

Sikringsniveau	Obligatoriske elementer
Lav	1. Godtgørelse af identiteten af den fysiske person, der handler på vegne af den juridiske person, kontrolleres på sikringsniveau »lav« eller derover. 2. Forbindelsen kan oprettes på grundlag af nationalt anerkendte procedurer. 3. Den fysiske person er ikke registreret af en autoritativ kilde med en status, der afholder den fysiske person fra at handle på vegne af den juridiske person.
Betydelig	Kravene i punkt 3 i sikringsniveauet »lav« samt: 1. Godtgørelse af identiteten af den fysiske person, der handler på vegne af den juridiske person, kontrolleres på sikringsniveau »betydelig« eller »høj«.

Sikringsniveau	Obligatoriske elementer
	2. Forbindelsen er blevet etableret på grundlag af nationalt anerkendte procedurer, som resulterede i registrering af forbindelsen i en autoritativ kilde. 3. Forbindelsen er blevet kontrolleret på grundlag af oplysninger fra en autoritativ kilde.
Høj	Kravene i punkt 3 i sikringsniveau »lav«, punkt 2 i sikringsniveau »betydelig« samt: 1. Godtgørelse af identiteten af den fysiske person, der handler på vegne af den juridiske person, kontrolleres på sikringsniveau »høj«. 2. Forbindelsen er blevet kontrolleret på grundlag af et entydigt identifikationsnummer, der repræsenterer den juridiske person, og som bruges i nationale sammenhænge, og på grundlag af oplysninger, der entydigt repræsenterer den fysiske person, fra en autoritativ kilde.

2.2. *Håndtering af elektroniske identifikationsmidler*

2.2.1. Elektroniske identifikationsmidler — egenskaber og udformning

Sikringsniveau	Obligatoriske elementer
Lav	1. Det elektroniske identifikationsmiddel gør brug af mindst en autentifikationsfaktor. 2. Det elektroniske identifikationsmiddel er udformet således, at udstederen tager rimelige skridt til at kontrollere, at det kun er den person, som det tilhører, der har kontrol over og er i besiddelse af det.
Betydelig	1. Det elektroniske identifikationsmiddel gør brug af mindst to autentifikationsfaktorer fra forskellige kategorier. 2. Det elektroniske identifikationsmiddel er udformet således, at det kan antages, at det kun kan bruges, når det er den person, som det tilhører, der har kontrol over og er i besiddelse af det.
Høj	Kravene til sikringsniveau »betydelig« samt: 1. Det elektroniske identifikationsmiddel er beskyttet mod kopiering og manipulation samt angribere med stor angrebskapacitet 2. Det elektroniske identifikationsmiddel er udformet således, at den person, som det tilhører, kan beskytte det sikkert mod, at andre bruger det.

2.2.2. Udstedelse, levering og aktivering

Sikringsniveau	Obligatoriske elementer
Lav	Det elektroniske identifikationsmiddel leveres efter udstedelse via en mekanisme, som gør det muligt at antage, at det kun leveres til den tilsigtede person.
Betydelig	Det elektroniske identifikationsmiddel leveres efter udstedelse via en mekanisme, som gør det muligt at antage, at det kun udleveres til den person, som det tilhører.
Høj	Aktiveringsprocessen kontrollerer, at det elektroniske identifikationsmiddel kun blev udleveret til den person, som det tilhører.

2.2.3. Suspendering, tilbagekaldelse og reaktivering

Sikringsniveau	Obligatoriske elementer
Lav	1. Det er muligt at suspendere og/eller tilbagekalde et elektronisk identifikationsmiddel rettidigt og effektivt. 2. Der findes foranstaltninger, som skal forhindre uautoriseret suspendering, tilbagekaldelse og/eller reaktivering. 3. Reaktivering skal kun finde sted, hvis de samme sikringskrav som forud for suspenderingen eller reaktiveringen fortsat er opfyldt.
Betydelig	Samme niveau som »lav«.
Høj	Samme niveau som »lav«.

2.2.4. Fornyelse og erstatning

Sikringsniveau	Obligatoriske elementer
Lav	Under hensyntagen til risikoen for ændringer i personidentifikationsdata lever fornyelser og erstatninger op til de samme sikringskrav som ved den indledende proces for godtgørelse og kontrol af identitet, eller de foretages på grundlag af et gyldigt elektronisk identifikationsmiddel med samme sikringsniveau eller højere.
Betydelig	Samme niveau som »lav«.
Høj	Kravene til sikringsniveau »lav« samt: Hvis fornyelse eller erstatning er baseret på et gyldigt elektronisk identifikationsmiddel, skal identitetsdata kontrolleres i en autoritativ kilde.

2.3. *Autentifikation*

Dette afsnit omhandler de trusler, der er forbundet med brug af autentifikationsmekanismen, og det indeholder en liste over kravene til hvert sikringsniveau. I dette afsnit skal kontroller forstås som stående i et rimeligt forhold til risikoen på et givet sikringsniveau.

2.3.1. Autentifikationsmekanismen

Følgende tabel fastsætter kravene pr. sikringsniveau til den autentifikationsmekanisme, hvorigennem fysiske og juridiske personer anvender det elektroniske identifikationsmiddel til at bekræfte deres identitet over for en modtager.

Sikringsniveau	Obligatoriske elementer
Lav	1. Frigivelsen af personidentifikationsdata finder sted efter en pålidelig kontrol af det elektroniske identifikationsmiddel og dets gyldighed. 2. Hvis personidentifikationsdata er lagret som en del af autentifikationsmekanismen, er disse oplysninger sikret på en måde, der beskytter dem mod at gå tabt eller blive kompromitteret, herunder analyse offline. 3. Autentifikationsmekanismen implementerer sikkerhedskontroller til at efterprøve det elektroniske identifikationsmiddel, således at det er højst usandsynligt, at det er muligt for en angriber med en øget basal angrebskapacitet at gætte, lytte sig til, gengive eller manipulere kommunikationen og på den måde omgå autentifikationsmekanismen.

Sikringsniveau	Obligatoriske elementer
Betydelig	Kravene til sikringsniveau »lav« samt: 1. Frigivelsen af personidentifikationsdata finder sted efter en pålidelig kontrol af det elektroniske identifikationsmiddel og dets gyldighed via en dynamisk autentifikationsmekanisme. 2. Autentifikationsmekanismen implementerer sikkerhedskontroller til at efterprøve det elektroniske identifikationsmiddel, således at det er højst usandsynligt, at det er muligt for en angriber med en moderat angrebskapacitet at gætte, lytte sig til, gengive eller manipulere kommunikationen og på den måde omgå autentifikationsmekanismen.
Høj	Kravene til sikringsniveau »betydelig« samt: Autentifikationsmekanismen implementerer sikkerhedskontroller til at efterprøve det elektroniske identifikationsmiddel, således at det er højst usandsynligt, at det er muligt for en angriber med en høj angrebskapacitet at gætte, lytte sig til, gengive eller manipulere kommunikationen og på den måde omgå autentifikationsmekanismen.

2.4. *Håndtering og organisering*

Alle parter, der leverer tjenester, som vedrører elektronisk identifikation på tværs af grænser (»leverandører«), skal have dokumenteret praksis og dokumenterede politikker for forvaltning af informationssikkerhed, tilgange til risikohåndtering og andre anerkendte kontroller, som over for de relevante forvaltningsorganer for elektroniske identifikationsordninger i de respektive medlemsstater kan sikre, at der er indført effektiv praksis. I hele afsnit 2.4 skal alle krav/elementer forstås som stående i et rimeligt forhold til risikoen på et givet sikringsniveau.

2.4.1. Generelle bestemmelser

Sikringsniveau	Obligatoriske elementer
Lav	1. Leverandører af enhver driftstjeneste, der er omfattet af denne forordning, er en offentlig myndighed eller en juridisk enhed, som er anerkendt af den pågældende medlemsstat efter national ret. De har en etableret organisation og er fuldt operationsdygtige inden for alle de områder, der er relevante for at levere tjenesten. 2. Leverandørerne overholder alle lovkrav, der pålægges dem i forbindelse med drift og levering af tjenesten, herunder krav til hvilke typer oplysninger der kan søges, hvordan kontrol af identitet foretages samt hvilke oplysninger der opbevares og hvor længe. 3. Leverandørerne er i stand til at dokumentere deres evne til at påtage sig risikoen for at bære erstatningsansvar, og de har tilstrækkelige finansielle ressourcer til at fortsætte driften og levere tjenester. 4. Leverandørerne er ansvarlige for at opfylde alle forpligtelser, der måtte være outsourcet til en anden enhed, og for at overholde ordningens politikker som var det leverandørerne selv, der havde udført opgaverne. 5. Elektroniske identifikationsordninger, som ikke bygger på national ret, skal have en effektiv plan i tilfælde af virksomhedsafbrydelse. En sådan plan skal indeholde en korrekt nedlæggelse af tjenesten eller en fortsættelse med en anden udbyder, en metode til underretning af de relevante myndigheder og slutbrugere, samt oplysninger om, hvordan registreringer skal beskyttes, opbevares eller destrueres i overensstemmelse med ordningens politikker.
Betydelig	Samme niveau som »lav«.
Høj	Samme niveau som »lav«.

2.4.2. Offentliggjorte meddelelser og brugeroplysninger

Sikringsniveau	Obligatoriske elementer
Lav	1. Der skal forelægge en offentliggjort definition af tjenesten, som omfatter de gældende betingelser, vilkår og gebyrer, herunder eventuelle begrænsninger af brug af tjenesten. Definitionen af tjenesten skal indeholde en erklæring om behandling af personoplysninger. 2. Der skal indføres egnede politikker og procedurer for at sikre, at tjenestens brugere rettidigt og konsekvent oplyses om eventuelle ændringer i definitionen af tjenesten eller i de gældende betingelser, vilkår eller erklæringen om behandling af personoplysninger for den pågældende tjeneste. 3. Der skal indføres egnede politikker og procedurer, som sikrer fuldstændige og korrekte besvarelser af anmodninger om oplysninger.
Betydelig	Samme niveau som »lav«.
Høj	Samme niveau som »lav«.

2.4.3. Forvaltning af informationssikkerhed

Sikringsniveau	Obligatoriske elementer
Lav	Der er indført et effektivt system til forvaltning af informationssikkerhed til at forvalte og kontrollere risici for informationssikkerhed.
Betydelig	Kravene til sikringsniveau »lav« samt: Systemet til forvaltning af informationssikkerhed overholder velprøvede standarder eller principper for forvaltning og kontrol af risici for informationssikkerhed.
Høj	Samme niveau som »betydelig«.

2.4.4. Registerføring

Sikringsniveau	Obligatoriske elementer
Lav	1. Relevante oplysninger registreres og ajourføres ved hjælp af et effektivt registreringssystem, der tager hensyn til gældende lovgivning og god praksis inden for beskyttelse og opbevaring af data. 2. Oplysninger opbevares — i det omfang det er tilladt efter national lovgivning eller andre nationale administrative ordninger — og beskyttes, så længe der er behov for dem med henblik på revision, undersøgelser af brud på sikkerheden og opbevaring, hvorpå de destrueres på en sikker måde.
Betydelig	Samme niveau som »lav«.
Høj	Samme niveau som »lav«.

2.4.5. Faciliteter og personale

Følgende tabel indeholder de krav, der gælder for faciliteter og personale og eventuelt underleverandører, som påtager sig pligter, der er omfattet af denne forordning. Overholdelsen af kravene skal stå i et rimeligt forhold til den risiko, der er forbundet med det pågældende sikringsniveau.

Sikringsniveau	Obligatoriske elementer
Lav	1. Der skal findes procedurer, som sikrer, at personale og underleverandører er tilstrækkeligt uddannede, kvalificerede og erfarne inden for de færdigheder, der er behov for, når de skal udfylde deres roller. 2. Der skal være tilstrækkeligt med personale og underleverandører til at drive og vedligeholde tjenesten i henhold til de relevante politikker og procedurer. 3. Faciliteter, der bruges til at levere tjenesten, kontrolleres løbende for og beskyttes mod skader forårsaget af miljøhændelser, uautoriseret adgang og andre faktorer, som kan påvirke tjenestens sikkerhed. 4. Faciliteter, der bruges til at levere tjenesten, sikrer, at adgang til de områder, hvor personlige, kryptografiske og andre følsomme oplysninger opbevares og behandles, er begrænset til autoriseret personale og autoriserede underleverandører.
Betydelig	Samme niveau som »lav«.
Høj	Samme niveau som »lav«.

2.4.6. Tekniske kontroller

Sikringsniveau	Obligatoriske elementer
Lav	1. Der findes rimelige tekniske kontroller, som gør det muligt at afværge trusler mod tjenesternes sikkerhed og sikrer de behandlede oplysningers fortrolighed, integritet og tilgængelighed. 2. Elektroniske kommunikationskanaler, der bruges til at udveksle personlige eller følsomme oplysninger, beskyttes mod aflytning, manipulation og gengivelse. 3. Adgang til følsomt kryptografisk materiale er, hvis det bruges til at udstede elektroniske identifikationsmidler eller autentifikation, begrænset til de roller og anvendelsesområder, der absolut skal have adgang. Det skal sikres, at den slags materiale aldrig lagres permanent som klartekst. 4. Der er indført procedurer, som garanterer, at sikkerheden bevares over tid, og at der er mulighed for at reagere på ændringer i risikoniveau, sikkerhedshændelser og brud på sikkerheden. 5. Alle medier, som indeholder personlige, kryptografiske eller andre følsomme oplysninger, lagres, transporteres og bortskaffes på en sikker måde.
Betydelig	Samme niveau som »lav«, samt: Følsomt kryptografisk materiale er, hvis det anvendes til at udstede elektroniske identifikationsmidler eller autentifikation, beskyttet mod manipulation.
Høj	Samme niveau som »betydelig«.

2.4.7. Overholdelse og revision

Sikringsniveau	Obligatoriske elementer
Lav	Der gennemføres jævnlige interne revisioner, som omfatter alle de relevante dele til levering af den pågældende tjeneste, og som sikrer overholdelse af den relevante politik.

Sikringsniveau	Obligatoriske elementer
Betydelig	Der gennemføres jævnligt interne eller eksterne revisioner, som omfatter alle de relevante dele til levering af den pågældende tjeneste, og som sikrer overholdelse af den relevante politik.
Høj	1. Der gennemføres jævnligt uafhængige eksterne revisioner, som omfatter alle de relevante dele til levering af den pågældende tjeneste, og som sikrer overholdelse af den relevante politik. 2. Hvis en ordning forvaltes direkte af et statsorgan, foretages revision i henhold til national lovgivning.

KOMMISSIONENS GENNEMFØRELSESFORORDNING (EU) 2015/1503

af 8. september 2015

om faste importværdier med henblik på fastsættelse af indgangsprisen for visse frugter og grøntsager

EUROPA-KOMMISSIONEN HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde,

under henvisning til Europa-Parlamentets og Rådets forordning (EU) nr. 1308/2013 af 17. december 2013 om en fælles markedsordning for landbrugsprodukter og om ophævelse af Rådets forordning (EØF) nr. 922/72, (EØF) nr. 234/79, (EF) nr. 1037/2001 og (EF) nr. 1234/2007 ([1]),

under henvisning til Kommissionens gennemførelsesforordning (EU) nr. 543/2011 af 7. juni 2011 om nærmere bestemmelser for anvendelsen af Rådets forordning (EF) nr. 1234/2007 for så vidt angår frugt og grøntsager og forarbejdede frugter og grøntsager ([2]), særlig artikel 136, stk. 1, og

ud fra følgende betragtninger:

(1) Ved gennemførelsesforordning (EU) nr. 543/2011 fastsættes der på basis af resultatet af de multilaterale handelsforhandlinger under Uruguayrunden kriterier for Kommissionens fastsættelse af faste importværdier for tredjelande for de produkter og perioder, der er anført i del A i bilag XVI til nævnte forordning.

(2) Der beregnes hver arbejdsdag en fast importværdi i henhold til artikel 136, stk. 1, i gennemførelsesforordning (EU) nr. 543/2011 under hensyntagen til varierende daglige data. Derfor bør nærværende forordning træde i kraft på dagen for offentliggørelsen i *Den Europæiske Unions Tidende* —

VEDTAGET DENNE FORORDNING:

Artikel 1

De faste importværdier som omhandlet i artikel 136 i gennemførelsesforordning (EU) nr. 543/2011 fastsættes i bilaget til nærværende forordning.

Artikel 2

Denne forordning træder i kraft på dagen for offentliggørelsen i *Den Europæiske Unions Tidende*.

Denne forordning er bindende i alle enkeltheder og gælder umiddelbart i hver medlemsstat.

Udfærdiget i Bruxelles, den 8. september 2015.

På Kommissionens vegne

For formanden

Jerzy PLEWA

Generaldirektør for landbrug og udvikling af landdistrikter

([1]) EUT L 347 af 20.12.2013, s. 671.
([2]) EUT L 157 af 15.6.2011, s. 1.

BILAG

Faste importværdier med henblik på fastsættelse af indgangsprisen for visse frugter og grøntsager

(EUR/100 kg)

KN-kode	Tredjelandskode ([1])	Fast importværdi
0702 00 00	MA	173,3
	MK	48,7
	XS	41,5
	ZZ	87,8
0707 00 05	MK	76,3
	TR	116,3
	XS	42,0
	ZZ	78,2
0709 93 10	TR	133,1
	ZZ	133,1
0805 50 10	AR	135,9
	BO	135,7
	CL	125,5
	UY	142,2
	ZA	136,9
	ZZ	135,2
0806 10 10	EG	239,8
	MK	63,9
	TR	129,5
	ZZ	144,4
0808 10 80	AR	188,7
	BR	93,9
	CL	134,4
	NZ	143,4
	US	112,5
	UY	110,5
	ZA	117,6
	ZZ	128,7
0808 30 90	AR	131,9
	CL	100,0
	TR	122,9
	ZA	113,5
	ZZ	117,1
0809 30 10, 0809 30 90	MK	80,1
	TR	141,7
	ZZ	110,9

(EUR/100 kg)

KN-kode	Tredjelandskode (1)	Fast importværdi
0809 40 05	BA	54,8
	IL	336,8
	MK	44,1
	XS	70,3
	ZZ	126,5

(1) Landefortegnelse fastsat ved Kommissionens forordning (EU) nr. 1106/2012 af 27. november 2012 om gennemførelse af Europa-Parlamentets og Rådets forordning (EF) nr. 471/2009 om fællesskabsstatistikker over varehandelen med tredjelande for så vidt angår ajourføring af den statistiske lande- og områdefortegnelse (EUT L 328 af 28.11.2012, s. 7). Koden »ZZ« = »anden oprindelse«.

AFGØRELSER

KOMMISSIONENS GENNEMFØRELSESAFGØRELSE (EU) 2015/1504

af 7. september 2015

om indrømmelse af undtagelser for visse medlemsstater for så vidt angår indberetning af statistikker i henhold til Europa-Parlamentets og Rådets forordning (EF) nr. 1099/2008 om energistatistik

(meddelte under nummer C(2015) 6105)

(Kun den estiske, den franske, den græske, den nederlandske og den slovakiske udgave er autentiske)

(EØS-relevant tekst)

EUROPA-KOMMISSIONEN HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde,

under henvisning til Europa-Parlamentets og Rådets forordning (EF) nr. 1099/2008 af 22. oktober 2008 om energistatistik ([1]), særlig artikel 5, stk. 4, og artikel 10, stk. 2, og

ud fra følgende betragtninger:

(1) I henhold til artikel 5, stk. 4, i forordning (EF) nr. 1099/2008 kan der på begrundet anmodning fra en medlemsstat indrømmes undtagelser for indsamling af de dele af de nationale statistikker, der medfører for stor en byrde for respondenterne.

(2) Belgien, Estland, Cypern og Slovakiet har indgivet anmodninger om at opnå undtagelser for så vidt angår indberetning af statistikker vedrørende det detaljerede energiforbrug i husholdninger efter type slutanvendelse for visse referenceår.

(3) Oplysningerne fra disse medlemsstater berettiger, at der bør indrømmes undtagelser.

(4) Foranstaltningerne i denne afgørelse er i overensstemmelse med udtalelse fra Udvalget for det Europæiske Statistiske System —

VEDTAGET DENNE AFGØRELSE:

Artikel 1

Der indrømmes herved følgende undtagelser fra bestemmelserne i forordning (EF) nr. 1099/2008:

1) Belgien fritages for at udarbejde statistikker for referenceåret 2015 for så vidt angår punkt 1.2.3, nr. 4.2.1 til 4.2.5, punkt 2.2.3, nr. 4.2.1 til 4.2.5, punkt 3.2.3, nr. 3.1 til 3.6, punkt 4.2.3, nr. 7.2.1 til 7.2.5, og punkt 5.2.4, nr. 4.2.1 til 4.2.5, i bilag B om statistikker om det detaljerede energiforbrug i husholdninger efter type slutanvendelse (som defineret i punkt 2.3, nr. 26 »Andre sektorer — husholdningssektoren« i bilag A).

([1]) EUT L 304 af 14.11.2008, s. 1.

2) Estland fritages for at udarbejde statistikker for referenceåret 2015, 2016 og 2017 for så vidt angår punkt 1.2.3, nr. 4.2.1 til 4.2.5, punkt 2.2.3, nr. 4.2.1 til 4.2.5, punkt 3.2.3, nr. 3.1 til 3.6, punkt 4.2.3, nr. 7.2.1 til 7.2.5, og punkt 5.2.4, nr. 4.2.1 til 4.2.5, i bilag B om statistikker om det detaljerede energiforbrug i husholdninger efter type slutanvendelse (som defineret i punkt 2.3, nr. 26 »Andre sektorer — husholdningssektoren« i bilag A).

3) Cypern fritages for at udarbejde statistikker for referenceåret 2015, 2016 og 2017 for så vidt angår punkt 1.2.3, nr. 4.2.1 til 4.2.5, punkt 2.2.3, nr. 4.2.1 til 4.2.5, punkt 3.2.3, nr. 3.1 til 3.6, og punkt 5.2.4, nr. 4.2.1 til 4.2.5, i bilag B om statistikker om det detaljerede energiforbrug i husholdninger efter type slutanvendelse (som defineret i punkt 2.3, nr. 26 »Andre sektorer — husholdningssektoren« i bilag A).

4) Slovakiet fritages for at udarbejde statistikker for referenceåret 2015 og 2016 for så vidt angår punkt 1.2.3, nr. 4.2.1 til 4.2.5, punkt 2.2.3, nr. 4.2.1 til 4.2.5, punkt 3.2.3, nr. 3.1 til 3.6, punkt 4.2.3, nr. 7.2.1 til 7.2.5, og punkt 5.2.4, nr. 4.2.1 til 4.2.5, i bilag B om statistikker om det detaljerede energiforbrug i husholdninger efter type slutanvendelse (som defineret i punkt 2.3, nr. 26 »Andre sektorer — husholdningssektoren« i bilag A).

Artikel 2

Denne afgørelse er rettet til Kongeriget Belgien, Republikken Estland, Republikken Cypern og Den Slovakiske Republik.

Udfærdiget i Bruxelles, den 7. september 2015.

På Kommissionens vegne

Marianne THYSSEN

Medlem af Kommissionen

KOMMISSIONENS GENNEMFØRELSESAFGØRELSE (EU) 2015/1505

af 8. september 2015

om fastlæggelse af tekniske specifikationer og formater for positivlister i henhold til artikel 22, stk. 5, i Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked

(EØS-relevant tekst)

EUROPA-KOMMISSIONEN HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde,

under henvisning til Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF ([1]), særlig artikel 22, stk. 5, og

ud fra følgende betragtninger:

(1) Positivlister er afgørende for at opbygge tillid blandt markedsaktørerne, da de fastslår tjenesteudbyderens status på overvågningstidspunktet.

(2) Anvendelsen af elektroniske signaturer på tværs af landegrænser er blevet lettet via Kommissionens beslutning 2009/767/EF ([2]), som forpligter medlemsstaterne til at oprette, vedligeholde og offentliggøre positivlister med oplysninger om certificeringstjenesteudbydere, der udsteder kvalificerede certifikater til offentligheden i overensstemmelse med Europa-Parlamentets og Rådets direktiv 1999/93/EF ([3]), og som overvåges og akkrediteres af medlemsstaterne.

(3) I henhold til artikel 22 i forordning (EU) Nr. 910/2014 er medlemsstaterne forpligtede til under sikre forhold at oprette, ajourføre og offentliggøre positivlister, som er elektronisk underskrevne eller forseglede i en form, der er egnet til automatiseret behandling. Medlemsstaterne er også forpligtede til at meddele Kommissionen de organer, de er ansvarlige for at oprette de nationale positivlister.

(4) En tillidstjenesteudbyder og de tillidstjenester, som den udbyder, bør anses for at være kvalificerede, når udbyderen ifølge positivlisten er tildelt status som kvalificeret tillidstjenesteudbyder. For at sikre, at andre forpligtelser hidrørende fra forordning (EU) nr. 910/2014, især dem i artikel 27 og 37, uden besvær kan opfyldes af tjenesteudbyderne på afstand og ad elektronisk vej, og for at leve op til de berettigede forventninger fra andre certificeringstjenesteudbydere, som ikke udsteder kvalificerede certifikater, men yder tjenester vedrørende elektroniske signaturer i henhold til direktiv 1999/93/EF og opføres på listen inden den 30. juni 2016, bør det være muligt for medlemsstaterne på frivillig basis og på nationalt niveau at tilføje andre tillidstjenester end de kvalificerede tjenester på positivlisterne, forudsat at det klart fremgår, at de ikke er kvalificerede i henhold til forordning (EU) nr. 910/2014.

(5) I overensstemmelse med betragtning 25 i forordning (EU) nr. 910/2014 kan medlemsstaterne tilføje andre typer nationalt definerede tillidstjenester end dem, som er defineret i artikel 3, nr. 16, i forordning (EU) nr. 910/2014, forudsat at det klart fremgår, at de ikke er kvalificerede i henhold til forordning (EU) nr. 910/2014.

(6) Foranstaltningerne i denne afgørelse er i overensstemmelse med udtalelsen fra det udvalg, der er nedsat ved artikel 48 i forordning (EU) nr. 910/2014 —

VEDTAGET DENNE AFGØRELSE:

Artikel 1

Medlemsstaterne opstiller, offentliggør og ajourfører positivlister med oplysninger om de kvalificerede tillidstjenesteudbydere, som de overvåger, samt oplysninger om de kvalificerede tillidstjenester, som disse udbydere udbyder. Disse lister skal overholde de tekniske specifikationer i bilag I.

([1]) EUT L 257 af 28.8.2014, s. 73.
([2]) Kommissionens beslutning 2009/767/EF af 16. oktober 2009 om fastlæggelse af foranstaltninger, der skal lette anvendelsen elektroniske procedurer ved hjælp af »kvikskranker« i henhold til Europa-Parlamentets og Rådets direktiv 2006/123/EF om tjenesteydelser i det indre marked (EUT L 274 af 20.10.2009, s. 36).
([3]) Europa-Parlamentets og Rådets direktiv 1999/93/EF af 13. december 1999 om en fællesskabsramme for elektroniske signaturer (EFT L 13 af 19.1.2000, s. 12).

Artikel 2

I positivlisterne kan medlemsstaterne inkludere oplysninger om ikke kvalificerede tillidstjenesteudbydere sammen med oplysninger vedrørende de ikke kvalificerede tillidstjenester, som disse udbydere udbyder. Det skal fremgå klart af listen, hvilke tillidstjenesteudbydere og tillidstjenester ikke er kvalificerede.

Artikel 3

1. I henhold til artikel 22, stk. 2, i forordning (EU) nr. 910/2014 underskriver eller forsegler medlemsstaterne elektronisk deres positivliste i den form, der egner sig til automatiseret behandling, i overensstemmelse med de tekniske specifikationer i bilag I.

2. Hvis en medlemsstat elektronisk offentliggør en menneskeligt læsbar udgave af positivlisten, sikres det, at denne udgave af positivlisten indeholder de samme data som den udgave, der er egnet til automatiseret behandling, og den underskrives eller forsegles elektronisk i overensstemmelse med de tekniske specifikationer i bilag I.

Artikel 4

1. Medlemsstaterne meddeler Kommissionen de oplysninger, som der henvises til i artikel 22, stk. 3, i forordning (EU) nr. 910/2014, ved hjælp af skabelonen i bilag II.

2. Oplysningerne, som der henvises til i stk. 1, skal indeholde to eller flere operatører af offentlige nøglecertifikater med forskudte gyldighedsperioder på mindst tre måneder, der svarer til de private nøgler, der kan bruges til elektronisk at underskrive eller forsegle den udgave af positivlisten, der er egnet til automatiseret behandling, og den menneskeligt læsbare udgave, når de offentliggøres.

3. I henhold til artikel 22, stk. 4, i forordning (EU) nr. 910/2014 stiller Kommissionen de oplysninger, der er omhandlet i stk. 1 og 2, og som er indgivet af medlemsstaterne, til rådighed for offentligheden via en sikker kommunikationsforbindelse til en godkendt webserver og i en elektronisk underskrevet eller forseglet form, der egner sig til automatiseret behandling.

4. Kommissionen kan stille de oplysninger, der er omhandlet i stk. 1 og 2, og som er indgivet af medlemsstaterne, til rådighed for offentligheden via en sikker kommunikationsforbindelse til en godkendt webserver og i en underskrevet eller forseglet menneskeligt læsbar form.

Artikel 5

Denne afgørelse træder i kraft på tyvendedagen efter offentliggørelsen i *Den Europæiske Unions Tidende*.

Denne afgørelse er bindende i alle enkeltheder og gælder umiddelbart i hver medlemsstat.

Udfærdiget i Bruxelles, den 8. september 2015.

På Kommissionens vegne

Jean-Claude JUNCKER

Formand

BILAG I

TEKNISKE SPECIFIKATIONER FOR DEN FÆLLES SKABELON FOR POSITIVLISTEN

KAPITEL I

ALMINDELIGE SPECIFIKATIONER

Positivlisterne skal indeholde både aktuelle og alle historiske oplysninger om de angivne tillidstjenesteudbydere fra det tidspunkt, hvor den pågældende tillidstjenesteudbyder optages på positivlisten.

Betegnelserne »godkendt«, »akkrediteret« og/eller »overvåget« i de nærværende specifikationer omfatter også de nationale godkendelsesordninger, men yderligere oplysninger om arten af sådanne eventuelle nationale ordninger vil blive afgivet af medlemsstaterne i deres positivliste, herunder afklaring af eventuelle forskelle fra de overvågningsordninger, der gælder for kvalificerede tillidstjenesteudbydere og de kvalificerede tillidstjenester, som de udbyder.

Hovedformålet med oplysningerne i positivlisten er at støtte valideringen af kvalificerede trust service tokens, dvs. fysiske eller binære (logiske) genstande, der genereres eller udstedes som følge af anvendelsen af en kvalificeret tillidstjeneste, f.eks. netop kvalificerede elektroniske signaturer/segl, avancerede elektroniske signaturer/segl understøttet af et kvalificeret certifikat, kvalificerede tidsstempler, kvalificerede elektroniske leveringsbeviser, osv.

KAPITEL II

DETALJEREDE SPECIFIKATIONER FOR DEN FÆLLES SKABELON FOR POSITIVLISTEN

Nærværende specifikationer bygger på de specifikationer og krav, som er angivet i ETSI TS 119 612 v2.1.1 (herefter kaldet ETSI TS 119 612).

Hvis der ikke er angivet noget specifikt krav i nærværende specifikationer, finder kravene i punkt 5 og 6 i ETSI TS 119 612 fuld anvendelse. Når der er angivet specifikke krav i nærværende specifikationer, har de forrang over de tilsvarende krav fra ETSI TS 119 612. I tilfælde af uoverensstemmelser mellem nærværende specifikationer og specifikationerne i ETSI TS 119 612, betragtes nærværende specifikationer som de normative.

Scheme name (punkt 5.3.6)

Dette felt er påkrævet og skal være i overensstemmelse med specifikationerne fra TS 119 612 punkt 5.3.6, hvori det følgende navn skal anvendes for ordningen:

»EN_name_value« = »Positivliste med oplysninger om de kvalificerede tillidstjenesteudbydere, som overvåges af medlemsstaterne, samt oplysninger om de kvalificerede tillidstjenester, som udbyderne udbyder, i overensstemmelse med de relevante bestemmelser i Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF.«

Scheme information URI (punkt 5.3.7)

Dette felt er påkrævet og skal være i overensstemmelse med specifikationerne fra TS 119 612, punkt 5.3.7, hvori de »passende oplysninger om ordningen« mindst skal omfatte:

a) Indledende oplysninger, som er fælles for alle medlemsstaterne, vedrørende positivlistens anvendelsesområde og kontekst, den pågældende overvågningsordning og, hvor det er relevant, de national(e) godkendelsesordning(er) f.eks. til akkreditering. Den nedenstående tekst er den fælles tekst, der bruges, hvori tekststrengen »[*name of the relevant Member State*]« skal erstattes med navnet på den pågældende medlemsstat:

   »Nærværende liste er positivlisten med oplysninger om de kvalificerede tillidstjenesteudbydere, som overvåges af »[*name of the relevant Member State*]«, samt oplysninger om de kvalificerede tillidstjenester, som udbyderne udbyder, i overensstemmelse med de relevante bestemmelser i Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF.

Anvendelsen af elektroniske signaturer på tværs af landegrænser er blevet lettet via Kommissionens beslutning 2009/767/EF af 16. oktober 2009, som forpligter medlemsstaterne til at oprette, vedligeholde og offentliggøre positivlister med oplysninger om certificeringstjenesteudbydere, der udsteder kvalificerede certifikater til offentligheden i overensstemmelse med Europa-Parlamentets og Rådets direktiv 1999/93/EF af 13. december 1999 om en fællesskabsramme for elektroniske signaturer, og som overvåges/akkrediteres af medlemsstaterne. Nærværende positivliste er en videreførelse af positivlisten, som blev opstillet i forbindelse med beslutning 2009/767/EF.«

Positivlister er afgørende elementer for at opbygge tillid blandt markedsaktørerne, da brugere kan anvende dem til at fastslå tillidstjenesteudbydernes og deres tjenesters kvalificerede status og statushistorik.

Medlemsstaternes positivlister omfatter som minimum de oplysninger, som der henvises til i artikel 1 og 2 i Kommissionens gennemførelsesafgørelse (EU) 2015/1505.

I positivlisterne kan medlemsstaterne inkludere oplysninger om ikke kvalificerede tillidstjenesteudbydere sammen med oplysninger vedrørende de ikke kvalificerede tillidstjenester, som disse udbydere udbyder. Det skal klart fremgå, at disse ikke er kvalificerede i henhold til forordning (EU) nr. 910/2014.

I positivlisterne kan medlemsstaterne inkludere oplysninger om nationalt definerede tillidstjenester af andre typer end dem, som er defineret i artikel 3, nr. 16, i forordning (EU) nr. 910/2014. Det skal klart fremgå, at disse ikke er kvalificerede i henhold til forordning (EU) nr. 910/2014.

b) Specifikke oplysninger om den pågældende overvågningsordning og, hvor det er relevant, de national(e) godkendelsesordning(er) f.eks. til akkreditering, især ([1]):

1) oplysninger om den nationale overvågningsordning, der finder anvendelse på kvalificerede og ikke kvalificerede tillidstjenesteudbydere samt de kvalificerede og ikke kvalificerede tillidstjenester, som udbyderne udbyder, i henhold til forordning (EU) nr. 910/2014

2) oplysninger, hvor det er relevant, om de nationale frivillige akkrediteringsordninger, der finder anvendelse på certificeringstjenesteudbydere, som har udstedt kvalificerede certifikater i henhold til direktiv 1999/93/EF.

Disse særlige oplysninger skal for hver af de pågældende ovenfor angivne ordninger mindst omfatte:

1) en generel beskrivelse

2) oplysninger om processen i den nationale overvågningsordning og, hvor det er relevant, for godkendelse efter en national godkendelsesordning

3) oplysninger om de kriterier, som tillidstjenesteudbydere overvåges eller, hvor det er relevant, godkendes efter

4) oplysninger om de kriterier og bestemmelser, som anvendes til at udvælge tilsynsførende/revisorer og fastlægge, hvordan disse vurderer tillidstjenesteudbydere og de tillidstjenester, som udbyderne udbyder

5) andre generelle oplysninger, som vedrører ordningens drift, samt kontaktoplysninger, hvor det er relevant.

Scheme type/community/rules (clause 5.3.9)

This field shall be present and shall comply with the specifications from TS 119 612 clause 5.3.9.

It shall only include UK English URIs.

([1]) Disse sæt af oplysninger er af afgørende betydning for, at modtagerparter kan vurdere kvaliteten og sikkerhedsniveauet ved sådanne ordninger. Disse sæt af oplysninger skal angives på positivliste-niveau ved anvendelse af nærværende »Scheme information URI« (punkt 5.3.7 — oplysninger, der leveres af medlemsstaten), »Scheme type/community/rules« (punkt 5.3.9 — gennem anvendelse af en fælles tekst for alle medlemsstater) og »TSL policy/legal notice« (punkt 5.3.11 — en fælles tekst for alle medlemsstater, hvor hver medlemsstat har mulighed for at tilføje medlemsstatsspecifik tekst/medlemsstatsspecifikke henvisninger). Yderligere oplysninger om sådanne ordninger for ikke kvalificerede tillidstjenester og nationalt definerede (kvalificerede) tillidstjenester kan afgives på tjenesteniveau, i det omfang det er relevant og påkrævet (f.eks. for at skelne mellem flere kvalitets-/sikkerhedsniveauer) gennem anvendelse af »Scheme service definition URI« (punkt 5.5.6).

It shall include at least two URIs:

(1) A URI common to all Member States' Trusted Lists pointing towards a descriptive text that shall be applicable to all Trusted Lists, as follows:

URI: http://uri.etsi.org/TrstSvc/TrustedList/schemerules/EUcommon

Descriptive text:

»*Participation in a scheme*

Each Member State must create a trusted list including information related to the qualified trust service providers that are under supervision, together with information related to the qualified trust services provided by them, in accordance with the relevant provisions laid down in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

The present implementation of such trusted lists is also to be referred to in the list of links (pointers) towards each Member State's trusted list, compiled by the European Commission.

Policy/rules for the assessment of the listed services

Member States must supervise qualified trust service providers established in the territory of the designating Member State as laid down in Chapter III of Regulation (EU) No 910/2014 to ensure that those qualified trust service providers and the qualified trust services that they provide meet the requirements laid down in the Regulation.

The trusted lists of Member States include, as a minimum, information specified in Articles 1 and 2 of Commission Implementing Decision (EU) 2015/1505

The trusted lists include both current and historical information about the status of listed trust services.

Each Member State's trusted list must provide information on the national supervisory scheme and where applicable, national approval (e.g. accreditation) scheme(s) under which the trust service providers and the trust services that they provide are listed.

Interpretation of the Trusted List

The general user guidelines for applications, services or products relying on a trusted list published in accordance with Regulation (EU) No 910/2014 are as follows:

The »qualified« status of a trust service is indicated by the combination of the »Service type identifier« (»Sti«) value in a service entry and the status according to the »Service current status« field value as from the date indicated in the »Current status starting date and time«. Historical information about such a qualified status is similarly provided when applicable.

Regarding qualified trust service providers issuing qualified certificates for electronic signatures, for electronic seals and/or for website authentication:

A »CA/QC« »Service type identifier« (»Sti«) entry (possibly further qualified as being a »RootCA-QC« through the use of the appropriate »Service information extension« (»Sie«) additionalServiceInformation Extension)

— indicates that any end-entity certificate issued by or under the CA represented by the »Service digital identifier« (»Sdi«) CA's public key and CA's name (both CA data to be considered as trust anchor input), is a qualified certificate (QC) provided that it includes at least one of the following:

  — the id-etsi-qcs-QcCompliance ETSI defined statement (id-etsi-qcs 1),

  — the 0.4.0.1456.1.1 (QCP +) ETSI defined certificate policy OID,

— the 0.4.0.1456.1.2 (QCP) ETSI defined certificate policy OID,

and provided this is ensured by the Member State Supervisory Body through a valid service status (i.e. »undersupervision«, »supervisionincessation«, »accredited« or »granted«) for that entry.

— **and IF** »Sie« »Qualifications Extension« information is present, then in addition to the above default rule, those certificates that are identified through the use of »Sie« »Qualifications Extension« information, constructed as a sequence of filters further identifying a set of certificates, must be considered according to the associated qualifiers providing additional information regarding their qualified status, the »SSCD support« and/or »Legal person as subject« (e.g. certificates containing a specific OID in the Certificate Policy extension, and/or having a specific »Key usage« pattern, and/or filtered through the use of a specific value to appear in one specific certificate field or extension, etc.). These qualifiers are part of the following set of »Qualifiers« used to compensate for the lack of information in the corresponding certificate content, and that are used respectively:

  — to indicate the qualified certificate nature:

    — »QCStatement« meaning the identified certificate(s) is(are) qualified under Directive 1999/93/EC;

    — »QCForESig« meaning the identified certificate(s), when claimed or stated as qualified certificate(s), is (are) qualified certificate(s) for electronic signature under Regulation (EU) No 910/2014;

    — »QCForESeal« meaning the identified certificate(s), when claimed or stated as qualified certificate(s), is (are) qualified certificate(s) for electronic seal under Regulation (EU) No 910/2014;

    — »QCForWSA« meaning the identified certificate(s), when claimed or stated as qualified certificate(s), is (are) qualified certificate(s) for web site authentication under Regulation (EU) No 910/2014.

  — to indicate that the certificate is not to be considered as qualified:

    — »NotQualified« meaning the identified certificate(s) is(are) not to be considered as qualified; And/or

  — to indicate the nature of the SSCD support:

    — »QCWithSSCD« meaning the identified certificate(s), when claimed or stated as qualified certificate(s), have their private key residing in an SSCD, or

    — »QCNoSSCD« meaning the identified certificate(s), when claimed or stated as qualified certificate(s), have not their private key residing in an SSCD, or

    — »QCSSCDStatusAsInCert« meaning the identified certificate(s), when claimed or stated as qualified certificate(s), does(do) contain proper machine processable information about whether or not their private key residing in an SSCD;

  — to indicate the nature of the QSCD support:

    — »QCWithQSCD« meaning the identified certificate(s), when claimed or stated as qualified certificate(s), have their private key residing in a QSCD, or

    — »QCNoQSCD« meaning the identified certificate(s), when claimed or stated as qualified certificate(s), have not their private key residing in a QSCD, or

    — »QCQSCDStatusAsInCert« meaning the identified certificate(s), when claimed or stated as qualified certificate(s), does(do) contain proper machine processable information about whether or not their private key is residing in a QSCD;

    — »QCQSCDManagedOnBehalf« indicating that all certificates identified by the applicable list of criteria, when they are claimed or stated as qualified, have their private key is residing in a QSCD for which the generation and management of that private key is done by a qualified TSP on behalf of the entity whose identity is certified in the certificate; And/or

— to indicate issuance to Legal Person:

— »QCForLegalPerson« meaning the identified certificate(s), when claimed or stated as qualified certificate(s), are issued to a Legal Person under Directive 1999/93/EC.

Note: The information provided in the trusted list is to be considered as accurate meaning that:

— if none of the id-etsi-qcs 1 statement, QCP OID or QCP + OID information is included in an end-entity certificate, and

— if no »Sie« »Qualifications Extension« information is present for the trust anchor CA/QC corresponding service entry to qualify the certificate with a »QCStatement« qualifier, or

— an »Sie« »Qualifications Extension« information is present for the trust anchor CA/QC corresponding service entry to qualify the certificate with a »NotQualified« qualifier,

then the certificate is not to be considered as qualified.

»Service digital identifiers« are to be used as Trust Anchors in the context of validating electronic signatures or seals for which signer's or seal creator's certificate is to be validated against TL information, hence only the public key and the associated subject name are needed as Trust Anchor information. When more than one certificate are representing the public key identifying the service, they are to be considered as Trust Anchor certificates conveying identical information with regard to the information strictly required as Trust Anchor information.

The general rule for interpretation of any other »Sti« type entry is that, for that »Sti« identified service type, the listed service named according to the »Service name« field value and uniquely identified by the »Service digital identity« field value has the current qualified or approval status according to the »Service current status« field value as from the date indicated in the »Current status starting date and time«.

Specific interpretation rules for any additional information with regard to a listed service (e.g. »Service information extensions« field) may be found, when applicable, in the Member State specific URI as part of the present »Scheme type/community/rules« field.

Please refer to the applicable secondary legislation pursuant to Regulation (EU) No 910/2014 for further details on the fields, description and meaning for the Member States' trusted lists.«

(2) A URI specific to each Member State's trusted list pointing towards a descriptive text that shall be applicable to this Member State trusted list:

http://uri.etsi.org/TrstSvc/TrustedList/schemerules/CC where CC = the ISO 3166-1 ([1]) alpha-2 Country Code used in the »Scheme territory« field (clause 5.3.10)

— Where users can obtain the referenced Member State's specific policy/rules against which trust services included in the list are assessed, in compliance with the Member State's supervisory regime and where applicable, approval scheme.

— Where users can obtain a referenced Member State's specific description about how to use and interpret the content of the trusted list with regard to the listed non-qualified trust services and/or to nationally defined trust services. This may be used to indicate a potential granularity in the national approval system related to CSPs not issuing QCs and how the »Scheme service definition URI« (clause 5.5.6) and the »Service information extension« field (clause 5.5.9) are used for this purpose.

Member States MAY define and use additional URIs expanding the above Member State specific URI (i.e. URIs defined from this hierarchical specific URI).

TSL policy/legal notice (punkt 5.3.11)

Dette felt er påkrævet og skal være i overensstemmelse med specifikationerne fra TS 119 612, punkt 5.3.11, hvor den politiske/juridiske erklæring om ordningens retslige status eller retslige krav, som ordningen overholder i henhold til den jurisdiktion, hvor den er oprettet, og/eller enhver hindring og betingelse for vedligeholdelsen og offentliggørelsen af

([1]) ISO 3166-1:2006: »Codes for the representation of names of countries and their subdivisions Part 1: Country codes«.

positivlisten, skal være en række multisprogede tekststrenge (se punkt 5.1.4), som på følgende måde formidler en sådan erklærings faktiske tekst på britisk engelsk som obligatorisk sprog og eventuelt på et eller flere andre nationale sprog på valgfri basis:

(1) En første obligatorisk del, som er fælles for alle medlemsstaters positivlister, hvori de relevante retlige rammer angives, og hvis engelske version lyder:

> The applicable legal framework for the present trusted list is Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

Teksten på medlemsstatens nationalsprog:

> De relevante retlige rammer for nærværende positivliste er Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF.

(2) En anden, valgfri del, som er specifik for hver positivliste, med henvisninger til specifikke gældende nationale retlige rammer

Service current status (punkt 5.5.4)

Dette felt er påkrævet og skal være i overensstemmelse med specifikationerne fra TS 119 612, punkt 5.5.4.

Overførslen af »Service current status«-værdien for de tjenester, der optræder på medlemsstaternes positivlister på dagen før datoen, hvorfra forordning (EU) nr. 910/2014 finder anvendelse, dvs. 30. juni 2016, skal udføres på datoen, hvorfra forordningen finder anvendelse, dvs. 1. juli 2016, som anført i bilag J til ETSI TS 119 612.

KAPITEL III

POSITIVLISTERS KONTINUITET

Certifikater, der skal meddeles til Kommissionen i overensstemmelse med artikel 4, stk. 2, i denne afgørelse, skal leve op til kravene i punkt 5.7.1 fra ETSI TS 119 612 og skal udstedes sådan, at:

— der er mindst tre måneder mellem deres sidste gyldighedsdatoer (»ikke efter«)

— de er genereret på nye nøglepar. Ingen tidligere anvendte nøglepar må gencertificeres.

Hvis et af de offentlige nøglecertifikater, der kan anvendes til at validere positivlistens signatur eller segl, og som er blevet meddelt til Kommissionen og offentliggjort i Kommissionens centrale pointerliste, er udløbet, skal medlemsstaterne:

— hvis den aktuelt offentliggjorte positivliste var underskrevet eller forseglet med en privat nøgle, hvis offentlige nøglecertifikat er udløbet, straks udstede en ny positivliste, som er underskrevet eller forseglet med en privat nøgle, hvis meddelte offentlige nøglecertifikat ikke er udløbet

— når det er påkrævet, generere nye nøglepar, der kan bruges til at underskrive eller forsegle positivlisten, og generere deres tilsvarende offentlige nøglecertifikater

— straks underrette Kommissionen om den nye liste over offentlige nøglecertifikater, der svarer til de private nøgler, der kan bruges til at underskrive eller forsegle positivlisten.

Hvis en af de private nøgler, der svarer til et af de offentlige nøglecertifikater, der kan bruges til at validere positivlistens signatur eller segl, og som er blevet meddelt til Kommissionen og offentliggjort i Kommissionens centrale pointerliste, er blevet kompromitteret eller afviklet, skal medlemsstaterne:

— straks genudstede en ny positivliste, som er underskrevet eller forseglet med en ikke-kompromitteret privat nøgle, i tilfælde hvor den offentliggjorte positivliste var underskrevet eller forseglet med en kompromitteret eller afviklet privat nøgle

— når det er påkrævet, generere nye nøglepar, der kan bruges til at underskrive eller forsegle positivlisten, og generere deres tilsvarende offentlige nøglecertifikater

— straks underrette Kommissionen om den nye liste over offentlige nøglecertifikater, der svarer til de private nøgler, der kan bruges til at underskrive eller forsegle positivlisten.

Hvis alle de private nøgler, der svarer til de offentlige nøglecertifikater, der kan bruges til at validere positivlistens signatur, og som er blevet meddelt til Kommissionen og offentliggjort i Kommissionens centrale pointerliste, er blevet kompromitteret eller afviklet, skal medlemsstaterne:

— generere nye nøglepar, der kan bruges til at underskrive eller forsegle positivlisten, og generere deres tilsvarende offentlige nøglecertifikater

— straks genudstede en ny positivliste, der er underskrevet eller forseglet med en af disse nye private nøgler, og hvis tilsvarende offentlige nøglecertifikat skal meddeles

— straks underrette Kommissionen om den nye liste over offentlige nøglecertifikater, der svarer til de private nøgler, der kan bruges til at underskrive eller forsegle positivlisten.

KAPITEL IV

SPECIFIKATIONER FOR DEN MENNESKELIGT LÆSBARE UDGAVE AF POSITIVLISTEN

Når en menneskeligt læsbar form af positivlisten er genereret og offentliggjort, skal den foreligge som et PDF-dokument (Portable Document Format) i overensstemmelse med ISO 32000 ([1]), som skal have et format i overensstemmelse med profil PDF/A (ISO 19005 ([2])).

Indholdet i de PDF/A-baserede menneskeligt læsbare udgaver af positivlisten skal opfylde følgende krav:

— Opbygningen af den menneskeligt læsbare udgave skal afspejle den logiske model, der er beskrevet i TS 119 612

— Hvert forekommende felt skal vises og angive:

  — Feltets titel (f.eks. »*Service type identifier*«)

  — Feltets værdi (f.eks. http://uri.etsi.org/TrstSvc/Svctype/CA/QC)

  — Betydningen (beskrivelse) af feltets værdi, såfremt dette er relevant (f.eks. »En certifikatgenereringstjeneste, der genererer og underskriver kvalificerede certifikater på basis af identiteten og andre egenskaber, som er bekræftet af de relevante registreringstjenester.«)

  — Flere versioner i naturligt sprog som angivet i positivlisten, såfremt dette er relevant.

— Følgende felter med tilhørende værdier i de digitale certifikater ([3]) skal, hvis de forefindes i feltet »Service digital identity«, som minimum vises i den menneskeligt læsbare udgave:

  — Version

  — Certifikatets serienummer

  — Signaturalgoritme

  — Udsteder — alle relevante særskilte navnefelter

  — Gyldighedsperiode

  — Bruger — alle relevante særskilte navnefelter

([1]) ISO 32000-1:2008: Dokumentstyring — Portable document format — Del 1: PDF 1.7
([2]) ISO 19005-2:2011: Dokumentstyring — Filformat for elektroniske dokumenter til langtidsopbevaring — Del 2: Brug af ISO 32000-1 (PDF/A-2)
([3]) Recommendation ITU-T X.509 | ISO/IEC 9594-8: Information technology — Open systems interconnection — The Directory: Public-key and attribute certificate frameworks (se http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=X.509).

— Offentlig nøgle

— Identifikator for myndighedsnøgle

— Identifikator for brugernøgle

— Nøglebrug

— Forlænget nøglebrug

— Certifikatpolitikker — alle politikidentifikatorer og politikkvalifikatorer

— Kortlægning af politikker

— Alternativt brugernavn

— Brugerens katalogegenskaber

— Grundlæggende begrænsninger

— Politikbegrænsninger

— CRL-distributionspunkter ([1])

— Myndighedens adgang til oplysninger

— Brugerens adgang til oplysninger

— Bemærkninger til det kvalificerede certifikat ([2])

— Hash-algoritme

— Certifikatets hash-værdi

— Den menneskeligt læsbare udgave skal let kunne udskrives

— Den menneskeligt læsbare udgave skal underskrives eller forsegles af ordningens operatør i henhold til avanceret PDF-signatur som beskrevet i artikel 1 og 3 i Kommissionens gennemførelsesafgørelse (EU) 2015/1505.

([1]) RFC 5280: Internet X.509 PKI Certificate and CRL Profile
([2]) RFC 3739: Internet X.509 PKI: Qualified Certificate Profile.

BILAG II

SKABELON FOR MEDLEMSSTATERNES MEDDELELSER

Oplysningerne, som medlemsstaterne skal meddele i henhold til artikel 4, stk. 1, i nærværende afgørelse, skal indeholde de følgende oplysninger og eventuelle ændringer heraf:

1) Medlemsstat, hvor ISO 3166-1 ([1]) Alpha 2-koderne anvendes med følgende undtagelser:

   a) Landekoden for Det Forenede Kongerige er »UK«.

   b) Landekoden for Grækenland er »EL«.

2) Organet/organerne med ansvar for oprettelsen, vedligeholdelsen og offentliggørelsen af positivlisterne i en form, der er egnet til automatiseret behandling, og i en menneskeligt læsbar udgave:

   a) Navnet på ordningens operatør: de angivne oplysninger skal være identiske — også med hensyn til forskel på store og små bogstaver — med værdien »Navnet på ordningens operatør« i positivlisten og på lige så mange sprog, som der anvendes i positivlisten

   b) Valgfrie oplysninger til intern brug i Kommissionen, kun i tilfælde hvor der er behov for kontakt til det relevante organ (oplysningerne offentliggøres ikke i den af Europa-Kommissionen sammensatte liste over positivlister):

      — Adressen på ordningens operatør

      — Kontaktoplysninger for den eller de ansvarlige person(er) (navn, telefonnummer, e-mailadresse).

3) Stedet, hvor positivlisten offentliggøres i en form, der er egnet til automatiseret behandling *(stedet, hvor den aktuelle positivliste er offentliggjort)*.

4) Stedet, om muligt, hvor positivlisten offentliggøres i en menneskeligt læsbar form *(stedet, hvor den aktuelle positivliste er offentliggjort)*. Hvis en menneskeligt læsbar udgave af positivlisten ikke længere offentliggøres, angives dette.

5) De offentlige nøglecertifikater, der svarer til de private nøgler, som kan anvendes til at underskrive eller forsegle positivlisten i den form, der egner sig til automatiseret behandling, og den menneskeligt læsbare udgave af positivlisten. Disse certifikater skal indsendes som DER-certifikater indkodet med Privacy Enhanced Mail Base64. Hvad angår meddelelser om ændring, tilføjes yderligere oplysninger, hvis et nyt certifikat skal erstatte et specifikt certifikat i Kommissionens liste, og hvis det meddelte certifikat skal føjes til det eksisterende certifikat i stedet for at erstatte det.

6) Dato for indgivelse af oplysninger, der meddeles i henhold til punkt 1) til 5).

Oplysninger, der meddeles i henhold til punkt 1), punkt 2), litra a), punkt 3), punkt 4) og punkt 5) indarbejdes i den af Europa-Kommissionen sammensatte liste over positivlister og erstatter de tidligere meddelte oplysninger i denne sammensatte liste.

([1]) ISO 3166-1: »Koder for navne på lande og deres underinddelinger — Del 1: Landekoder«.

KOMMISSIONENS GENNEMFØRELSESAFGØRELSE (EU) 2015/1506

af 8. september 2015

om fastlæggelse af specifikationer vedrørende formater for avancerede elektroniske signaturer og avancerede segl, som skal anerkendes af offentlige myndigheder i henhold til artikel 27, stk. 5, og artikel 37, stk. 5, i Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked

(EØS-relevant tekst)

EUROPA-KOMMISSIONEN HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde,

under henvisning til Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF ([1]), særlig artikel 27, stk. 5, og artikel 37, stk. 5, og

ud fra følgende betragtninger:

(1) Medlemsstaterne skal indføre de fornødne tekniske foranstaltninger, således at de kan behandle de elektronisk underskrevne dokumenter, der kræves, når der bruges en onlinetjeneste, som udbydes af eller på vegne af en offentlig myndighed.

(2) Forordning (EU) nr. 910/2014 pålægger medlemsstater, der kræver en avanceret elektronisk signatur eller et avanceret elektronisk segl for at bruge en onlinetjeneste, som udbydes af eller på vegne af en offentlig myndighed, at anerkende avancerede elektroniske signaturer og segl, avancerede elektroniske signaturer og segl, som er baseret på et kvalificeret certifikat, samt kvalificerede elektroniske signaturer og segl i specifikke formater eller alternative formater, som er godkendt i henhold til specifikke referencemetoder.

(3) Ved fastlæggelse af de specifikke formater og referencemetoder bør der tages hensyn til eksisterende praksis, standarder og EU's retsakter.

(4) I Kommissionens gennemførelsesafgørelse 2014/148/EU ([2]) er der fastlagt en række af de mest almindelige formater for avancerede elektroniske signaturer, som skal understøttes teknisk af medlemsstaterne, når der kræves avancerede elektroniske signaturer i forbindelse med en online administrativ procedure. Formålet med at fastsætte referenceformaterne er at gøre det lettere at validere elektroniske signaturer på tværs af landegrænser og at forbedre interoperabiliteten mellem elektroniske procedurer på tværs af landegrænser.

(5) Standarderne i bilaget til nærværende afgørelse er de eksisterende standarder for formater for avancerede elektroniske signaturer. På grund af standardiseringsorganernes igangværende revision af de langsigtede arkiveringsmetoder for referenceformaterne udelukkes standarder for langtidsarkivering uden fra denne afgørelses anvendelsesområde. Når den nye version af referencestandarderne foreligger, vil henvisninger til standarderne og klausulerne om langtidsarkivering blive revideret.

(6) Avancerede elektroniske signaturer og avancerede elektroniske segl er ud fra et teknisk synspunkt det samme. Derfor bør standarderne for formater for avancerede elektroniske signaturer finde tilsvarende anvendelse på formater for avancerede elektroniske segl.

(7) Når der anvendes andre elektroniske signatur- eller seglformater end dem, som er almindeligt teknisk understøttet, til underskrift eller forsegling, bør der stilles en valideringsmekanisme til rådighed, med hvilken underskrifter eller segl kan kontrolleres på tværs af landegrænser. For at modtagende medlemsstater kan have tillid til disse valideringsværktøjer fra en anden medlemsstat er det nødvendigt at gøre information om disse værktøjer let tilgængelig og lade den indgå i de elektroniske dokumenter, i de elektroniske signaturer eller i containerne med de elektroniske dokumenter.

([1]) EUT L 257 af 28.8.2014, s. 73.

([2]) Kommissionens gennemførelsesafgørelse 2014/148/EU af 17. marts 2014 om ændring af afgørelse 2011/130/EU om fastsættelse af mindstekrav ved behandling af elektronisk underskrevne dokumenter på tværs af grænserne foretaget af de kompetente myndigheder som omhandlet i Europa-Parlamentets og Rådets direktiv 2006/123/EF om tjenesteydelser i det indre marked (EUT L 80 af 19.3.2014, s. 7).

(8) Når der i en medlemsstats offentlige tjenester er muligheder for validering af elektroniske signaturer eller segl, som egner sig til automatiseret behandling, bør disse valideringsmuligheder gøres tilgængelige og stilles til rådighed for den modtagende medlemsstat. Denne afgørelse bør dog ikke hindre anvendelsen af artikel 27, stk. 1 og 2, og artikel 37, stk. 1 og 2, i forordning (EU) nr. 910/2014, når den automatiserede behandling af valideringsmuligheder ikke er mulig for alternative metoder.

(9) For at der kan være sammenlignelige krav til validering og for at øge tilliden til de valideringsmuligheder, som tilbydes af medlemsstaterne for andre formater for elektroniske signaturer og segl end de almindeligvis understøttede, er de krav, der stilles til valideringsværktøjerne i denne afgørelse, baseret på de krav til validering af kvalificerede elektroniske signaturer og segl, som der henvises til i artikel 32 og 40 i forordning (EU) nr. 910/2014.

(10) Foranstaltningerne i denne afgørelse er i overensstemmelse med udtalelse fra det udvalg, der er nedsat ved artikel 48 i forordning (EU) nr. 910/2014 —

VEDTAGET DENNE AFGØRELSE:

Artikel 1

Medlemsstater, der kræver en avanceret elektronisk signatur eller en avanceret elektronisk signatur, som er baseret på et kvalificeret certifikat, jf. artikel 27, stk. 1 og 2, i forordning (EU) nr. 910/2014, anerkender avancerede elektroniske XML-, CMS- eller PDF-signaturer på overensstemmelsesniveau B, T eller LT eller ved anvendelse af en container med tilhørende signatur, når disse signaturer er i overensstemmelse med de tekniske specifikationer i bilaget.

Artikel 2

1. Medlemsstater, der kræver en avanceret elektronisk signatur eller en avanceret elektronisk signatur, som er baseret på et kvalificeret certifikat, jf. artikel 27, stk. 1 og 2, i forordning (EU) nr. 910/2014, anerkender andre formater for elektroniske signaturer end dem, som der henvises til i denne afgørelses artikel 1, forudsat at den medlemsstat, hvor den tillidstjenesteudbyder, som underskriveren anvender, er hjemmehørende, tilbyder andre medlemsstater muligheder for signaturvalidering, som, hvor det er muligt, egner sig til automatiseret behandling.

2. Mulighederne for signaturvalidering skal:

a) tillade andre medlemsstater at validere de modtagne elektroniske signaturer online, gratis og på en måde, som kan forstås af ikke indfødte sprogbrugere

b) fremtræde i det underskrevne dokument, i den elektroniske signatur eller i containeren med det elektroniske dokument og

c) bekræfte en avanceret elektronisk signaturs gyldighed, såfremt:

   1) certifikatet, der støtter den avancerede elektroniske signatur, var gyldigt på underskriftstidspunktet, og i tilfælde hvor den avancerede elektroniske signatur støttes af et kvalificeret certifikat, det kvalificerede certifikat, der støtter den avancerede elektroniske signatur, på underskriftstidspunktet var et kvalificeret certifikat for elektronisk signatur i overensstemmelse med bilag I i forordning (EU) nr. 910/2014, og at det var udstedt af en kvalificeret tillidstjenesteudbyder

   2) signaturvalideringsdataene stemmer overens med de data, der leveres til modtagerparten

   3) det entydige sæt data, der repræsenterer underskriveren, leveres korrekt til modtagerparten

   4) en eventuel anvendelse af et pseudonym fremgår klart for modtagerparten, hvis der på underskriftstidspunktet blev anvendt et pseudonym

5) hvis den avancerede elektroniske signatur genereres af et kvalificeret elektronisk signaturgenereringssystem, fremgår brugen af et sådant system klart for modtagerparten

6) de underskrevne datas integritet ikke er bragt i fare

7) kravene i artikel 26 i forordning (EU) nr. 910/2014 var opfyldt på underskriftstidspunktet

8) det system, der anvendes til validering af den avancerede elektroniske signatur, leverer det korrekte resultat af valideringsprocessen til modtagerparten og gør det muligt for vedkommende at opdage eventuelle sikkerhedsproblemer.

Artikel 3

Medlemsstater, der kræver et avanceret elektronisk segl eller et avanceret elektronisk segl, som er baseret på et kvalificeret certifikat, jf. artikel 37, stk. 1 og 2, i forordning (EU) nr. 910/2014, anerkender avancerede elektroniske XML-, CMS- eller PDF-segl på overensstemmelsesniveau B, T eller LT eller ved anvendelse af en container med tilhørende segl, når disse er i overensstemmelse med de tekniske specifikationer i bilaget.

Artikel 4

1. Medlemsstater, der kræver et avanceret elektronisk segl eller et avanceret elektronisk segl, som er baseret på et kvalificeret certifikat, jf. artikel 37, stk. 1 og 2, i forordning (EU) nr. 910/2014, anerkender andre formater for elektroniske segl end dem, som der henvises til i denne afgørelses artikel 3, forudsat at den medlemsstat, hvor den tillidstjenesteudbyder, som underskriveren anvender, er hjemmehørende, tilbyder andre medlemsstater muligheder for seglvalidering, som, hvor det er muligt, egner sig til automatiseret behandling.

2. Mulighederne for seglvalidering skal:

a) tillade andre medlemsstater at validere de modtagne elektroniske segl online, gratis og på en måde, som kan forstås af ikke indfødte sprogbrugere

b) fremtræde i det forseglede dokument, i det elektroniske segl eller i containeren med det elektroniske dokument

c) bekræfte et avanceret elektronisk segls gyldighed, såfremt:

1) certifikatet, der støtter det avancerede elektroniske segl, var gyldigt på underskriftstidspunktet, og i tilfælde hvor det avancerede elektroniske segl støttes af et kvalificeret certifikat, det kvalificerede certifikat, der støtter det avancerede elektroniske segl, på forseglingstidspunktet var et kvalificeret certifikat for elektroniske segl i overensstemmelse med bilag III i forordning (EU) nr. 910/2014, og at det var udstedt af en kvalificeret tillidstjenesteudbyder

2) seglvalideringsdataene stemmer overens med de data, der leveres til modtagerparten

3) det entydige sæt data, der repræsenterer den forseglende part, leveres korrekt til modtagerparten

4) en eventuel anvendelse af et pseudonym fremgår klart for modtagerparten, såfremt der på forseglingstidspunktet blev anvendt et pseudonym

5) brugen af et kvalificeret elektronisk seglgenereringssystem fremgår klart for modtagerparten, i tilfælde hvor det avancerede elektroniske segl genereres af et sådant system

6) de forseglede datas integritet ikke er bragt i fare

7) kravene i artikel 36 i forordning (EU) nr. 910/2014 var opfyldt på forseglingstidspunktet

8) det system, der anvendes til validering af det avancerede elektroniske segl, leverer det korrekte resultat af valideringsprocessen til modtagerparten og gør det muligt for vedkommende at opdage eventuelle sikkerhedsproblemer.

Artikel 5

Denne afgørelse træder i kraft på tyvendedagen efter offentliggørelsen i *Den Europæiske Unions Tidende*.

Denne afgørelse er bindende i alle enkeltheder og gælder umiddelbart i hver medlemsstat.

Udfærdiget i Bruxelles, den 8. september 2015.

På Kommissionens vegne
Jean-Claude JUNCKER
Formand

BILAG

Liste over tekniske specifikationer for avancerede elektroniske XML-, CMS- eller PDF-signaturer og containeren med tilhørende signatur

Avancerede elektroniske signaturer nævnt i artikel 1, stk. 1, i afgørelsen, skal være i overensstemmelse med en af følgende tekniske specifikationer fra ETSI med undtagelse af punkt 9 heri:

XAdES Baseline Profile	ETSI TS 103171 v.2.1.1 ([1])
CAdES Baseline Profile	ETSI TS 103173 v.2.2.1 ([2])
PAdES Baseline Profile	ETSI TS 103172 v.2.2.2 ([3])

([1]) http://www.etsi.org/deliver/etsi_ts/103100_103199/103171/02.01.01_60/ts_103171v020101p.pdf
([2]) http://www.etsi.org/deliver/etsi_ts/103100_103199/103173/02.02.01_60/ts_103173v020201p.pdf
([3]) http://www.etsi.org/deliver/etsi_ts/103100_103199/103172/02.02.02_60/ts_103172v020202p.pdf

Containeren med tilhørende signatur nævnt i artikel 1, i afgørelsen, skal være i overensstemmelse med følgende tekniske specifikationer fra ETSI:

Associated Signature Container Baseline Profile	ETSI TS 103174 v.2.2.1 ([1])

([1]) http://www.etsi.org/deliver/etsi_ts/103100_103199/103174/02.02.01_60/ts_103174v020201p.pdf

Liste over tekniske specifikationer for avancerede elektroniske XML-, CMS- eller PDF-segl og containeren med tilhørende segl

Avancerede elektroniske segl nævnt i artikel 3, i afgørelsen, skal være i overensstemmelse med en af følgende tekniske specifikationer fra ETSI med undtagelse af punkt 9 heri:

XAdES Baseline Profile	ETSI TS 103171 v.2.1.1
CAdES Baseline Profile	ETSI TS 103173 v.2.2.1
PAdES Baseline Profile	ETSI TS 103172 v.2.2.2

Containeren med tilhørende segl nævnt i artikel 3, i afgørelsen, skal være i overensstemmelse med følgende tekniske specifikationer fra ETSI:

Associated Seal Container Baseline Profile	ETSI TS 103174 v.2.2.1

ISSN 1977-0634 (elektronisk udgave)
ISSN 1725-2520 (papirudgave)

Den Europæiske Unions Publikationskontor
2985 Luxembourg
LUXEMBOURG

DA