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.