COMMISSION IMPLEMENTING REGULATION (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market

**KOMMISJONENS GJENNOMFØRINGSFORORDNING (EU) 2015/1502**

**av 8. september 2015**

**om fastsettelse av tekniske minstespesifikasjoner og minstekrav til framgangsmåter for sikkerhetsnivåene for elektroniske identifikasjonsmidler i henhold til artikkel 8 nr. 3 i europaparlaments- og rådsforordning (EU) nr. 910/2014 om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked**

EUROPAKOMMISJONEN HAR —

under henvisning til traktaten om Den europeiske unions virkemåte,

under henvisning til europaparlaments- og rådsforordning (EU) nr. 910/2014 av 23. juli 2014 om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked og om oppheving av direktiv 1999/93/EF([1]), og særlig artikkel 8 nr. 3, og

ut fra følgende betraktninger:

1) I henhold til artikkel 8 i forordning (EU) nr. 910/2014 skal en ordning for elektronisk identifikasjon som er meldt i henhold til artikkel 9 nr. 1, spesifisere sikkerhetsnivåene «lavt», «betydelig» og «høyt» for elektroniske identifikasjonsmidler utstedt innenfor rammen av denne ordningen.

2) Det er svært viktig å fastsette tekniske minstespesifikasjoner, minstestandarder og minstekrav til framgangsmåter for å sikre en felles forståelse av detaljene i sikkerhetsnivåene og sikre samvirkingsevne ved kartlegging av nasjonale sikkerhetsnivåer for meldte ordninger for elektronisk identifikasjon sett i forhold til sikkerhetsnivåene i henhold til artikkel 8, som fastsatt i artikkel 12 nr. 4 bokstav b) i forordning (EU) nr. 910/2014.

3) For spesifikasjonene og framgangsmåtene i denne gjennomføringsrettsakten er det tatt hensyn til den internasjonale standarden ISO/IEC 29115, som er den viktigste internasjonale standarden for sikkerhetsnivåer for elektronisk identifikasjon. Imidlertid avviker innholdet i forordning (EU) nr. 910/2014 fra den internasjonale standarden, særlig hva angår krav til bekreftelse og kontroll av identitet, samt hvordan det tas hensyn til forskjellene mellom medlemsstatenes identitetsbestemmelser og eksisterende verktøy i EU for det samme formålet. Derfor bør vedlegget, selv om det bygger på denne internasjonale standarden, ikke vise til noe spesifikt innhold i ISO/IEC 29115.

4) Denne forordning er utarbeidet med en resultatorientert tilnærming, som anses som mest hensiktsmessig, noe som også kommer til uttrykk i definisjonene av termer og begreper. De tar hensyn til formålet med forordning (EU) nr. 910/2014 hva angår sikkerhetsnivåer for elektroniske identifikasjonsmidler. Ved fastsettelse av spesifikasjoner og framgangsmåter i denne gjennomføringsrettsakten bør det derfor tas størst mulig hensyn til det omfattende forsøksprosjektet STORK, herunder spesifikasjoner utarbeidet i den forbindelse, og definisjoner og begreper i ISO/IEC 29115.

5) Autoritative kilder kan ta mange former, og kan for eksempel være registre, dokumenter eller organer, avhengig av i hvilken sammenheng et bestemt aspekt ved identiteten skal kontrolleres. Autoritative kilder kan være ulike i de forskjellige medlemsstatene, selv i sammenhenger som ligner hverandre.

6) Kravene til bekreftelse og kontroll av identitet bør ta høyde for ulike systemer og ulik praksis, samtidig som de gir tilstrekkelig sikkerhet til å skape nødvendig tillit. Derfor bør godkjenning av framgangsmåter som tidligere har vært brukt til et annet formål enn å utstede elektroniske identifikasjonsmidler, forutsette at det bekreftes at disse framgangsmåtene oppfyller kravene for det tilsvarende sikkerhetsnivået.

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

7) Det benyttes vanligvis bestemte autentiseringsfaktorer, for eksempel delte hemmeligheter, fysiske innretninger og fysiske attributter. Det bør imidlertid oppfordres til bruk av flere autentiseringsfaktorer, framfor alt fra forskjellige kategorier av faktorer, for å bedre sikkerheten i autentiseringsprosessen.

8) Denne forordning bør ikke påvirke juridiske personers rett til å la seg representere. Vedlegget bør imidlertid inneholde krav til knytning mellom elektroniske identifikasjonsmidler for fysiske og juridiske personer.

9) Det er viktig å innse betydningen av styringssystemer for informasjonssikkerhet og tjenester, og betydningen av å benytte anerkjente metoder og følge de prinsipper som er nedfelt i standarder som ISO/IEC 27000 og ISO/IEC 20000-serien.

10) Det bør også tas hensyn til god praksis i forbindelse med medlemsstatenes sikkerhetsnivåer.

11) IT-sikkerhetssertifisering basert på internasjonale standarder er et viktig verktøy til å kontrollere at produktene er i samsvar med sikkerhetskravene i denne gjennomføringsrettsakten.

12) Komiteen nevnt i artikkel 48 i forordning (EU) nr. 910/2014 har ikke avgitt en uttalelse innen fristen som ble fastsatt av komitélederen —

VEDTATT DENNE FORORDNING:

*Artikkel 1*

1. Sikkerhetsnivåene «lavt», «betydelig» og «høyt» for elektroniske identifikasjonsmidler utstedt innenfor rammen av en meldt ordning for elektronisk identifikasjon, skal fastlegges med henvisning til spesifikasjonene og framgangsmåtene i vedlegget.

2. Spesifikasjonene og framgangsmåtene i vedlegget skal benyttes til å spesifisere sikkerhetsnivået for elektroniske identifikasjonsmidler utstedt innenfor rammen av en meldt ordning for elektronisk identifikasjon, ved å fastslå følgende elementers pålitelighet og kvalitet:

a) registrering, som fastsatt i nr. 2.1 i vedlegget til denne forordning, i henhold til artikkel 8 nr. 3 bokstav a) i forordning (EU) nr. 910/2014,

b) håndtering av elektroniske identifikasjonsmidler, som fastsatt i nr. 2.2 i vedlegget til denne forordning, i henhold til artikkel 8 nr. 3 bokstav b) og f) i forordning (EU) nr. 910/2014,

c) autentisering, som fastsatt i nr. 2.3 i vedlegget til denne forordning, i henhold til artikkel 8 nr. 3 bokstav c) i forordning (EU) nr. 910/2014,

d) håndtering og organisering, som fastsatt i nr. 2.4 i vedlegget til denne forordning, i henhold til artikkel 8 nr. 3 bokstav d) og e) i forordning (EU) nr. 910/2014.

3. Når et elektronisk identifikasjonsmiddel innenfor rammen av en meldt ordning for elektronisk identifikasjon, oppfyller et krav oppført for et høyere sikkerhetsnivå, skal det antas å oppfylle det tilsvarende kravet for et lavere sikkerhetsnivå.

4. Med mindre det er angitt noe annet i den relevante delen av vedlegget, skal alle elementer oppført i vedlegget for et bestemt sikkerhetsnivå for elektroniske identifikasjonsmidler utstedt innenfor rammen av en meldt ordning for elektronisk identifikasjon, være oppfylt for å stemme overens med det aktuelle sikkerhetsnivået.

*Artikkel 2*

Denne forordning trer i kraft den 20. dagen etter at den er kunngjort i *Den europeiske unions tidende*.

Denne forordning er bindende i alle deler og kommer direkte til anvendelse i alle medlemsstater.

Utferdiget i Brussel 8. september 2015.

*For Kommisjonen*

Jean-Claude JUNCKER

*President*

*VEDLEGG*

**Tekniske spesifikasjoner og framgangsmåter for sikkerhetsnivåene «lavt», «betydelig» og «høyt» for elektroniske identifikasjonsmidler utstedt innenfor rammen av en meldt ordning for elektronisk identifikasjon**

1. **Definisjoner**

I dette vedlegg menes med:

1) «autoritativ kilde» enhver pålitelig kilde, uansett form, som med eksakthet kan gi data, informasjon og/eller dokumentasjon som kan benyttes til å fastslå identitet,

2) «autentiseringsfaktor» en faktor som bekreftes å være knyttet til en person, og som tilhører en av følgende kategorier:

a) «besittelsesbasert autentiseringsfaktor» en autentiseringsfaktor som personen skal bevise at den er i besittelse av,

b) «kunnskapsbasert autentiseringsfaktor» en autentiseringsfaktor som personen skal bevise at den har kjennskap til,

c) «iboende autentiseringsfaktor» en faktor som er basert på et fysisk attributt hos en fysisk person, og som personen skal bevise at den har,

3) «dynamisk autentisering» en elektronisk prosess der det benyttes kryptografi eller andre teknikker som et middel til å framstille, på anmodning, elektronisk dokumentasjon på at personen har kontroll over eller er i besittelse av identifikasjonsdataene, og som endres ved hver autentisering mellom personen og systemet som kontrollerer personens identitet,

4) «styringssystem for informasjonssikkerhet» en rekke prosesser og framgangsmåter som skal håndtere risiko knyttet til informasjonssikkerhet, slik at de ligger på akseptable nivåer.

2. **Tekniske spesifikasjoner og framgangsmåter**

Elementene i de tekniske spesifikasjonene og framgangsmåtene som beskrives i dette vedlegg, skal benyttes til å bestemme hvordan kravene og kriteriene i artikkel 8 i forordning (EU) nr. 910/2014 skal anvendes for elektroniske identifikasjonsmidler utstedt innenfor rammen av en ordning for elektronisk identifikasjon.

2.1. *Registrering*

2.1.1. Søknad og registrering

| Sikkerhetsnivå | Nødvendige elementer |
|---|---|
| Lavt | 1. Det sikres at søkeren er kjent med vilkårene for bruk av elektroniske identifikasjonsmidler.<br>2. Det sikres at søkeren er kjent med anbefalte sikkerhetstiltak knyttet til elektroniske identifikasjonsmidler.<br>3. Relevante identitetsdata som kreves ved bekreftelse og kontroll av identitet, samles inn. |
| Betydelig | Samme som lavt nivå. |

| | |
|---|---|
| Høyt | Samme som lavt nivå. |

2.1.2. Bekreftelse og kontroll av identitet (fysisk person)

| Sikkerhetsnivå | Nødvendige elementer |
|---|---|
| Lavt | 1. Personen kan antas å være i besittelse av et bevis som er godkjent av medlemsstaten der det søkes om det elektroniske identitetsmiddelet, og som representerer den påberopte identiteten.<br>2. Beviset kan antas å være ekte eller eksistere i henhold til en autoritativ kilde, og framstår som gyldig.<br>3. Den påberopte identiteten eksisterer i henhold til en autoritativ kilde, og det kan antas at vedkommende er den person som påberoper seg identiteten. |
| Betydelig | Kravene til lavt nivå, samt ett av alternativene i nr. 1–4, skal være oppfylt:<br>1. Det er kontrollert at personen er i besittelse av et bevis som er godkjent av medlemsstaten der det søkes om det elektroniske identitetsmiddelet, og som representerer den påberopte identiteten,<br>og<br>beviset kontrolleres for å fastslå at det er ekte, eller at det i henhold til en autoritativ kilde eksisterer og gjelder en virkelig person,<br>og<br>det er truffet tiltak for å minimalisere faren for at personens identitet ikke er den påberopte identiteten, for eksempel ved å ta hensyn risikoen for at beviset er tapt, stjålet, midlertidig opphevet, tilbakekalt eller utløpt,<br>eller<br>2. det legges fram et dokument i løpet av en registreringsprosess i medlemsstaten der dokumentet er utstedt, og dokumentet framstår som det tilhører personen som legger det fram,<br>og<br>det er truffet tiltak for å minimalisere faren for at personens identitet ikke er den påberopte identiteten, for eksempel ved å ta hensyn risikoen for at dokumentene er tapt, stjålet, midlertidig opphevet, tilbakekalt eller utløpt,<br>eller<br>3. når framgangsmåter som tidligere er benyttet av en offentlig eller privat enhet i samme medlemsstat, men for et annet formål enn utstedelse av elektroniske identifikasjonsmidler, gir en sikkerhet tilsvarende det som er oppført i nr. 2.1.2 for sikkerhetsnivået «betydelig», behøver den registreringsansvarlige enheten ikke gjenta de tidligere framgangsmåtene, forutsatt at den likeverdige sikkerheten bekreftes av et samsvarsvurderingsorgan som nevnt i artikkel 2 nr. 13 i europaparlaments- og rådsforordning (EF) nr. 765/2008([1]) eller av et tilsvarende organ, |

| Sikkerhetsnivå | Nødvendige elementer |
|---|---|
| | eller<br>4. når det elektroniske identifikasjonsmiddelet er utstedt på grunnlag av et gyldig, meldt elektronisk identifikasjonsmiddel med sikkerhetsnivået «betydelig» eller «høyt», og det samtidig tas hensyn til risikoen for en endring i personidentifikasjonsopplysningene, er det ikke nødvendig å gjenta bekreftelsen og kontrollen av identitet. Når det elektroniske identifikasjonsmiddelet som ligger til grunn ikke er meldt, skal sikkerhetsnivået «betydelig» eller «høyt» bekreftes av et samsvarsvurderingsorgan som nevnt i artikkel 2 nr. 13 i forordning (EF) nr. 765/2008, eller av et tilsvarende organ. |
| Høyt | Kravene i nr. 1 eller 2 skal være oppfylt:<br>1. Kravene til betydelig nivå, samt ett av alternativene oppført i bokstav a)–c), skal være oppfylt:<br>a) Når det er bekreftet at personen er i besittelse av et fotografisk eller biometrisk identifikasjonsbevis som er godkjent av medlemsstaten der det søkes om det elektroniske identitetsmiddelet, og beviset representerer den påberopte identiteten, kontrolleres beviset med sikte på å fastslå at det er gyldig i henhold til en autoritativ kilde,<br>og<br>søkeren identifiseres som den påberopte identiteten ved å sammenligne ett eller flere av personens fysiske kjennetegn med en autoritativ kilde,<br>eller<br>b) når framgangsmåter som tidligere er benyttet av en offentlig eller privat enhet i samme medlemsstat, men for et annet formål enn utstedelse av elektroniske identifikasjonsmidler, gir en sikkerhet tilsvarende det som er oppført i nr. 2.1.2 for sikkerhetsnivået «høyt», behøver den registreringsansvarlige enheten ikke gjenta de tidligere framgangsmåtene, forutsatt at den likeverdige sikkerheten bekreftes av et samsvarsvurderingsorgan som nevnt i artikkel 2 nr. 13 i forordning (EF) nr. 765/2008, eller av et tilsvarende organ<br>og<br>det treffes tiltak for å dokumentere at resultatene fra tidligere framgangsmåter fortsatt er gyldige,<br>eller<br>c) når det elektroniske identifikasjonsmiddelet er utstedt på grunnlag av et gyldig, meldt elektronisk identifikasjonsmiddel med sikkerhetsnivået «høyt», og det samtidig tas hensyn til risikoen for en endring i personidentifikasjonsopplysningene, er det ikke nødvendig å gjenta bekreftelsen og kontrollen av identitet. Når det elektroniske identifikasjonsmiddelet som ligger til grunn ikke er meldt, skal sikkerhetsnivået «høyt» bekreftes av et samsvarsvurderingsorgan som nevnt i artikkel 2 nr. 13 i forordning (EF) nr. 765/2008, eller av et tilsvarende organ,<br>og<br>det treffes tiltak for å dokumentere at resultatene av denne tidligere framgangsmåten for utstedelse av et meldt elektronisk identifikasjonsmiddel fortsatt er gyldig.<br>ELLER<br>2. når søkeren ikke legger fram et godkjent fotografisk eller biometrisk identifikasjonsbevis, benyttes samme framgangsmåte for å få et slikt godkjent fotografisk eller biometrisk identifikasjonsbevis som det som benyttes på nasjonalt plan i den aktuelle medlemsstaten av den registreringsansvarlige enheten. |

| Sikkerhetsnivå | Nødvendige elementer |
|---|---|

([1]) Europaparlaments- og rådsforordning (EF) nr. 765/2008 av 9. juli 2008 om fastsettelse av kravene til akkreditering og markedstilsyn for markedsføring av produkter, og om oppheving av forordning (EØF) nr. 339/93 (EUT L 218 av 13.8.2008, s. 30).

2.1.3. Bekreftelse og kontroll av identitet (juridisk person)

| Sikkerhetsnivå | Nødvendige elementer |
|---|---|
| Lavt | 1. Den juridiske personens påberopte identitet dokumenteres på grunnlag av bevis som er godkjent av medlemsstaten der det søkes om det elektroniske identitetsmiddelet. |
| | 2. Dokumentasjonen framstår som gyldig, og kan antas å være ekte eller eksistere i henhold til en autoritativ kilde, når oppføring av en juridisk person i den autoritative kilden er frivillig og er regulert ved en avtale mellom den juridiske personen og den autoritative kilden.<br>3. Den juridiske personen har ikke, i henhold til en autoritativ kilde, en status som er til hinder for at den handler som denne juridiske person. |
| Betydelig | Kravene til lavt nivå, samt ett av alternativene oppført i nr. 1–3, skal være oppfylt:<br>1. Den juridiske personens påberopte identitet dokumenteres på grunnlag av bevis som er godkjent av medlemsstaten der det søkes om det elektroniske identitetsmiddelet, herunder den juridiske personens navn, juridiske form, og (eventuelt) registreringsnummer,<br>og<br>beviset kontrolleres for å fastslå om det er ekte, eller om det eksisterer i henhold til en autoritativ kilde, når det kreves at den juridiske personen er oppført i den autoritative kilden for å kunne drive virksomhet i sin sektor,<br>og<br>det er truffet tiltak for å minimalisere faren for at personens identitet ikke er den påberopte identiteten, for eksempel ved å ta hensyn risikoen for at dokumentene er tapt, stjålet, midlertidig opphevet, tilbakekalt eller utløpt,<br>eller<br>2. når framgangsmåter som tidligere er benyttet av en offentlig eller privat enhet i samme medlemsstat, men for et annet formål enn utstedelse av elektroniske identifikasjonsmidler, gir en sikkerhet tilsvarende det som er oppført i nr. 2.1.3 for sikkerhetsnivået «betydelig», behøver den registreringsansvarlige enheten ikke gjenta de tidligere framgangsmåtene, forutsatt at den likeverdige sikkerheten bekreftes av et samsvarsvurderingsorgan som nevnt i artikkel 2 nr. 13 i forordning (EF) nr. 765/2008, eller av et tilsvarende organ,<br>eller<br>3. når det elektroniske identifikasjonsmiddelet er utstedt på grunnlag av et gyldig, meldt elektronisk identifikasjonsmiddel med sikkerhetsnivået «betydelig» eller «høyt», er det ikke nødvendig å gjenta bekreftelsen og kontrollen av identitet. Når det |

| Sikkerhetsnivå | Nødvendige elementer |
|---|---|
| | elektroniske identifikasjonsmiddelet som ligger til grunn ikke er meldt, skal sikkerhetsnivået «betydelig» eller «høyt» bekreftes av et samsvarsvurderingsorgan som nevnt i artikkel 2 nr. 13 i forordning (EF) nr. 765/2008, eller av et tilsvarende organ. |
| Høyt | Kravene til betydelig nivå, samt ett av alternativene oppført i nr. 1–3, skal være oppfylt:<br>1. Den juridiske personens påberopte identitet dokumenteres på grunnlag av bevis som er godkjent av medlemsstaten der det søkes om det elektroniske identitetsmiddelet, herunder den juridiske personens navn, juridiske form, og minst én entydig identifikasjon som representerer den juridiske personen, og som brukes i en nasjonal sammenheng,<br>og<br>beviset kontrolleres for å fastslå at det er gyldig i henhold til en autoritativ kilde,<br>eller |
| | 2. når framgangsmåter som tidligere er benyttet av en offentlig eller privat enhet i samme medlemsstat, men for et annet formål enn utstedelse av elektroniske identifikasjonsmidler, gir en sikkerhet tilsvarende det som er oppført i nr. 2.1.3 for sikkerhetsnivået «høyt», behøver den registreringsansvarlige enheten ikke gjenta de tidligere framgangsmåtene, forutsatt at den likeverdige sikkerheten bekreftes av et samsvarsvurderingsorgan som nevnt i artikkel 2 nr. 13 i forordning (EF) nr. 765/2008, eller av et tilsvarende organ,<br>og<br>det treffes tiltak for å dokumentere at resultatene av denne tidligere framgangsmåten fortsatt er gyldige,<br>eller<br>3. når det elektroniske identifikasjonsmiddelet er utstedt på grunnlag av et gyldig, meldt elektronisk identifikasjonsmiddel med sikkerhetsnivået «høyt», er det ikke nødvendig å gjenta bekreftelsen og kontrollen av identitet. Når det elektroniske identifikasjonsmiddelet som ligger til grunn ikke er meldt, skal sikkerhetsnivået «høyt» bekreftes av et samsvarsvurderingsorgan som nevnt i artikkel 2 nr. 13 i forordning (EF) nr. 765/2008, eller av et tilsvarende organ,<br>og<br>det treffes tiltak for å dokumentere at resultatene av denne tidligere framgangsmåten for utstedelse av et meldt elektronisk identifikasjonsmiddel fortsatt er gyldig. |



2.1.4. Knytning mellom fysiske og juridiske personers elektroniske identifikasjonsmidler

Følgende vilkår gjelder for knytning mellom en fysisk persons elektroniske identifikasjonsmiddel og en juridisk persons elektroniske identifikasjonsmiddel («knytning»):

1) Det skal være mulig å oppheve en knytning midlertidig og/eller tilbakekalle den. En knytnings livssyklus (for eksempel aktivering, midlertidig oppheving, fornyelse, tilbakekalling) skal forvaltes etter nasjonalt godkjente framgangsmåter.

2) Den fysiske personen som har sitt elektroniske identifikasjonsmiddel knyttet til en juridisk persons elektroniske identifikasjonsmiddel, kan delegere bruken av knytningen til en annen fysisk person etter nasjonalt godkjente framgangsmåter. Den fysiske personen som delegerer, skal imidlertid fortsatt være ansvarlig.

3) Knytning skal skje på følgende måte:

| Sikkerhetsnivå | Nødvendige elementer |
|---|---|
| Lavt | 1. Det kontrolleres at identiteten til den fysiske personen som handler på vegne av den juridiske personen, er bekreftet på lavt nivå eller høyere.<br>2. Knytningen er opprettet på grunnlag av nasjonalt godkjente framgangsmåter.<br>3. Den fysiske personen har ikke, i henhold til en autoritativ kilde, en status som er til hinder for at den handler på vegne av den juridiske personen. |
| Betydelig | Kravene lavt nivå nr. 3, samt:<br>1. Det kontrolleres at identiteten til den fysiske personen som handler på vegne av den juridiske personen, er bekreftet på betydelig eller høyt nivå. |
| | 2. Knytningen er opprettet på grunnlag av nasjonalt godkjente framgangsmåter, noe som førte til at knytningen ble registrert i en autoritativ kilde.<br>3. Knytningen er kontrollert på grunnlag av opplysninger fra en autoritativ kilde. |
| Høyt | Kravene til lavt nivå nr. 3 og betydelig nivå nr. 2, samt:<br>1. Det kontrolleres at identiteten til den fysiske personen som handler på vegne av den juridiske personen, er bekreftet på høyt nivå.<br>2. Knytningen er kontrollert på grunnlag av en entydig identifikasjon som representerer den juridiske personen og brukes på nasjonalt plan, og på grunnlag av opplysninger som på en entydig måte representerer den fysiske personen, fra en autoritativ kilde. |

2.2. *Håndtering av elektroniske identifikasjonsmidler*

2.2.1. De elektroniske identifikasjonsmidlenes karakteristika og utforming

| Sikkerhetsnivå | Nødvendige elementer |
|---|---|
| Lavt | 1. Det elektroniske identifikasjonsmiddelet benytter minst én autentiseringsfaktor.<br>2. Det elektroniske identifikasjonsmiddelet er utformet slik at utstederen treffer rimelige tiltak for å kontrollere at det bare brukes når eieren har kontroll over eller er i besittelse av det. |
| Betydelig | 1. Det elektroniske identifikasjonsmiddelet benytter minst to autentiseringsfaktorer fra ulike kategorier.<br>2. Det elektroniske identifikasjonsmiddelet er utformet slik at det kan antas det bare brukes dersom eieren har kontroll over eller er i besittelse av det. |

| | |
|---|---|
| Høyt | Kravene til betydelig nivå, samt:<br>1. Det elektroniske identifikasjonsmiddelet beskytter mot kopiering og manipulering, og mot angripere med høy angrepskapasitet.<br>2. Det elektroniske identifikasjonsmiddelet er utformet slik at eieren kan beskytte det på en trygg måte, og slik at det ikke brukes av andre. |

2.2.2. Utstedelse, levering og aktivering

| Sikkerhetsnivå | Nødvendige elementer |
|---|---|
| Lavt | Etter utstedelse leveres det elektroniske identifikasjonsmiddelet via en mekanisme som gjør at det kan antas at det bare leveres til den tiltenkte personen. |
| Betydelig | Etter utstedelse leveres det elektroniske identifikasjonsmiddelet via en mekanisme som gjør at det kan antas at det bare leveres til dets eier. |
| Høyt | Aktiveringsprosessen kontrollerer at det elektroniske identifikasjonsmiddelet ikke er levert til andre enn dets eier. |

2.2.3. Midlertidig oppheving, tilbakekalling og reaktivering

| Sikkerhetsnivå | Nødvendige elementer |
|---|---|
| Lavt | 1. Det er mulig å oppheve et elektronisk identifikasjonsmiddel midlertidig og/eller tilbakekalle det til rett tid og på en effektiv måte.<br>2. Det finnes tiltak for å hindre uautorisert midlertidig oppheving, tilbakekalling og/eller reaktivering.<br>3. Reaktivering skal bare finne sted bare dersom de samme sikkerhetskravene som før den midlertidige opphevingen eller tilbakekallingen fortsatt er oppfylt. |
| Betydelig | Samme som lavt nivå. |
| Høyt | Samme som lavt nivå. |

2.2.4. Fornyelse og erstatning

| Sikkerhetsnivå | Nødvendige elementer |
|---|---|
| Lavt | Samtidig som det tas hensyn til risikoen for en endring i personidentifikasjonsopplysningene, skal fornyelse eller erstatning oppfylle de samme sikkerhetskravene som ved opprinnelig bekreftelse og kontroll av identitet, eller være basert på et gyldig elektronisk identifikasjonsmiddel på samme eller høyere sikkerhetsnivå. |

| | |
|---|---|
| Betydelig | Samme som lavt nivå. |
| Høyt | Kravene til lavt nivå, samt:<br>Når fornyelse eller erstatning er basert på et gyldig elektronisk identifikasjonsmiddel, skal identitetsdataene kontrolleres mot en autoritativ kilde. |

2.3. *Autentisering*

Dette avsnittet omhandler truslene forbundet med bruken av autentiseringsordningen og inneholder en kravsliste for hvert sikkerhetsnivå. I dette avsnittet skal kontroller antas å stå i forhold til risikoene på det aktuelle nivået.

2.3.1. Autentiseringsordning

I tabellen nedenfor angis kravene per sikkerhetsnivå for autentiseringsordningen, som gjør det mulig for den fysiske eller juridiske personen å bruke det elektroniske identifikasjonsmiddelet til å bekrefte sin identitet overfor en tjenestebruker.

| Sikkerhetsnivå | Nødvendige elementer |
|---|---|
| Lavt | 1. Personidentifikasjonsopplysninger utleveres etter behørig kontroll av det elektroniske identifikasjonsmiddelet og dets gyldighet.<br>2. Når personidentifikasjonsopplysninger lagres som en del av autentiseringsordningen, sikres disse opplysningene slik at de beskyttes mot tap og kompromittering, herunder frakoplet analyse.<br>3. Autentiseringsordningen gjennomfører sikkerhetskontroller av det elektroniske identifikasjonsmiddelet, slik at det er svært usannsynlig at det er mulig for en angriper med økt grunnleggende angrepskapasitet å gjette seg til, avlytte, avspille eller manipulere kommunikasjonen og på den måten omgå autentiseringsordningen. |
| Betydelig | Kravene til lavt nivå, samt:<br>1. Personidentifikasjonsopplysninger utleveres etter behørig kontroll av det elektroniske identifikasjonsmiddelet og dets gyldighet ved dynamisk autentisering.<br>2. Autentiseringsordningen gjennomfører sikkerhetskontroller av det elektroniske identifikasjonsmiddelet, slik at det er svært usannsynlig at det er mulig for en angriper med moderat angrepskapasitet å gjette seg til, avlytte, avspille eller manipulere kommunikasjonen og på den måten omgå autentiseringsordningen. |
| Høyt | Kravene til betydelig nivå, samt:<br>Autentiseringsordningen gjennomfører sikkerhetskontroller av det elektroniske identifikasjonsmiddelet, slik at det er svært usannsynlig at det er mulig for en angriper med høy angrepskapasitet å gjette seg til, avlytte, avspille eller manipulere kommunikasjonen og på den måten omgå autentiseringsordningen. |

2.4. *Håndtering og organisering*

Alle deltakere som leverer en tjeneste knyttet til elektronisk identifikasjon over landegrensene («tilbydere»), skal ha dokumentert praksis for håndtering av informasjonssikkerhet, strategier og metoder for risikohåndtering, samt andre anerkjente kontroller som kan gi de relevante styrende organer for ordninger for elektronisk identifikasjon i de respektive medlemsstater sikkerhet for at effektiv praksis er innført. I hele nr.

2.4 skal alle krav/elementer antas å stå forhold til risikoene på et gitt nivå.

2.4.1. Generelle bestemmelser

| Sikkerhetsnivå | Nødvendige elementer |
|---|---|
| Lavt | 1. Tilbydere av operative tjenester som omfattes av denne forordning, er en offentlig myndighet eller en enhet anerkjent som en juridisk person i en medlemsstats nasjonale rett, som har en etablert organisasjon og er fullt operativ på alle områder som er relevante for leveringen av tjenestene.<br>2. Tilbyderne oppfyller alle lovfestede krav de er pålagt i forbindelse med drift og levering av tjenesten, blant annet hva slags opplysninger som kan innhentes, hvordan identitet bekreftes, samt hvilke opplysninger som kan lagres og hvor lenge.<br>3. Tilbyderne kan dokumentere sin evne til å påta seg risikoen ved erstatningsansvar, og at de har tilstrekkelige økonomiske midler til fortsatt drift og tjenestelevering.<br>4. Det er tilbydernes ansvar at alle forpliktelser som er satt ut til en annen enhet blir oppfylt, og at retningslinjene for ordningen blir fulgt, som om de selv hadde utført oppgavene.<br>5. Ordninger for elektronisk identifikasjon som ikke er opprettet i henhold til nasjonal rett, skal inneholde en effektiv plan for virksomhetsopphør. En slik plan skal innbefatte en ryddig avvikling av tjenesten, eller videreføring av en annen tilbyder, hvordan vedkommende myndigheter og sluttbrukere informeres, samt nærmere opplysninger om hvordan registre skal beskyttes, oppbevares og destrueres i samsvar med retningslinjene for ordningen. |
| Betydelig | Samme som lavt nivå. |
| Høyt | Samme som lavt nivå. |

2.4.2. Offentliggjorte meldinger og brukerinformasjon

| Sikkerhetsnivå | Nødvendige elementer |
|---|---|
| Lavt | 1. Det finnes en offentliggjort definisjon av tjenesten, som omfatter alle gjeldende vilkår og gebyrer, herunder eventuelle begrensninger i bruken. Tjenestedefinisjonen skal inneholde et personvernprogram.<br>2. Det skal innføres hensiktsmessige retningslinjer og framgangsmåter for å sikre at brukerne av tjenesten informeres til rett tid og på behørig måte om eventuelle endringer av tjenestedefinisjonen og av gjeldende vilkår og personvernprogram for den aktuelle tjenesten.<br>3. Det skal innføres hensiktsmessige retningslinjer og framgangsmåter som sikrer fullstendige og riktige svar på henvendelser om informasjon. |
| Betydelig | Samme som lavt nivå. |
| Høyt | Samme som lavt nivå. |

2.4.3. Håndtering av informasjonssikkerhet

| Sikkerhetsnivå | Nødvendige elementer |
|---|---|
| Lavt | Det finnes et effektivt styringssystem for informasjonssikkerhet, til håndtering og kontroll av risiko knyttet til informasjonssikkerhet. |
| Betydelig | Kravene til lavt nivå, samt:<br>Styringssystemet for informasjonssikkerhet følger dokumenterte standarder eller prinsipper for håndtering og kontroll av sikkerhetsrisiko. |
| Høyt | Samme som betydelig nivå. |

2.4.4. Registrering

| Sikkerhetsnivå | Nødvendige elementer |
|---|---|
| Lavt | 1. Relevante opplysninger registreres og ajourføres ved hjelp av et effektivt registreringssystem, der det tas hensyn til relevant lovgivning og god praksis i forbindelse med vern av personopplysninger og datalagring.<br>2. Opplysninger oppbevares, i den grad det er tillatt i henhold til nasjonal rett eller andre nasjonale administrative ordninger, og beskyttes så lenge det er behov for dem med sikte på revisjon, undersøkelse av sikkerhetsbrudd og oppbevaring, og destrueres deretter på en sikker måte. |
| Betydelig | Samme som lavt nivå. |
| Høyt | Samme som lavt nivå. |

2.4.5. Lokaler og personale

Tabellen nedenfor inneholder krav til lokaler og personale, og eventuelt til underleverandører, som utfører oppgaver som omfattes av denne forordning. Oppfyllelsen av hvert enkelt krav skal stå i forhold til risikoen knyttet til det aktuelle sikkerhetsnivået.

| Sikkerhetsnivå | Nødvendige elementer |
|---|---|
| Lavt | 1. Det finnes framgangsmåter for å sikre at personale og underleverandører har tilstrekkelig opplæring, kvalifikasjoner og erfaring til å kunne utføre sine oppgaver.<br>2. Det finnes tilstrekkelig med personale og underleverandører til å drive og vedlikeholde tjenesten i samsvar med de retningslinjer og framgangsmåter som gjelder for den.<br>3. Lokalene som benyttes til å levere tjenesten, kontrolleres kontinuerlig og beskyttes mot skader forårsaket av miljøhendelser, uautorisert tilgang og andre faktorer som kan påvirke tjenestens sikkerhet. |

| | |
|---|---|
| | 4. Lokalene som benyttes til å levere tjenesten, sikrer at adgangen til områder der personopplysninger og kryptografiske eller andre sensitive opplysninger oppbevares eller behandles, er begrenset til godkjent personale eller godkjente underleverandører. |
| Betydelig | Samme som lavt nivå. |
| Høyt | Samme som lavt nivå. |

2.4.6. Tekniske kontroller

| Sikkerhetsnivå | Nødvendige elementer |
|---|---|
| Lavt | 1. Det finnes passende tekniske kontroller til å håndtere risikoene knyttet til tjenestenes sikkerhet og sikre de behandlede opplysningenes fortrolighet, integritet og tilgjengelighet.<br>2. Elektroniske kommunikasjonskanaler som benyttes til å utveksle personopplysninger eller sensitive opplysninger, beskyttes mot avlytting, manipulering og avspilling.<br>3. Tilgang til sensitivt, kryptografisk materiale begrenses til funksjoner og applikasjoner som absolutt krever tilgang, dersom det benyttes til å utstede elektroniske identifikasjonsmidler og autentisering. Det skal sikres at et slikt materiale aldri lagres permanent i ren tekst.<br>4. Det finnes framgangsmåter som garanterer at sikkerheten opprettholdes over tid, og at det kan reageres på endrede risikonivåer, hendelser og sikkerhetsbrudd.<br>5. Alle medier som inneholder personopplysninger og kryptografiske eller andre sensitive opplysninger, lagres, transporteres og fjernes på en trygg og sikker måte. |
| Betydelig | Samme som lavt nivå, samt:<br>Sensitivt kryptografisk materiale beskyttes mot ulovlige inngrep dersom det benyttes til å utstede elektroniske identifikasjonsmidler og autentisering, |
| Høyt | Samme som betydelig nivå. |

2.4.7. Overholdelse og revisjon

| Sikkerhetsnivå | Nødvendige elementer |
|---|---|
| Lavt | Det gjennomføres jevnlig interne revisjoner som omfatter alle deler som er relevante for levering av tjenestene, for å sikre samsvar med relevante retningslinjer. |
| Betydelig | Det gjennomføres jevnlig uavhengige interne eller eksterne revisjoner som omfatter alle |

| | |
|---|---|
| | deler som er relevante for levering av tjenestene, for å sikre samsvar med relevante retningslinjer. |
| Høyt | 1. Det gjennomføres jevnlig uavhengige eksterne revisjoner som omfatter alle deler som er relevante for levering av tjenestene, for å sikre samsvar med relevante retningslinjer.<br>2. Når en ordning forvaltes direkte av et statlig organ, skjer revisjon i samsvar med nasjonal rett. |