Utfärdad:	Träder i kraft:	Giltighetstid:
x.x.2022	x.4.2022	tills vidare

Rättsgrund

Lagen om stark autentisering och betrodda elektroniska tjänster (617/2009) 42 §, sådan den lyder efter ändring genom lagen 230/2021

Om följderna vid verksamhet mot bestämmelsen stiftas i:

Lag 617/2009 45 §, 45 a §

Genomförd EU-lagstiftning:
-

Ändringsuppgifter:
Genom denna föreskrift upphävs föreskriften Kommunikationsverket 72 A/2018 M

Föreskrift om elektroniska identifieringstjänster och betrodda elektroniska tjänster (M72 B/2022)

Innehållsförteckning

1 kap. Allmänna bestämmelser

1 Tillämpningsområde

1.1

Denna föreskrift tillämpas på tillhandahållande av sådana identifieringsverktyg för stark autentisering och sådana tjänster för identifieringsförmedling som avses i lagen om stark autentisering och betrodda elektroniska tjänster (617/2009, nedan benämnd *autentiseringslagen*) och som har anmälts till Transport- och kommunikationsverket samt på bedömning av deras överensstämmelse.

1.2

Denna föreskrift tillämpas på sådana kvalificerade betrodda elektroniska tjänster, en sådan bedömning av deras överensstämmelse och en sådan certifiering av anordningar för skapande av elektroniska underskrifter eller stämplar som avses i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG (nedan benämnd *EU:s förordning om elektronisk identifiering och betrodda tjänster*, eller *eIDAS-förordningen*).

1.3

Denna föreskrift tillämpas på de system för stark autentisering som avses 1 punkten eller på betrodda tjänster som avses i 2 punkten som ska anmälas till Europeiska kommissionen och på bedömning av deras överensstämmelse samt certifiering av anordningar för skapande av elektroniska underskrifter eller stämplar endast om inget annat följer av eIDAS-förordningen eller kommissionens genomförandeakter som har getts med stöd av eIDAS.

2 Syfte

Syftet med denna föreskrift är att

1) främja informationssäkerheten och den tekniska interoperabiliteten i identifieringsverktyg för stark autentisering och i tjänster för identifieringsförmedling,

2) precisera kriterierna för bedömning av överensstämmelse i fråga om tjänster för stark autentisering och kriterierna för oberoende och kompetens hos bedömningsorgan,

3) komplettera kraven för kvalificerade betrodda elektroniska tjänster och kriterierna för bedömning av överensstämmelse i fråga om deras oberoende och kompetens till den del bestämmelser om dessa inte ingår i Europeiska unionens lagstiftning; samt

4) komplettera kriterierna för certifiering av anordningar för skapande av elektroniska underskrifter eller stämplar till den del bestämmelser om dessa kriterier inte ingår i Europeiska unionens lagstiftning.

3 Definitioner

3.1

I denna föreskrift avses med

1) *gränssnitt* specifikationer och implementeringar som gäller dataöverföring mellan två olika system eller delar av systemen;

2) *certifikat* ett elektroniskt intyg vars syfte är att visa att innehavaren av intyget är en viss person, en viss organisation eller ett visst system, och som kopplar ihop autentiseringsuppgifter med innehavaren.

3.2

I denna föreskrift följs också de definitioner som ges i 2 § i autentiseringslagen, artikel 3 i eIDAS-förordningen samt punkt 1 i bilagan till kommissionens genomförandeförordning (EU) 2015/1502, nedan *förordningen om tillitsnivåer vid elektronisk identifiering*, som utfärdats i enlighet med artikel 8.3 i eIDAS-förordningen.

2 kap. Krav på informationssäkerhet i en identifieringstjänst

4 System för ledning av informationssäkerheten hos leverantörer av identifieringstjänster

4.1 Standard för ledning av informationssäkerheten

Vid ledning avseende informationssäkerheten i identifieringssystem ska leverantörerna av identifieringstjänster följa standarden ISO/IEC 27001 eller någon annan allmänt känd motsvarande standard för ledning avseende informationssäkerhet. Ledningen avseende informationssäkerheten kan också bygga på en kombination av flera standarder.

4.2 Informationssäkerhetsledningens täckning

Ledningen avseende informationssäkerheten ska omfatta följande delområden som påverkar tillhandahållandet av en identifieringstjänst:

1) identifieringstjänsteleverantörens verksamhetsmiljö som en helhet,

2) styrning, organisering och administration av ledningen avseende informationssäkerheten,

3) hantering av informationssäkerhetsrisker vid tillhandahållande av en identifieringstjänst,

4) resurser för informationssäkerheten, kompetens, personalens medvetenhet om informationssäkerheten, kommunikation och dokumentation samt administration av dokumenterad information,

5) planering och styrning av tillhandahållandet av en identifieringstjänst för att informationssäkerhetskraven ska kunna uppfyllas, och

6) bedömning av effektivitet och funktion i ledningen avseende informationssäkerheten.

5 Krav på informationssäkerhet i identifieringssystem

5.1 Identifieringssystemets skyddsförmåga

5.1.1

Identifieringssystemets datakommunikation och informationssystem samt användningen av dem ska planeras, förverkligas och kontinuerligt upprätthållas under hela deras livscykel så att identifieringstjänstens integritet och sekretess skyddas. Identifieringstjänsten ska ha skyddsförmåga åtminstone på tillitsnivån väsentlig eller hög mot hot och angreppspotential enligt punkt 2.3 i bilagan till förordningen om tillitsnivåer vid elektronisk identifiering, i enlighet med identifieringstjänstens tillitsnivå.

5.1.2

Krypteringskraven för datakommunikationsförbindelser mellan leverantörer av identifieringstjänster samt mellan identifieringstjänster och förlitande parter definieras i punkt 7. I identifieringssystemets övriga datakommunikationsförbindelser samt i krypteringen av informationssystem och information ska man till de delar det är tekniskt tillämpligt använda krypteringslösningar enligt punkt 7 i föreskriften, om inte skyddsförmågan bedömd som helhet förverkligas genom andra säkerhetsåtgärder.

5.2 Datakommunikationssäkerhet

I identifieringssystemets datakommunikation ska man planera, förverkliga och kontinuerligt upprätthålla

a) säkerhet i nätstrukturen,

b) indelning av datakommunikationsnätet i zoner,

c) filtreringsregler enligt principen om behovsenlig behörighet,

d) administration av filtrering och kontrollsystem,

e) säkra administrationsförbindelser; samt

f) använda krypteringslösningar som rekommenderas internationellt eller nationellt.

5.3 Säkerhet i informationssystem

I identifieringssystemets informationssystem ska man planera, förverkliga och kontinuerligt upprätthålla

a) hantering av behörigheter enligt principen om behovsenlig behörighet,

b) individuell identifiering av systemanvändarna,

c) härdande av system,

d) ett skydd mot skadliga program,

e) förmågan och en process för att spåra säkerhetsrelaterade händelser,

f) förmågan att upptäcka avvikelser och en process för att åtgärda dem, och

g) använda krypteringslösningar som rekommenderas internationellt eller nationellt.

5.4 Säkerhet vid användning

I driften av identifieringssystemet ska man planera, förverkliga och kontinuerligt upprätthålla

a) omsorgsfull hantering av förändringar,

b) en behandlingsmiljö och förvaring för sekretessbelagt material som baserar sig på klassificeringen av informationen,

c) ett skydd av användning och administration på distans mot hot i distansanvändningsmiljön,

d) hantering av programutveckling och sårbarheter i programvara,

e) säkerhetskopiering; samt

f) använda krypteringslösningar som rekommenderas internationellt eller nationellt.

5.5 Administratörs- och distansförbindelser i identifieringssystemets produktionsnät

Ett produktionsnät och administrationsförbindelser samt distansanvändning och -administration enligt underpunkterna 5.2 e) och 5.4 c) ovan ska genomföras så att informationssäkerhetshot som orsakas av organisationens övriga tjänster, som e-post eller webbsurfning, samt informationssäkerhetshot som orsakas av organisationens terminalenhet vid hantering av andra funktioner än de som är nödvändiga för hanteringen är

a) speciellt bedömda och minimerade på tillitsnivån väsentlig och

b) förhindrade bedömda som helhet på tillitsnivån hög.

6 Informationssäkerhetskrav på identifieringsmedlet

6.1 Identifieringsmedlets egenskaper och skyddsförmåga

6.1.1

Identifieringsmedlets autentiseringsfaktorer, autentiseringsmekanism och säkerhetsåtgärder ska planeras, genomföras och upprätthållas så att de skyddar identifieringsmedlets integritet och sekretess. Identifieringsmedlet ska ha skyddsförmåga åtminstone på tillitsnivån väsentlig eller hög mot hot och angreppspotential enligt punkt 2.3 i bilagan till förordningen om tillitsnivåer vid elektronisk identifiering, i enlighet med identifieringstjänstens tillitsnivå.

Skyddsförmågan ska basera sig på en riskbedömning, där man separat bedömer hot mot autentiseringsfaktorer och -mekanismer som baserar sig på innehav, information och egenskaper samt säkerhetsåtgärder som skyddar mot hoten.

6.1.2

Genom identifieringsmedlets egenskaper och säkerhetsåtgärder ska man förhindra att äventyrande av en autentiseringsfaktor äventyrar tillförlitligheten hos andra autentiseringsfaktorer. Genom identifieringsmedlets säkerhetsåtgärder ska man separera och skydda autentiseringsfaktorerna i synnerhet om de används på samma terminal.

6.1.3

I identifieringsmedlet och autentiseringen måste man använda krypteringslösningar som rekommenderas internationellt eller nationellt. I datakommunikationsförbindelsen mellan identifieringsverktyget och identifieringssystemet ska man till de delar det är tekniskt tillämpligt använda krypteringslösningar enligt punkt 7 i föreskriften, om inte skyddsförmågan bedömd som helhet förverkligas genom andra säkerhetsåtgärder.

6.2 Särskilda säkerhetsåtgärder

6.2.1

Vid en identifiering ska identifieringstjänsten visa information för användaren av identifieringsverktyget utifrån vilken användaren kan koppla ihop den bekräftelsebegäran som kommer till identifieringsverktyget med det aktuella ärendet. Visning av informationen är obligatorisk vid sådana identifieringsmedel där det är tekniskt möjligt.

6.2.2

Vid identifieringen ska identifieringstjänsten visa användaren av identifieringsverktyget information om den förlitande parten till vilken identifieringen förmedlas. Visning av informationen är obligatorisk vid sådana identifieringsmedel där det är tekniskt möjligt.

6.2.3

Med samlad inloggning avses i denna föreskrift att identifieringstjänsten erbjuder fler än en förlitande part bekräftelse utifrån en autentisering av en innehavare av ett identifieringsverktyg som gjorts med ett starkt elektroniskt identifieringsmedel.

Identifieringstjänsten ska i planeringen, genomförandet och upprätthållandet av samlad inloggning sörja för säkerhetsåtgärder som anknyter till hanteringen av samlade inloggningssessionernas längd samt överföringen och avslutandet av dem samt för att visa uppgifter om sådana förlitande parter som avses i punkt 6.2.2 för användaren.

6.3 Koppling av ett identifieringsverktyg till en person

6.3.1

Identifieringsmedlets autentiseringsfaktorer ska kopplas till innehavaren av identifieringsverktyget i identifieringssystemet.

6.3.2

Identifieringsverktyg får inte kopplas med den sökande förrän en inledande identifiering av den sökande har gjorts, eller så ska det vid processen för beviljande av identifieringsverktyg på annat sätt säkerställas att identifieringsverktyget inte kan användas innan en inledande identifiering av sökanden enligt 17 § i autentiseringslagen har gjorts.

6.4 Behandling av innehavarspecifika uppgifter i identifieringsmedlet

6.4.1

Leverantören av identifieringstjänsten ska säkerställa att hemliga uppgifter om identifieringsverktyget inte under några omständigheter röjs för dess personal.

6.4.2

Leverantören av identifieringstjänsten får inte kopiera hemliga uppgifter om identifieringsverktyget.

7 Krypteringskrav på identifieringssystemets gränssnitt

7.1 Krypteringsmetoder för datakommunikationen

7.1.1

Trafiken i gränssnitten mellan leverantörer av identifieringstjänster och mellan leverantörer av identifieringstjänster och förlitande parter ska krypteras. Följande metoder ska användas vid kryptering, vid nyckelutbyte, i certifikat och i underskrifter i anslutning till kryptering:

1) **Nyckelutbyte:** DHE-metoder, eller ECDHE-metoder som använder elliptiska kurvor, ska användas vid nyckelutbyte. Den ändliga kroppen (finite field) som används i räkneoperationer ska utgöra minst 2 048 bitar i DHE-metoden och minst 224 bitar i ECDHE-metoden.

2) **Underskrift eller asymmetrisk kryptering:** Vid användning av RSA för elektronisk underskrift eller kryptering ska nyckeln utgöra minst 2 048 bitar. Vid användning av metoder för elliptisk kurva från ECDSA eller EdDSA ska storleken på den ändliga kroppen vara minst 224 bitar.

3) **Symmetrisk kryptering:** Krypteringsalgoritmen ska vara AES, Serpent eller ChaCha20. Nyckeln ska utgöra minst 128 bitar. Krypteringsläget ska vara CBC, CCM, GCM eller CTR.

4) **Hashfunktioner:** Hashfunktionen eller autentiseringskoden ska vara SHA-2, SHA-3, Whirlpool eller Poly1305.

7.1.2

Utöver de som nämns i punkt 7.1.1 kan man följa metoder och värden som har bedömts vara säkra för sådan användning som avses i underpunkterna 1–4 i de aktuella versionerna av följande dokument:

a) Anvisningen Kryptografiset vahvuusvaatimukset luottamuksellisuuden suojaamiseen – kansalliset turvallisuusluokat (Dnr 190/651/2015) av myndigheten för godkännande av krypteringsprodukter *(Crypto Approval Authority)* inom Transport- och kommunikationsverket, eller

b) dokumentet SOG-IS Crypto Evaluation Shceme Agreed Cryptographic Mechanisms, utgivet av vissa certifieringsorgan i EU-medlemsstater eller i medlemsstater i EES-området (*Senior Officers Group for Information Systems, Mutual Recognition Agreement SOGIS-MRA*).

7.1.3

Krypteringsinställningarna ska tekniskt tvingas till miniminivåerna ovan för att handskakningen inte ska resultera i inställningar som är sämre än miniminivåerna.

7.2 Krypteringsprotokoll för datakommunikationen

Om man använder TLS-protokoll ska man använda minst version 1.2.

8 Verifiering av parterna i datakommunikationen

8.1 Identifiering av parterna i en datakommunikationsförbindelse

När man upprättar en datakommunikationsförbindelse mellan identifieringstjänster eller mellan en identifieringstjänst och en förlitande part måste man autentisera äktheten och integriteten hos de certifikat som används för att kryptera datakommunikationen eller meddelandena samt deras innehavare.

Autentiseringen ska basera sig på en kvalificerad elektronisk underskrift eller en kvalificerad elektronisk stämpel enligt eIDAS-förordningen eller direkt på ett bilateralt förfarande. Autentiseringen kan inte baseras endast på ett certifikat som det råder allmänt förtroende för.

8.2 Förnyande av certifikat och nycklar

De certifikat och nycklar som avses ovan i punkt 8.1 ska förnyas regelbundet.

För att säkerställa äktheten och integriteten hos nya certifikat och nycklar ska förnyelsen göras antingen

a) enligt det förfarande som beskrivs i punkt 8.1,

b) genom att skicka de nya nycklarna via en datakommunikationsförbindelse vars integritet och sekretess har säkerställts genom att knyta parternas datakommunikation till certifikat eller nycklar som levererats enligt punkt 8.1, eller

c) genom att underteckna de nya nycklarna med en nyckel som levererats enligt punkt 8.1.

9 Identifieringsmeddelandenas integritet och sekretess

9.1 Kryptering av meddelanden mellan identifieringstjänster och en förlitande part

9.1.1

I datakommunikation mellan identifieringstjänster samt mellan en identifieringstjänst och en förlitande part måste man trygga integriteten och sekretessen hos identifieringsmeddelanden som innehåller personuppgifter antingen

a) genom att säkerställa datakommunikationsförbindelsens integritet och sekretess genom att knyta parternas datakommunikation till certifikat eller nycklar som levererats enligt punkt 8, eller

b) genom att kryptera och underteckna meddelandena med nycklar som levererats enligt punkt 8.

9.1.2

I datakommunikation mellan tjänsten för identifieringsförmedling och den förlitande part måste identifieringsmeddelanden autentiseras genom underskrift.

9.2 Kryptering av meddelanden i användargränssnittet

Om identifieringsmeddelanden förmedlas via användarens webbläsare eller terminal, måste de krypteras och undertecknas enligt underpunkt 9.1.1.b.

9.3 Krypteringsalgoritmer och metoder

Vid krypteringen och undertecknandet av meddelanden ska man till tillämpliga delar använda metoder enligt punkt 7.1.

10 Krav på informationssäkerhet i gränssnitt för en nationell nod

Gränssnittet mellan leverantören av tjänster för identitetsförmedling och den nationella noden ska uppfylla de krav som definieras i punkt 7–9.

11 Anmälningar om störningar från leverantören av identifieringstjänsten till Transport- och kommunikationsverket

11.1 Betydande hot eller störningar

Till de betydande störningar i identifieringstjänster som ska anmälas till Transport- och kommunikationsverket enligt 16 § i autentiseringslagen hör händelser som anknyter till felaktigheter i eller missbruk av en elektronisk identitet eller ett hot mot eller en störning i informationssäkerheten, som äventyrar identifieringens integritet och tillförlitlighet. Även oförutsedda funktionsstörningar som har större än ringa negativa effekter för förtroendenätet räknas som betydande.

11.2 Uppgifter som ska anmälas

I en anmälan till Transport- och kommunikationsverket om ett betydande hot eller en betydande störning ska åtminstone följande uppgifter ingå:

1) identifieringsverktyget eller tjänsten för identifieringsförmedling som störningen eller hotet påverkar,
2) en beskrivning av störningen eller hotet och dess kända orsaker samt varaktighet,
3) en beskrivning av störningens eller hotets konsekvenser, inklusive konsekvenser för beviljandet av nya identifieringsverktyg samt för användare, förlitande parter, andra aktörer i förtroendenätet och gränsöverskridande användning,
4) en beskrivning av korrigerande åtgärder, och
5) en beskrivning av informationen om störningen eller hotet till förlitande parter, innehavare av identifieringsverktyg och förtroendenätet samt uppgift om anmälan till andra myndigheter.

11.3 Anmälningsförfarande

Anmälningar om betydande störningar eller hot ska göras elektroniskt via Transport- och kommunikationsverkets webbformulär, e-post eller säker e-post.

Uppgifterna i anmälan kan kompletteras senare, om alla uppgifter inte är tillgängliga när man gör en första anmälan enligt 16 § i autentiseringslagen utan oskäligt dröjsmål.

3 kap. Identifieringstjänsternas interoperabilitet

12 Minimiuppsättning uppgifter som ska förmedlas i förtroendenätet

12.1 Obligatoriska uppgifter

Följande uppgifter ska förmedlas via gränssnitten mellan leverantörer av identifieringsverktyg och leverantörer av tjänster för identifieringsförmedling:

1) vid identifiering av en fysisk person åtminstone den identifieringsuppgift som identifierar personen som säkerställts av leverantören av identifieringsverktyget samt personens förnamn, efternamn och födelsedatum,

2) vid identifiering av en juridisk person åtminstone den identifieringsuppgift som säkerställts av leverantören av identifieringsverktyget som identifierar den fysiska personen som företräder den juridiska personen, personens efternamn och förnamn samt den identifieringsuppgift som identifierar organisationen,

3) information om huruvida identifieringsverktyget ligger på tillitsnivån väsentlig eller hög, och

4) information som säkerställts av tjänsten för identifieringsförmedling om den förlitande parten

12.2 Valfria uppgifter

Gränssnitten mellan leverantörer av identifieringsverktyg och leverantörer av tjänster för identifieringsförmedling ska ha tekniskt planerad beredskap att förmedla följande uppgifter:

1) information om huruvida en identifieringstransaktion gäller en offentlig eller en privat tjänst för ärendehantering,

2) vid identifiering av en fysisk person: förnamn och efternamn vid födseln, födelseort, nuvarande adress och kön,

3) vid identifiering av en juridisk person:

   a) nuvarande adress,

   b) momsregistreringsnummer,

   c) skatteregisteringsnummer,

   d) den identifikator som avses i artikel 3.1 i Europaparlamentets och[1] rådets direktiv 2009/101/EG,

[1] Europaparlamentets och rådets direktiv 2009/101/EG av den 16 september 2009 om samordning av de skyddsåtgärder som krävs i medlemsstaterna av de i artikel 48 andra stycket i fördraget avsedda bolagen i bolagsmännens och tredje mans intressen, i syfte att göra skyddsåtgärderna likvärdiga inom gemenskapen (EUT L 258, 1.10.2009, s. 11).

e) den identifieringskod för juridiska personer (LEI) som avses i[2] kommissionens genomförandeförordning (EU) nr 1247/2012,

f) det registrerings- och identitetsnummer för ekonomiska aktörer (EORI-nummer)[3] som avses i kommissionens genomförandeförordning (EU) nr 1352/2013, och

g) punktskattenummer som avses i artikel 2.12 [4]i rådets förordning nr 389/2012.

12.3 Pseudonymisering av identifiering

De skyldigheter som definieras ovan i punkterna 12.1 och 12.2 gäller gränssnittet mellan identifieringsverktyget och tjänsten för identifieringsförmedling vid autentisering av identifieringsverktygets användare även i fall där tjänsten för identifieringsförmedling på det sätt som avses i 8 § 2 mom. i autentiseringslagen endast meddelar den förlitande parten en pseudonym för användaren av identifieringsverktyget eller en begränsad mängd personuppgifter.

13 Uppgifter som förutsätts vid gränsöverskridande identifiering

Vid identifiering med finländska identifieringsverktyg som anmälts enligt eIDAS-förordningen i utländska tjänster för ärendehantering ska samma uppgifter förmedlas i gränssnittet mellan leverantören av identifieringsverktyget och leverantören av tjänsten för identifieringsförmedling som vid nationell identifiering i förtroendenätet enligt punkt 12. Uppgifterna ska kunna vidarebefordras mellan tjänsten för identifieringsförmedling och den nationella noden. Dessutom ska man förmedla information om huruvida identifieringstransaktionen gäller en offentlig eller en privat tjänst för ärendehantering.

14 Protokoll som används vid dataöverföring samt övriga krav

14.1 Protokoll som används vid dataöverföring

Leverantören av identifieringstjänsten ska för egen del möjliggöra sammankoppling av inledande identifieringar enligt 17 § i autentiseringslagen samt förmedling av identifieringar i förtroendenätet enligt 12 a § i autentiseringslagen åtminstone via gränssnitt enligt Open IDConnect- eller SAML-protokollet.

14.2 Gränssnittets övriga egenskaper

Leverantörer av identifieringsverktyg, leverantörer av tjänster för identifieringsförmedling och förlitande parter samt genomföraren av den nationella noden kan sinsemellan avtala om sådana övriga egenskaper för gränssnitten mellan dem och sådana tillämpliga protokoll som inte fastställs i denna föreskrift.

[2] Kommissionens genomförandeförordning (EU) nr 1247/2012 av den 19 december 2012 om fastställande av tekniska genomförandestandarder för form och frekvens för rapportering om handel till transaktionsregister enligt Europaparlamentets och rådets förordning (EU) nr 648/2012 om OTC-derivat, centrala motparter och transaktionsregister (EUT L 352, 21.12.2012, s. 20).
[3] Kommissionens genomförandeförordning (EU) nr 1352/2013 av den 4 december 2013 om fastställande av de formulär som avses i Europaparlamentets och rådets förordning (EU) nr 608/2013 om tullens säkerställande av skyddet för immateriella rättigheter (EUT L 341, 18.12.2013, s. 10).
[4] Rådets förordning (EU) nr 389/2012 av den 2 maj 2012 om administrativt samarbete i fråga om punktskatter och om upphävande av förordning (EG) nr 2073/2004 (EUT L 121, 8.5.2012, s. 1).

4 kap. Kriterier för bedömning av en identifieringstjänst

15 Bedömningskriterier för överensstämmelse

15.1 Funktioner som ska bedömas i identifieringssystemet och identifieringsmedlet

En bedömning enligt 29 § i autentiseringslagen måste omfatta alla de krav som ställs i lagen och i denna föreskrift som gäller

1) funktioner som påverkar tillhandahållandet av identifieringstjänsten (ett identifieringssystem)
    a) ledningen avseende informationssäkerhet
    b) förvaringen och behandlingen av uppgifter
    c) anläggningarna och personalen
    d) tekniska kontroller
    e) interoperabiliteten i förtroendenätet
2) identifieringsmedlet, dvs. identifieringsverktyget
    a) ansökan och registreringen
    b) styrkandet och kontrollen av den sökandes identitet
    c) identifieringsmedlets egenskaper och utformning
    d) utfärdandet, leveransen och aktiveringen
    e) upphävande, återkallelse och återaktivering
    f) förnyelse och ersättning
    g) autentiseringsmekanismerna.

15.2 Bedömningskriterier

Bedömningen av överensstämmelsen kan basera sig på Transport- och kommunikationsverkets bedömningsanvisning eller bestämmelser eller anvisningar som utfärdats av EU eller något annat internationellt organ, offentliggjorda och allmänt eller regionalt tillämpade anvisningar om informationssäkerhet eller allmänt använda standarder eller förfaranden för informationssäkerhet. Bedömningen kan basera sig på en kombination av flera av ovan nämnda källor.

16 Utredning av tillförlitligheten hos leverantören av en identifieringstjänst och de publicerade uppgifterna

Leverantören av en identifieringstjänst ska i sin anmälan enligt 10 § i autentiseringslagen genom en egen skriftlig utredning eller en oberoende och behörig utredning eller bedömning visa att följande krav på tillförlitligheten hos leverantören av identifieringstjänster och uppgifterna om identifieringstjänsten uppfylls:

1) en etablerad juridisk person som ansvarar för identifieringstjänsten samt de ansvarigas handlingsbehörighet och tillförlitlighet,

2) offentliggjorda meddelanden och användaruppgifter, såsom identifieringsprinciper, dataskyddsprinciper, användningsbegränsningar, avtalsvillkor och prislistor,

3) tillräckliga ekonomiska resurser för att ordna verksamheten och täcka eventuellt skadeståndsansvar,

4) ansvar för underleverantörer, och

5) en plan för att avsluta eller överföra tjänsten på ett kontrollerat sätt, behandla uppgifterna samt göra anmälningar till myndigheter, förtroendenätet, de förlitande parter och användarna om verksamheten avslutas.

17 Grunder för bedömning av den nationella noden

Bedömningen av informationssäkerheten i den nationella noden ska bygga på ISO/IEC 27001 och Europeiska kommissionens genomförandeförordning (EU) 2015/1501[5] .

5 kap. Kompetensen hos bedömningsorgan för identifieringstjänster

18 Krav på utomstående bedömningsorgan för identifieringstjänster

18.1 Bevisningsförfaranden

Att de oberoende- och kompetenskrav som ställs på bedömningsorgan i 33 § i autentiseringslagen är uppfyllda kan visas genom

1) ackreditering enligt standarden ISO/IEC 27001 eller genom att på annat sätt visa kompetensen för bedömning enligt standarden,

2) kompetens som har visats i enlighet med en internationellt känd självregleringsmetod som bygger på WebTrust-reglerna,

3) ackreditering enligt betalkortsstandarden PCI DSS eller genom att på annat sätt visa kompetensen för bedömning enligt standarden,

4) kompetens som har visats i enlighet med ISACA:s tillsynsram för standarder och informationssystem, eller

5) att visa eller följa en sådan kompetens som förutsätts i andra, med de ovannämnda jämställbara bestämmelser, anvisningar eller standarder för allmän ledning avseende informationssäkerhet eller sektorspecifik reglering eller standardisering.

[5] Kommissionens genomförandeförordning om interoperabilitetsramverket enligt artikel 12.8 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden

18.2 Kompetens

Att visa kompetensen för bedömning av identifieringssystem förutsätter att man också visar hur och till vilka delar de bestämmelser, anvisningar eller standarder som avses i punkt 18.1 gäller kraven på identifieringssystem.

19 Krav på interna kontrollorgan för identifieringstjänster

19.1 Oberoende

Att de oberoendekrav som ställs på interna kontrollorgan i 33 § i autentiseringslagen är uppfyllda kan visas genom att iaktta

1) IIA:s professionella standarder (oberoende och objektivitet vid intern kontroll, inklusive organisatoriskt oberoende),

2) ISACA:s tillsynsram för standarder och informationssystem,

3) BIS (Bank for International Settlements) guide som gäller intern kontroll,

4) föreskrifterna och anvisningarna om intern kontroll i Finansinspektionens samling av föreskrifter och anvisningar,

5) anvisningar och föreskrifter som utfärdats av motsvarande tillsynsmyndigheter i övriga medlemsstater inom EES-området, eller

6) andra med de ovannämnda jämställbara standarder för myndighetsreglering eller allmän hantering av oberoende intern kontroll.

19.2 Kompetens

Att visa kompetensen för bedömning av identifieringssystem förutsätter att man också visar hur och till vilka delar en intern kontroll som är organiserad enligt de bestämmelser, anvisningar eller standarder som avses i punkt 19.1 riktas mot kraven på identifieringssystemet.

6 kap. Kvalificerade betrodda tjänster

20 Kriterier för bedömning av kvalificerade tillhandahållare av betrodda tjänster

20.1 Standarder

20.1.1

Kvalificerade tillhandahållare av betrodda tjänster ska uppfylla kraven i eIDAS-förordningen och standarden SFS-EN 319 401.

20.1.2

Kvalificerade tillhandahållare av betrodda tjänster som beviljar kvalificerade certifikat för elektroniska underskrifter eller stämplar eller autentisering av webbplatser ska uppfylla kraven i punkt 20.1.1 samt standarderna EN 319 411-1 och EN 319 411-2.

20.1.3

Kvalificerade tillhandahållare av betrodda tjänster som beviljar kvalificerade tidsstämplingar ska uppfylla kraven i punkt 20.1.1 och standarden EN 319 421.

20.2 Standardernas frivillighet

Uppfyllande av kraven kan visas genom att iaktta standarderna i punkt 20.1 eller på något annat sätt på vilket motsvarande tillförlitlighet kan uppnås.

21 Kriterier för bedömning av kvalificerade betrodda tjänster

21.1 Standarder

21.1.1

Kvalificerade certifikat som beviljas av kvalificerade betrodda tjänster ska uppfylla kraven i eIDAS-förordningen på certifikat för elektroniska underskrifter och stämplar och autentisering av webbplatser samt i tillämpliga delar kraven i standarderna EN 319 412-1, EN 319 412-2, EN 319 412-3, EN 319 412-4 och EN 319 412-5.

21.1.2

Kvalificerade tjänster för tidsstämpling ska använda protokollet och profilen för tidsstämpling enligt EN 319 422.

21.1.3

En kvalificerad valideringstjänst för kvalificerade elektroniska underskrifter eller stämplar ska utöver kraven i eIDAS-förordningen även uppfylla kraven i standarden EN 319 102-1

21.1.4

Kvalificerade elektroniska tjänster för rekommenderade leveranser (*qualified electronic registered delivery services*) ska utöver kraven i eIDAS-förordningen även uppfylla kraven i standarderna EN 319 521 och EN 319 522.

21.2 Standardernas frivillighet

Uppfyllande av kraven kan visas genom att iaktta standarderna i punkt 21.1 eller på något annat sätt på vilket motsvarande tillförlitlighet kan uppnås.

7 kap. Bedömningsorgan för överensstämmelse hos betrodda tjänster

22 Bedömning av bedömningsorgans kompetens

22.1 Bedömningsorganets verksamhet

För att ett bedömningsorgan för överensstämmelse hos betrodda tjänster ska kunna uppfylla kraven i 33 § 1 mom. 3–4 punkten i autentiseringslagen ska bedömningsorganet uppfylla kraven i EN 319 403 eller motsvarande krav.

22.2 Kompetens

För att ett bedömningsorgan för överensstämmelse hos betrodda tjänster ska kunna uppfylla kraven i 33 § 1 mom. 2 punkten i autentiseringslagen ska bedömningsorganet ha tillräcklig kompetens för att utföra bedömningar enligt bedömningskriterierna

för tillhandahållare som uppräknas i punkt 20 och för betrodda tjänster som uppräknas i punkt 21.

8 kap. Certifiering av kvalificerade anordningar för skapande av elektroniska underskrifter och stämplar

23 Certifieringsorgan för anordning för skapande av elektronisk underskrift eller stämpel

För att kraven enligt 36 § i autentiseringslagen ska kunna uppfyllas, krävs tillräcklig kompetens och resurser i fråga om den anordning som certifieras för verifiering av kraven som ställs i[6] eIDAS-förordningen och kommissionens genomförandebeslut (EU) 2016/650 eller ett beslut som ersätter det.

Att certifieringsorganet uppfyller kraven kan visas genom en ackreditering eller någon annan oberoende utredning. Ett bevis på kompetens kan också vara att visa att organen omfattas av SOGIS-MRA-avtalet mellan vissa certifieringsorgan i EU-medlemsstater eller i medlemsstater i EES-området (Senior Officers Group for Information Systems, Mutual Recognition Agreement).

9 kap. Övergångsbestämmelser och underskrifter

24 Ikraftträdande och övergångsbestämmelser

24.1

Föreskriften träder i kraft x.4.2022

24.2

Kravet enligt punkt 6.2.1 i föreskriften ska uppfyllas senast X.10.2022.

Kraven enligt punkt 6.2.2 och underpunkt 12.1 4) i föreskriften ska uppfyllas senast x.10.2022.

24.3

Kravet på identifiering av parterna enligt punkt 8.1 i föreskriften ska uppfyllas

a) mellan identifieringstjänsterna senast x.10.2022,

b) mellan tjänster för identifieringsförmedling och nya förlitande parter senast x.10.2022 och

c) mellan tjänster för identifieringsförmedling och sådana förlitande parter med vilka man ingått avtal före x.10.2022 senast x.4.2023.

Kravet enligt punkt 8.2 i föreskriften på uppdatering av nycklar och certifikat måste införas senast x.4.2023.

[6] KOMMISSIONENS GENOMFÖRANDEBESLUT (EU) 2016/650 av den 25 april 2016 om fastställande av standarder för säkerhetsbedömning av kvalificerade anordningar för skapande av elektroniska underskrifter och stämplar enligt artiklarna 30.3 och 39.2 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden

24.4

Förfarandet enligt punkt 9.1.1 underpunkt a) i föreskriften kan användas när man har tillgång till en nyckel eller ett certifikat som uppfyller kraven i punkt 8.

Kraven enligt punkterna 9.1.1 b) och 9.1.2 i föreskriften måste uppfyllas senast inom övergångstiden enligt punkt 8.1.

Helsingfors (dag) (månad) 20(år)

Beslutsfattare

Föredragande