Motivering till föreskriften om elektroniska identifierings-tjänster och betrodda elektroniska tjänster (M72B/2022)

Innehållsförtecking

1 Föreskriftens bakgrund och rättsgrund

1.1 Föreskriftshistorik och orsaker till uppdateringen

Genom denna föreskrift upphävs föreskriften Kommunikationsverket 72 A/2018 och en ny, ändrad föreskrift ges.

Den tekniska utvecklingen, förändringarna i informationssäkerhetshoten, framstegen i ETSI-standarderna för betrodda tjänster, marknadens utveckling, företagens tillämpningserfarenheter samt Transport- och kommunikationsverkets erfarenheter av tillsynen kräver att kraven regelbundet utvärderas och uppdateras med tanke på aktualiteten.

Föreskriften om identifieringstjänster och betrodda tjänster gavs i sin nuvarande form ursprungligen den 1 november 2016 i samband med ikraftträdandet av EU:s eIDAS-förordning (EU) 910/2014 för att förenhetliga och samordna regleringen på nationell nivå och EU-nivå samt för att främja konkurrensförutsättningarna och förutsättningarna för teknisk interoperabilitet för det förtroendenät för stark autentisering som man lagstiftat om nationellt. Övergångstiden för den föreskrift som gavs år 2016 förlängdes genom en ändring den 14 maj 2018. Den ändrade föreskriften är alltså den tredje versionen av föreskriften i dess nuvarande form.

Föreskrift 72/2016 M ersatte Kommunikationsverkets tidigare föreskrift 7 B/2009 M *om skyldighet för leverantörer av identifieringstjänster och certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat att göra en anmälan om sin verk-*

samhet till Kommunikationsverket, och föreskrift 8 C/2010 M *om krav på tillförlitlighet och informationssäkerhet i verksamhet hos leverantörer av identifieringstjänster och certifikatutfärdare som tillhandahåller kvalificerade certifikat.* Föreskrift 7 innehöll bestämmelser om anmälan om inledande och ändring av verksamhet och om störningar. Föreskrift 8 innehöll bestämmelser om informationssäkerhetskrav. Bestämmelser om kvalitetscertifikat (termen i eIDAS-förordningen är kvalificerade certifikat) utfärdades första gången år 2003, och år 2009 kompletterades de med krav på tjänster för stark autentisering.

1.2 Rättsgrund för behörigheten att utfärda föreskrifter

Bemyndigande lagen om stark autentisering och betrodda elektroniska tjänster (617/2009 autentiseringslagen) 42 § [1]

1.3 Andra föreskrifter och författningar som hänför sig till ärendet

1.3.1 Elektronisk identifiering

Statsrådets förordning om förtroendenätet för leverantörer av tjänster för stark autentisering 169/2016, ändrad 1212/2018 (förordningen om förtroendenät) [2]

I förordningen finns bestämmelser om vissa administrativa rutiner och gränssnitt. Förordningen anknyter i synnerhet till kapitel 3 i föreskriften, som gäller identifieringstjänsternas interoperabilitet.

*EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG (**eIDAS**-förordningen)*[3]

Regler för betrodda elektroniska tjänster, ackrediterade bedömningsorgan för överensstämmelse och utnämnda verifieringsorgan för elektroniska underskrifter eller stämplar ges huvudsakligen genom eIDAS-förordningen. I föreskriften görs små och nödvändiga kompletteringar i regleringen.

Kraven i eIDAS-förordningen preciseras genom kommissionens genomförandeakter.

*EU-kommissionens genomförandeförordning (EU) 2015/1502 (**EU:s förordning om tillitsnivåer för elektronisk identifiering**) om fastställande av tekniska minimispecifikationer och förfaranden för tillitsnivåer för medel för elektronisk identifiering i enlighet med artikel 8.3 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden* [4]

I EU:s förordning om tillitsnivåer bestäms om kraven på tillitsnivåer för identifieringsmedel. Förordningen tillämpas på de identifieringsverktyg som anmäls till EU-kommissionen. Eftersom det i bestämmelserna om kraven på identifieringstjänsten i autentiseringslagen hänvisas till förordningen, tillämpas förordningen jämsides med lagen också på identifieringsverktyg som inte anmäls.

Motiveringspromemorian hänvisar till tillämpningsanvisningen för förordningen om tillitsnivåer, som har utarbetats som ett samarbete mellan experter från medlemsstaterna i ett samarbetsnätverk.

*EU-kommissionens genomförandeförordning (EU) 2015/1501 (**EU:s interoperabilitetsramverk**) 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.* [5]

EU:s interoperabilitetsförordning gäller i första hand den nationella noden som Myndigheten för digitalisering och befolkningsdata driver. Förordningens specifikationer om minimiattribut och optionella attribut har genom föreskriften också införts i den nationella identifieringen. Förordningen gäller också den nationella noden.

*EU-kommissionens genomförandebeslut (EU) 2015/1984 (**EU:s beslut om anmälningsförfarande**) om förutsättningar, format och förfaranden för anmälan enligt artikel 9.5 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden* [6]

I EU:s anmälningsförfarande anges de uppgifter som ska anmälas vid anmälan och det förfarande som ska användas. I praktiken anmäler Transport- och kommunikationsverket identifieringsmedlet (identifieringsverktyget) till kommissionen och de övriga medlemsstaterna tillsammans med leverantören av identifieringsverktyget.

*EU-kommissionens genomförandebeslut (EU) 2015/296 (**EU:s beslut om samarbetsnätverk**) om inrättande av förfaranden för samarbete mellan medlemsstaterna om elektronisk identifiering i enlighet med artikel 12.7 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden* [7]

I EU:s beslut om samarbetsnätverk bestäms om medlemsstaternas samarbete vid sakkunnighetsbedömningar som hänför sig till att anmäla identifieringssystem. Transport- och kommunikationsverket är medlem i samarbetsnätverket.

1.3.2 Anordning för skapande av elektroniska underskrifter och stämplar

*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 (Text av betydelse för EES)* [8]

I kommissionens genomförandebeslut bestäms om kraven på certifiering av anordningar för skapande av elektroniska underskrifter och elektroniska stämplar. Denna rättsakt anknyter till bestämmelse 23 i föreskriften.

1.3.3 Personuppgifter

*EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (**allmän dataskyddsförordning**)* [9]

Definition av personuppgifter i artikel 4

> *I denna förordning avses med 1)* personuppgifter*: varje upplysning som avser en identifierad eller identifierbar fysisk person (nedan kallad en* registrerad*), varvid en identifierbarfysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet,*

Bestämmelser om dataskyddet för personuppgifter finns i artikel 32 i den allmänna dataskyddsförordningen.

Artikel 32 Säkerhet i samband med behandlingen

1. Med beaktande av den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige och personuppgiftsbiträdet vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken, inbegripet, när det är lämpligt

a) pseudonymisering och kryptering av personuppgifter,
[…]

2. Vid bedömningen av lämplig säkerhetsnivå ska särskild hänsyn tas till de risker som behandling medför, i synnerhet från oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.

[…]

I dataskyddslagens (1050/2018) [10] 29 § 4 mom. behandlas behandlingen av personbeteckningar

En personbeteckning får inte onödigtvis antecknas i handlingar som skrivs ut eller upprättas på basis av ett personregister.

2 Föreskriftens syfte

2.1 Mål

De preciseringar av lagstiftningens krav som görs genom föreskriften gör regleringen förutsägbar för aktörerna och främjar jämlik konkurrens mellan dem. Genom föreskriften säkerställs tjänsternas informationssäkerhet och interoperabilitet.

Beredning av föreskriften tillsammans med sektorn bidrar till fastställande av genomförbara krav.

För kunder som använder autentisering och betrodda tjänster tryggar regleringen informationssäkerhet och integritetsskydd som standard. För att skapa förtroende för branschen förutsätts det att aktörerna bygger upp sina tjänster på rätt sätt från början.

2.2 Huvudsakliga ändringar och en bedömning av föreskriftens effekter

Ordalydelser i föreskriften har förtydligats. Föreskriftens utseende har ändrats i enlighet med Transport- och kommunikationsverkets enhetliga specifikation, och av denna orsak har man bland annat ersatt paragrafer och moment med avsnitt och stycken. För dessa används i denna motiveringspromemoria för tydlighetens skull termen bestämmelse för att skilja mellan dem och motiveringspromemorians avsnitt.

Motiveringspromemorian har utarbetats enligt Transport- och kommunikationsverkets nya praxis. Delar som tangerar de teman som förklaras har rensats bort från promemorian.

I de följande avsnitten beskrivs de huvudsakliga ändringarna och deras syften. Effekterna behandlas närmare i de bestämmelsespecifika motiveringarna.

Bestämmelse 4 Ledningssystem för informationssäkerhet

Ordalydelsen i bestämmelse 4.1 ändras så att den eller de valda **standarderna för ledning av informationssäkerheten måste följas, inte bara användas.** Detta innebär en lätt skärpning av kravet. Syftet är att lyfta fram betydelsen av engagemang hos ledningen för leverantören av en identifieringstjänst samt betydelsen av upprätthållande av ett system och en process för ledning av informationssäkerheten.

Certifiering är ett bra sätt att visa att ledningen av informationssäkerheten uppfyller kraven, men certifiering förutsätts fortfarande inte ens på tillitsnivån hög.

Förändringen av bestämmelse 4 kräver ingen övergångstid.

Bestämmelse 5 Krav på informationssäkerhet i identifieringssystem

Bestämmelse 5.1 identifieringssystemets skyddsförmåga är ny.

Föreskriften kompletteras med en precisering gällande kravnivån på identifieringssystemets skyddsförmåga. Genom bestämmelse 5.1 preciseras kravnivån för helheten av identifieringssystemets säkerhetsåtgärder och tekniska specifikationer. Tolkningsmässigt skulle kravet kunna härledas även från lagen, men man vill förtydliga saken i föreskriften.

Kravnivån för de säkerhetsåtgärder som förutsätts enligt avsnitt 2.4.6 i förordningen om tillitsnivåer för elektronisk identifiering, det vill säga tekniska kontroller, fastställs enligt förmågan till skydd mot angreppspotential enligt avsnitt 2.3.1 i förordningen om tillitsnivåer. För riskbedömningen fastställs inga närmare kriterier och ingen standard som ska följas. Bedömningen ska basera sig på goda kunskaper om branschen samt på uppföljning av hot, sårbarheter och den tekniska utvecklingen.

I fråga om säkerheten i datakommunikation, datasystem och användning enligt bestämmelserna 5.2–5.4 görs preciseringar som motsvarar den etablerade tillämpningen. Kravet på god krypteringspraxis och relationen till krypteringskraven i bestämmelse 7 förtydligas. Säkerhetskravet gällande lagring av information från 7 § har flyttats till bestämmelse 5.4.

Ändringarna i bestämmelse 5 kräver ingen övergångstid.

Ändring av rekommendationen i anknytning till bestämmelse 5: Rekommendation om tillförlitligheten hos klockslaget i identifieringssystem

Rekommendationen om tillförlitligheten hos klockslaget i identifieringssystem, vilken ingått i C-delen, avsnitt 1 i föreskriftens motiveringspromemoria 2016, flyttas i ändrad form till motiveringarna för bestämmelse 5.3 e). En tillförlitlig tid i systemet är en viktig delfaktor i klassificeringen och tidsstämplarna och även i övrigt ett centralt grundläggande krav. Man tar inte ställning till tidskällor och synkronisering.

Bestämmelse 6 Krav på informationssäkerhet i identifieringsmedel

Bestämmelse 6.1 Identifieringsmedlets egenskaper och skyddsförmåga är ny

Syftet är att förenhetliga och förbättra miniminivån för identifieringsmedlens säkerhet och utvärderingen av förändringar i dem. Identifieringsmedlen utvecklas hela tiden, och även informationssäkerhetshoten förändras.

Föreskriften kompletteras med ett krav på att göra en särskild riskbedömning för identifieringsmedlet, där man separat bedömer de hot som hänför sig

till autentiseringsfaktorerna och autentiseringsmekanismerna samt säkerhetsåtgärder som lämpar sig för dem. Av säkerhetsåtgärderna beaktar bestämmelsen uttryckligen krypteringslösningar och separation av autentiseringsfaktorer när de används på samma terminal (exempelvis mobilidentifieringsapp och fingeravtryck eller PIN-kod).

Syftet med det särskilda kravet på riskbedömning är att lyfta fram betydelsen av planering av säkerheten i identifieringsmedel. Bedömningarna ger också Transport- och kommunikationsverket motiverad information, utifrån vilken ämbetsverket vid behov kan uppmana till åtgärder i identifieringstjänster proaktivt, i stället för först när en eventuell störning har inträffat.

Föreskriften kompletteras med en precisering gällande kravnivån på identifieringsmedlets skyddsförmåga. Tolkningsmässigt skulle kravet kunna härledas även från lagen, men man vill förtydliga saken i föreskriften. (Jfr motsvarande ändring i bestämmelse 5.) Kraven på skyddsförmågan preciseras genom en hänvisning till förordningen om tillitsnivåer och genom att i föreskriften lista delfaktorer som ska beaktas i bedömningen av risker och hot.

Ämbetsverket bedömer att en sådan regleringsmodell är tillräckligt flexibel för att identifieringstjänsterna ska kunna utveckla sina identifieringsmedel. Modellen beaktar identifieringsmedlets säkerhetskontroller som helhet.

Ämbetsverket bedömer utifrån respons från berörda parter att det inte behövs någon övergångstid för identifieringsmedlets riskbedömningskrav.

Som alternativ till bestämmelse 6.1 har ämbetsverket bedömt regleringsmodeller där föreskriften skulle definiera specifika krav på autentiseringsfaktorer eller definiera krav på identifieringsmedlets skyddsförmåga genom en standardhänvisning. Specifik reglering för olika autentiseringsfaktorer skulle på grund av autentiseringsfaktorernas mångsidighet och utveckling inkludera många detaljer, som det enligt ämbetsverkets bedömning inte är möjligt eller ändamålsenligt att försöka täcka proaktivt på bestämmelsenivå. Inte heller hoten mot identifieringsmedlens säkerhet eller säkerhetsåtgärderna för att skydda sig mot hoten är helt specifika för typen av autentiseringsfaktor. Man kunde tänka sig indikatorer på skyddsförmågan eller andra preciseringar i föreskriften utifrån standarder, men man känner dock inte till någon sådan allmängiltig standard utifrån vilken man skulle kunna fastställa allmängiltiga, tvingande krav.

Bestämmelse 6.2 om särskilda säkerhetsåtgärder är ny.

Syftet är att på ett enhetligt sätt ta i bruk vissa goda säkerhetsrutiner i de identifieringsmedel där de är tekniskt genomförbara.

Föreskriften kompletteras med ett krav (6.2.1) på att identifierande information om identifieringsbegäran (***s.k. session binding***) måste visas för användaren. Utifrån denna information kan användaren koppla ihop en händelse i ärendehanteringen med identifieringsbegäran och undvika att bekräfta oberättigade identifieringsbegäranden.

Föreskriften kompletteras med ett krav (6.2.2) på att **namnet på den förlitande parten, det vill säga ärendehanteringstjänsten**, måste visas för användaren. Den information som visas verifieras av en identifieringsförmedlingstjänst, men man måste avtala specifikt för olika verksamhetsmodeller vem som ansvarar för att visa dem för användaren.

Bestämmelse 6.2.3 om samlad inloggning är ny.

Föreskriften kompletteras med en bestämmelse (6.2.3) om **säkerhetskrav för samlad inloggning**: en skyldighet att sköta hanteringen av längden på, överföring av och avslutande av sessioner som anknyter till enkel inloggning. Föreskriftens syfte är till denna del att på en allmän nivå definiera de principer som konstaterats i det tidigare samarbetet med berörda parter. Även vid enkel inloggning måste namnen på de förlitande parterna, det vill säga ärendehanteringstjänsterna, visas för användaren.

En övergångstid ges för uppfyllande av kraven i bestämmelserna 6.2.1 och 6.2.2.

Bestämmelse 7 Krypteringskrav för identifieringssystem och gränssnitt

Bestämmelse 7.1 Krypteringsmetoder för datakommunikation

Föreskriftens förteckning över krypteringsmetoder och algoritmer som godkänns för kryptering av datakommunikation (7.1.1) kompletteras på grund av den tekniska utvecklingen. Avsnittet preciseras så att det även kan tillämpas på kryptering av meddelanden enligt avsnitt 9. Krypteringsmodulen XTS, som inte lämpar sig tekniskt för kryptering av datakommunikation eller meddelanden utan för skivkryptering av information som lagras, lämnas bort ur avsnittet. Transport- och kommunikationsverket anser fortfarande utifrån sin tillsynserfarenhet att minimikraven måste definieras entydigt.

Föreskriften kompletteras med en möjlighet (7.1.2) att utöver de listade algoritmerna och förfarandena använda algoritmer och värden från de listor som upprätthålls av Transport- och kommunikationsverkets NCSA:s myndighet för godkännande av krypteringsprodukter (CAA) eller SOGIS MRA. Tanken är att göra kraven mer flexibla ifall föreskriften inte skulle hinna ändras i takt med den tekniska utvecklingen. Ämbetsverket anser att föreskriften inte kan ersättas endast med en hänvisning till dessa källor, eftersom de upprätthålls för ett annat syfte och till vissa delar är onödigt strikta i förhållande till kraven på identifiering med tillitsnivån hög.

Bestämmelse 7.2 Krypteringsprotokoll för datakommunikationen

Möjligheten att i undantagsfall använda versionen TLS 1.1 tas bort från föreskriften. Den miniminivå som krävs är därmed utan undantag TLS 1.2.

Utifrån erfarenheterna av förbudet mot användning av versionen TLS 1.0, vilket infördes genom föreskriften år 2016, är det bra med tanke på lika konkurrens att alla identifieringstjänster är skyldiga att göra ändringen samtidigt. Utifrån respons från berörda parter bedömer ämbetsverket att ingen övergångstid för kravet behövs. Man har i stor utsträckning övergått till TLS 1.2 redan i samband med den förra övergången, och beståndet av terminaler stöder denna version.

Ändringarna i bestämmelse 7 kräver ingen övergångstid.

Rekommendation om tillämpning av bestämmelse 7.1 på tillitsnivån hög

Rekommendationen från motiveringspromemorian för föreskriften från 2016 om krypteringsmetoder och algoritmer med tillitsnivån hög bibehålls som rekommendation och uppdateras.

Rekommendationen motsvarar definitionen för säkerhetsklass IV i bedömningsanvisningarna från myndigheten för godkännande av krypteringsprodukter (CAA). Ämbetsverket bedömer att det inte skulle uppstå interoperabilitetsproblem även om

värdena i rekommendationen om tillitsnivån hög gjordes obligatoriska, eftersom det är tekniskt möjligt att välja algoritmer specifikt för en viss transaktion i identifieringsförmedling. Ämbetsverket anser dock att konsekvenserna för förlitande parter som använder identifiering med tillitsnivån hög är svårare att bedöma.

Bestämmelse 8 Verifiering av parterna i datakommunikationen

Preciseringen av kraven i bestämmelse 8 och utvidgningen av dem till förlitande parter är den största förändringen i bestämmelsen och den förändring som har de mest omfattande effekterna.

Kravet på verifiering av parterna i datakommunikation enligt 8.2 § i den gällande föreskriften preciseras genom att man skiljer mellan grundande och upprätthållande av en förtroenderelation. I bestämmelse 8 i föreskriften preciseras kraven på datakommunikationsförbindelserna mellan identifieringstjänster samt mellan identifieringstjänster och förlitande parter, det vill säga ärendehanteringstjänster.

Genom bestämmelse 8.1 anges kraven gällande identifiering av parterna i en datakommunikationsförbindelse vid grundandet av en förtroenderelation.

I bestämmelse 8.2 preciseras de alternativa förfarandena för uppdatering av certifikat och nycklar vid upprätthållandet av en förtroenderelation.

Syftet är att förtydliga kraven och säkerställa enhetlig användning av säkra metoder oberoende av identifieringstjänst. Kraven har i praktiken varit otydliga och orsakat många tolkningsfrågor och säkerhetsmässigt varierande förfaranden i synnerhet i verifieringen av förlitande parter, det vill säga ärendehanteringstjänster.

Syftet med kraven är att säkerställa att identifieringstransaktioner endast förmedlas till tillförlitligt verifierade organisationer. Autentisering av den förlitande parten är ett centralt sätt att skydda användaren av ett identifieringsverktyg från att bekräfta bedrägliga identifieringsbegäranden. Ett ytterligare syfte är också att säkerställa integriteten och sekretessen i datakommunikation och meddelanden.

Genom kravet uppnår man bättre säkerhet än med de grundläggande rutinerna för protokollen, i vilka man litar på vilka certifikat som helst som är allmänt betrodda på internet, oberoende av deras tillförlitlighet. Uppfyllande av kraven förutsätter fastställande av processerna för leverans av nycklar och certifikat samt fastställande av olika inställningar i serverprogramvaran i såväl identifieringstjänster som ärendehanteringstjänster. Därför har effekterna och den tekniska genomförbarheten utvärderats och övervägts mycket noggrant och de tekniska möjligheterna att uppfylla kraven har utvärderats för OpenID Connect- och SAML-protokollens del i beredningen i samarbete med berörda parter. Ämbetsverkets bedömning är att ändringarna är tekniskt genomförbara och nödvändiga för den kontinuerliga utvecklingen av säkerheten i stark autentisering. Man måste dock reservera en övergångstid för kravet, särskilt i förhållande till ärendehanteringstjänster, och genomförandet av ändringarna förutsätter samarbete inom rådgivningen och informationen.

Ämbetsverket bedömer att ändringarna i bestämmelse 8 kräver en övergångstid, eftersom de har en väsentlig inverkan på förlitande parter, det vill säga ärendehanteringstjänster som använder identifieringstjänster.

Bestämmelse 9 Identifieringsmeddelandenas integritet och sekretess

Det kategoriska krypteringskravet på meddelandenivå för identifieringsmeddelanden ändras så att man för säkerställande av identifieringsmeddelandenas sekretess och integritet fastställer **ett alternativt förfarande parallellt med kryptering av**

meddelandena genom särskilt säkerställande av datakommunikationsförbindelsers sekretess och integritet. Det alternativa förfarandet är möjligt om meddelandena inte förmedlas via användarens webbläsare eller terminal.

Syftet med ändringen är att bättre än i den gällande föreskriften beakta egenskaperna hos olika protokoll och standarder samt regleringens syfte. Ändringen möjliggör exempelvis den nuvarande mobilcertifikatlösningen som använder ETSI MSS-standarden och ökar flexibiliteten vid användning av OpenID Connect-protokollet. Vid användning av SAML-protokoll används i allmänhet användarens webbläsare, så kryptering av meddelanden måste alltid förverkligas i dem.

Syftet med kravet är att personuppgifter inte ska röjas utan tillstånd i webbläsaren i användarens terminal eller i servrar. Tillsammans med kraven enligt bestämmelse 8 skyddar krypteringen och undertecknandet av identifieringsmeddelanden även identifieringstransaktionen från förfalskning och omspelning. Genom förfarandet bidrar man också till att säkerställa att bekräftelsen av användarautentisering och personuppgifterna vid autentiseringen endast förmedlas till rätt förlitande part, det vill säga ärendehanteringstjänsten. Skyddskravet gäller både kontakter mellan identifieringstjänster och kontakter mellan identifieringstjänster och förlitande parter.

I fråga om det tekniska förverkligandet av kryptering och underskrifter hänvisar man till bestämmelse 7, som har ändrats så att den tekniskt lämpar sig även för kryptering på meddelandenivå.

Ändringarna i bestämmelse 9 är knutna till kraven i avsnitt 8, och övergångstiderna motsvarar därför övergångstiderna enligt avsnitt 8.

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

Bestämmelsen kompletteras med krav på anmälningsförfarandet (11.3). Bestämmelsen beskriver den etablerade praxisen. Syftet är att förtydliga anmälningsskyldigheten för alla identifieringstjänster.

I övrigt förtydligar bestämmelsen anmälningströskeln för betydande hot eller störningar och vilka uppgifter som ska anmälas. Ändringarna motsvarar tillsynspraxisen och ändrar inte kravnivån.

Ämbetsverket ser det inte som ändamålsenligt eller nödvändigt att ställa upp en ny anmälningströskel för funktionsstörningar i föreskriften. Bedömningen ändras inte jämfört med bedömningen från 2016 i detta avseende. Det bör också noteras att autentiseringslagen inte innehåller uttryckliga krav på identifieringstjänsternas driftssäkerhet, säkerställande eller beredskap, och att befogenheterna därför inte fastställs enligt dessa.

I svaren på ämbetsverkets enkät om behoven av ändringar i föreskriften framkom en oro över att alla inte anmäler störningar till ämbetsverket med tillräckligt låg tröskel och att alla identifieringstjänster inte informerar varandra om störningar. Ämbetsverket bedömer att dessa observationer främst måste besvaras genom tillsyn och genom att ytterligare effektivisera den inbördes informationen inom förtroendenätet. Aktörernas skyldighet till inbördes information hör inte till behörigheten att utfärda föreskrifter, utan är en tillsynsfråga.

Ändringarna i bestämmelse 11 kräver ingen övergångstid.

Bestämmelse 12

Bestämmelse 12.1 Obligatoriska uppgifter som förmedlas i förtroendenätet (attribut)

I bestämmelse 12.1.4) **läggs information om den förlitande parten vilken verifierats av tjänsten för identifieringsförmedling, det vill säga ärendehanteringstjänstens namn, till i de obligatoriska uppgifterna**. Syftet är att möjliggöra den praxis för förbättrad säkerhet som anges i bestämmelse 6.2. att visa användaren namnet på den ärendehanteringstjänst som användaren är på väg att identifiera sig i.

Bestämmelse 12.3 Pseudonymisering av identifiering är ny

Dess syfte är att klargöra attributkraven i gränssnitt mellan tillhandahållarna av identifieringsverktyg och identifieringsförmedling inom förtroendenätet i fall där ärendehanteringstjänsten endast får en pseudonymiserad bekräftelse av autentiseringen av användaren.

I autentiseringslagens 8 § 2 mom. sägs att *Bestämmelserna i 1 mom. hindrar inte att specifika tjänster tillhandahålls så att leverantören av identifieringstjänster meddelar den tjänsteleverantör som använder en identifieringstjänst den pseudonym som innehavaren av identifieringsverktyget använder eller endast ett begränsat antal personuppgifter.*

Varken i lagen eller i denna föreskrift regleras vilka personuppgifter som ska skickas till den förlitande parten eller verifieras genom stark autentisering. I föreskriften fastställs attribut som behandlas inom förtroendenätet vid autentisering. Till den förlitande parten förmedlas vanligen exempelvis namn och personbeteckning, men på det sätt som beskrivs i lagen kan även exempelvis en pseudonym eller en begränsad mängd personuppgifter förmedlas till den förlitande parten. Även i detta fall ska användaren autentiseras genom stark autentisering och identifieringstransaktionens uppgifter ska sparas enligt lagens 24 §.

I föreskriften används termen pseudonym, eftersom det i fråga om regleringen av personuppgifter enligt ämbetsverkets bedömning är fråga om pseudonymiserade personuppgifter. Även om informationen skulle vara anonym ur den förlitande partens perspektiv på så sätt att den förlitande parten inte nödvändigtvis kan koppla den till en viss person, kan informationen kopplas till personen utifrån de uppgifter som identifieringstjänsterna sparat exempelvis om en störning behöver utredas.
Ändringarna i bestämmelse 12 kräver i huvudsak ingen övergångstid. Hanteringen av namnet på en förlitande part enligt 12.1 anknyter till genomförandet av bestämmelse 6.2.2 i föreskriften, och övergångstiden är därför densamma.

Sådan pseudonymisering som avses i 12.3 finns enligt ämbetsverkets uppfattning inte att tillgå, och eventuell utveckling av en sådan tjänst ska enligt ämbetsverkets bedömning basera sig på föreskriftens grunder utan övergångstid.

Bestämmelse 14 Protokoll som används vid dataöverföring samt övriga krav

Bestämmelse 14.1 om protokollet som ska användas vid informationsöverföring har preciserats genom att OpenID Connect och SAML fastställts som standarder, och ett gränssnitt till en identifieringstjänst enligt någondera måste åtminstone erbjudas för sammankoppling av en inledande identifiering mellan leverantörer av identifieringsverktyg enligt autentiseringslagens 17 § eller för identifieringsförmedling i enlighet med autentiseringslagens 12 a § mellan en leverantör av ett identifieringsverktyg och en identifieringsförmedlingstjänst.

Syftet med bestämmelsen är att begränsa antalet sådana standarder för gränssnitt som identifieringstjänsten måste ha beredskap att upprätthålla för att kunna förmedla eller ta emot identifieringsuppgifter vid inledande identifiering eller identifieringsförmedling.

Möjliggörande innebär i bestämmelsen att kravet tolkas med tanke på mottagarens rätt till den inledande identifieringen eller den identifieringstransaktion som förmedlas till den förlitande parten. En identifieringstjänst kan uppfylla sina skyldigheter genom att erbjuda en funktion via en annan identifieringstjänst inom förtroendenätet, så länge de angivna och fastställda kraven fortfarande uppfylls.

Ändringarna i bestämmelse 14 kräver ingen övergångstid.

Bestämmelse 15 Bedömningskriterier för överensstämmelse

I bestämmelse 15.1 har interoperabilitet inom förtroendenätet lagts till som en funktion som ska utvärderas. Interoperabilitet ingår enligt 29 § i autentiseringslagen i bedömningen av överensstämmelse; kraven preciseras i kapitel 3 i föreskriften och de har beaktats i Transport- och kommunikationsverkets bedömningsanvisningar.

Bestämmelsen har kompletterats med en hänvisning till Transport- och kommunikationsverkets bedömningsanvisning som en möjlig uppsättning bedömningskriterier. Ordalydelser har förtydligats.

Ändringarna i bestämmelse 15 kräver ingen övergångstid.

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

Bestämmelsen anknyter till skyldigheten att anmäla tjänster för stark autentisering vid inledande och ändring av verksamheten enligt autentiseringslagens 10 §. Bestämmelsens syfte är också att förtydliga de uppgifter som inte berör den oberoende och behöriga regelbundna bedömningen av överensstämmelse enligt bestämmelse 15. Bestämmelsen har kompletterats och justerats i enlighet med rutinerna för tillsyn och rådgivning.

Ändringarna i bestämmelse 16 kräver ingen övergångstid.

Bestämmelse 21 Kriterier för bedömning av kvalificerade betrodda tjänster

I bestämmelsen fastställs bedömningskriterierna för överensstämmelse i kvalificerade betrodda tjänster genom hänvisning till de färdiga ETSI-standarderna. Bestämmelsen kompletteras med hänvisningar som blivit klara efter den förra föreskriften till standarden för kvalificerad elektronisk underskrift eller stämpel och kvalificerad valideringstjänst samt standarderna för registrerad distributionstjänst.

Syftet är att precisera bedömningskriterierna till de delar som kommissionen inte har använt sin behörighet att utfärda genomförandeakter. Om kommissionen utfärdar genomförandeakter upphävs kraven i föreskriften.

Ändringarna i bestämmelse 21 kräver ingen övergångstid.

2.3 Andra alternativ för verkställandet

De alternativ som övervägts vid beredningen av bestämmelserna beskrivs i de bestämmelsespecifika motiveringarna.

Vid beredningen av föreskriften och i konsekvensbedömningen har man utrett om behoven av styrning på ett effektivt och jämlikt sätt kan lösas genom anvisningar och rekommendationer eller genom samreglering i stället för genom en föreskrift. Bedömningarna ingår i de bestämmelsespecifika motiveringarna.

3 Beredning av föreskriften

3.1 Beredning tillsammans med berörda parter

Traficom sände den 4 augusti 2020 en omfattande förhandsenkät till sektorn gällande eventuella ändringsbehov i föreskriften (dnr TRAFICOM/245890/03.04.05.00/2020). Enkäten innehöll 74 frågor. Åtta svar inkom. Svaren har beaktats under beredningen av föreskriften och i den beredningspromemoria som publicerats.

Gällande beredningen av ändringen av föreskriften publicerades den 7 december 2020 en arbetsplan, av vilken framgår vilka frågor som behandlas, grupperingen av temana i verkstäder för olika berörda parter och hela projektets tidtabell. Den 26 mars 2021 publicerades en uppdaterad version av arbetsplanen, som berättade om de riktlinjer som utarbetats under beredningen.

För berörda parter ordnades i enlighet med arbetsplanen sju verkstäder och två extra verkstäder under tiden 10.12.2020–16.6.2021. Ämbetsverket har också på begäran träffat några aktörer enskilt. För varje föreskriftsändringstema publicerades före verkstaden en beredningspromemoria, där man sammanställt den gällande bestämmelsen och dess motiveringar samt tidigare konsekvensbedömningar, källor, enkätsvar och förslag till ändringar i bestämmelsen samt synpunkter på ändringarnas konsekvenser för informationssäkerheten och genomförbarheten samt deras ekonomiska konsekvenser. Responsen från verkstäderna för berörda parter och ämbetsverkets slutsatser om den har sammanställts och publicerats i presentationerna om verkstäderna.

Information om beredningen av föreskriften har sänts ut via e-post till en begränsad samarbetsgrupp för förtroendenätet för identifieringstjänster, eIDAS-gruppen för identifieringstjänster och betrodda tjänster som är öppen för alla samt den tekniska eIDAS-gruppen för identifieringstjänster och betrodda tjänster som är öppen för alla. I distributionen ingår ett brett urval av leverantörer av autentisering och betrodda tjänster, IKT-aktörer, myndigheter samt en del tillhandahållare av elektroniska ärendehanteringstjänster, som använder autentisering och betrodda tjänster. Allt beredningsmaterial har publicerats på ämbetsverkets webbplats.

Den x.x.2021 skickades begäran om utlåtanden ut med samma distribution och publicerades samtidigt i statsförvaltningens utlåtandetjänst.

Föreskriften gäller informationssamhällets tjänster och har anmälts enligt EU:s så kallade transparensdirektiv (EU) 2015/1535[1] x.x.2021.

3.2 Remissrespons

Ett kort sammandrag av utlåtanden (från berörda parter) kan inkluderas i promemorian, ett längre bifogas som en separat bilaga.

[1] EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV (EU) 2015/1535 av den 9 september 2015 om ett informationsförfarande beträffande tekniska föreskrifter och beträffande föreskrifter för informationssamhällets tjänster

En beskrivning ges av hur och varför man har beaktat de utlåtanden och kommentarer som kommit in. Såväl synpunkter till stöd för förändringen som kritiska synpunkter inkluderas. Ett sammandrag av kommentarerna bifogas eventuellt som bilaga.
Kom också ihåg anmälningsresponsen.

4 Detaljmotivering

Kapitel 1 i föreskriften Allmänna bestämmelser

4.1 Bestämmelse 1 Tillämpningsområde

Föreskriften tillämpas på samma sätt som de tidigare föreskrifterna på tillhandahållande av identifieringsverktyg för stark autentisering. Identifieringsverktyg för stark autentisering är verktyg som har anmälts till Transport- och kommunikationsverket och som uppfyller de föreskrivna kraven.

Föreskriften tillämpas också på sådana *tjänster för identifieringsförmedling* som har anmälts till Transport- och kommunikationsverket. Med identifieringsförmedlingstjänster avses förmedling av identifieringstransaktioner till förlitande parter, det vill säga ärendehanteringstjänster.

Samma juridiska person kan vara både leverantör av identifieringsverktyg och tjänst för identifieringsförmedling.

Föreskriften tillämpas också på kvalificerade betrodda tjänster enligt eIDAS-förordningen, och med dem avses betrodda tjänster som uppfyller kraven i den förordningen.

Föreskriften tillämpas inte på betrodda tjänster för vilka godkännande inte har ansökts. Transport- och kommunikationsverkets uppgift är enligt 42 a § i autentiseringslagen och artikel 17 i eIDAS-förordningen att under vissa förutsättningar övervaka okvalificerade betrodda tjänster, om ämbetsverket får meddelande om att okvalificerade tillhandahållare av betrodda tjänster eller de betrodda tjänster som de tillhandahåller enligt uppgift inte uppfyller kraven i förordningen. Ämbetsverket bedömer att verksamheten i en tillsynssituation närmast kan jämföras med de standarder som utarbetats som stöd för verkställandet av eIDAS-förordningen.

Exakta hänvisningar till EU-lagstiftningen behövs som förtydligande information i föreskriften bland annat därför att EU-rättens primära ställning framgår tydligt.

Bestämmelsen ändras inte i föreskriften år 2022, med undantag för uppdatering av ämbetsverkets namn.

4.2 Bestämmelse 2 Syfte

I denna bestämmelse beskrivs kortfattat de huvudsakliga målen med föreskriften. Bestämmelsen är informativ och fastställer inte mer noggrant tillämpningsområdet för kraven.

Bestämmelsen ändras inte i föreskriften år 2022.

4.2.1 Identifieringstjänster

Enligt autentiseringslagen förutsätts det även på nationell nivå att minst kraven på tillitsnivån väsentlig enligt bilagan till EU:s förordning om tillitsnivåer uppfylls när identifieringstjänster tillhandahålls. Målet är att det ska vara enkelt för aktörerna att ansöka om att få sitt system anmält till EU i vilket skede som helst när de uppfyller

de nationella kraven. Leverantörerna av identifieringstjänster behöver inte ta fram särskilda identifieringslösningar för gränsöverskridande situationer och nationell identifiering.

Beredningen av föreskriften har också utgått från samma mål. Avsikten i beredningen har varit att utnyttja så många internationella standarder, kravspecifikationer och anmälningssätt som möjligt. Syftet med lösningen är att göra det lättare att tillhandahålla gränsöverskridande tjänster och att undvika nationellt anpassade krav.

4.2.2 Betrodda tjänster

Det allmänna målet för regleringen av betrodda tjänster är utveckling av informationssamhället och ökat förtroende för elektronisk ärendehantering. Reglerna för betrodda tjänster hjälper leverantörerna och användarna av elektroniska tjänster att känna igen de tjänster där det är möjligt att implementera olika funktioner för elektroniska ärendehanteringstjänster med högsta möjliga informationssäkerhet.

Målet med föreskriften är att förtydliga de krav som ställs på kvalificerade betrodda tjänster i eIDAS-förordningen genom hänvisningar till de internationella standarder som har tagits upp i EU:s beredningsarbete och som åtminstone hittills inte har hänvisats till genom kommissionens genomförandeakter, trots att kommissionen har befogenheter för det enligt eIDAS-förordningen.

Hänvisningarna till standarderna stöder också de faktorer som åtminstone ska beaktas som kompetenskrav på eventuella bedömningsorgan för överensstämmelse, när organen ackrediteras.

4.2.3 Bedömningsverksamhet

Målet med föreskriften är att för aktörerna och bedömningsorganen för överensstämmelse förtydliga kraven på betrodda tjänster till den del kommissionen inte har utövat sin lagstiftningskompetens gällande betrodda tjänster och utfärdat genomförandeakter med hänvisningar till nödvändiga standarder.

När det gäller bedömning av identifieringstjänster är målet för föreskriften att för aktörerna förtydliga på vilken grund de kvalitetsrevisorer som aktörerna använder är behöriga att göra kvalitetsrevisioner i identifieringssystem. De kvalitetsrevisorer som anlitas av leverantörerna av identifieringstjänster behöver inte särskilt ansöka om godkännande, om kvalitetsrevisorn inte är ett ackrediterad bedömningsorgan för överensstämmelse. Målet för föreskriften är att aktörerna ska kunna utnyttja så många som möjligt av de kvalitetsrevisioner som de gör eller har låtit göra redan tidigare.

4.3 Bestämmelse 3 Definitioner

4.3.1 Bestämmelse 3.1 Definitioner i föreskriften

Definitionen av gränssnitt omfattar både en närmare specificering av faktorer enligt det protokoll som används vid dataöverföring och optionella faktorer. Den omfattar också praktisk implementering, det vill säga urvalet och formen för de informationsinnehåll som ska överföras.

En definition av *certifikat* läggs till i föreskriften. Definitionen i autentiseringslagen är kopplad till certifikat för stark autentisering eller certifikat som tillhandahålls som betrodda tjänster.

I föreskriften används termen certifikat i bestämmelse 8 i dess mera allmänna betydelse. För certifikat finns allmänt taget olika förfaranden för beviljande, och deras tillförlitlighetsnivå varierar därför mycket. Innehavaren av ett certifikat identifieras inte alltid, utan informationen av innehavaren kan ha uppgetts av innehavaren själv. Med autentiseringsuppgifter avses innehavarens offentliga nyckel som är en del av en offentlig nyckel, det vill säga ett PKI-förfarande. En privat nyckel som anknyter till en offentlig nyckel ska enbart innehas av den innehavare som certifikatet anger.

Jämför autentiseringslagens 2 § 1 mom. 8 punkten *certifikat* [avser] *ett intyg i elektronisk form som verifierar identiteten eller verifierar identiteten och kopplar ihop autentiseringsuppgifter för en betrodd tjänst med en användare av tjänsten och som kan användas vid stark autentisering och betrodda tjänster*

Den nationella noden. Definitionen av *eIDAS-gränssnitt* tas bort ur föreskriften som obehövlig. Definitionen har gällt gränssnitt mellan nationella noder, och erfarenheterna av tillämpningen har visat att detta gränssnitt mellan noderna för Myndigheten för digitalisering och befolkningsdata och andra medlemsstaters offentliga förvaltning inte påverkar de nationella gränssnitten så att det skulle finnas ett behov av en definition. I stället används termen *nationell nod*. Enligt autentiseringslagens 30 § avses med en nationell nod *ett nationellt gränssnitt som ingår i EU:s interoperabilitetsramverk för elektronisk identifiering*. I kommissionens genomförandeförordning (EU) 2015/1501 [5] artikel 2 avses med *nod en förbindelsepunkt som utgör en del av den interoperativa arkitekturen för elektronisk identifiering och som medverkar vid gränsöverskridande autentisering av personer och som har förmågan att känna igen och behandla eller vidarebefordra överföringar till andra noder genom att bringa den nationella elektroniska identifieringsinfrastrukturen i en medlemsstat i kontakt med nationella elektroniska identifieringsinfrastrukturer i andra medlemsstater.*

Termen den nationella noden används i bestämmelserna 10, 13 och 17.

4.3.2 Bestämmelse 3.2 Definitioner i autentiseringslagen och eIDAS-förordningen

Hänvisningen till författningarna av den författningshierarkiskt högsta graden kompletteras.

Följande definitioner i 2 § i autentiseringslagen och i artikel 3 i eIDAS-förordningen är de viktigaste för föreskriften:

Autentiseringslagen [1] 2 §

*1) **stark autentisering** identifiering av en person, av en juridisk person eller av en fysisk person som företräder en juridisk person och verifiering av identifikatorns autenticitet och riktighet genom tillämpning av en elektronisk metod som motsvarar tillitsnivån väsentlig enligt artikel 8.2 b i EU:s förordning om elektronisk identifiering och betrodda tjänster eller tillitsnivån hög enligt artikel 8.2 c i den förordningen,*

*2) **identifieringsverktyg** ett sådant **medel för elektronisk identifiering** som avses i artikel 3.2 i EU:s förordning om elektronisk identifiering och betrodda tjänster,*

*3) **leverantör av identifieringstjänster** en leverantör av tjänster för identifieringsförmedling eller en leverantör av identifieringsverktyg,*

*4) **leverantör av identifieringsverktyg** en tjänsteleverantör som tillhandahåller eller ger ut identifieringsverktyg för stark autentisering till allmänheten samt tillhandahåller sitt identifieringsverktyg till leverantörer av tjänster för identifieringsförmedling för förmedling i förtroendenätet,*

*5) **leverantör av tjänster för identifieringsförmedling** en tjänsteleverantör som förmedlar identifieringstransaktioner baserade på stark autentisering till en part som förlitar sig på en elektronisk identifiering,*

*10) **förtroendenätet** de leverantörer av identifieringstjänster som har gjort en anmälan till Transport- och kommunikationsverket,*

*11) **bedömningsorgan för överensstämmelse** ett av Transport- och kommunikationsverket godkänt organ enligt artikel 2.13 i Europaparlamentets och rådets förordning (EG) nr 765/2008 om krav för ackreditering och marknadskontroll i samband med saluföring av produkter och upphävande av förordning (EEG) nr 339/93, som är ackrediterat i enlighet med den förordningen.*

eIDAS-förordningen [3] artikel 3

*2) **medel för elektronisk identifiering** en materiell och/eller immateriell enhet som innehåller personidentifieringsuppgifter och som används för autentisering för nättjänster,*

*4) **system för elektronisk identifiering** ett system för elektronisk identifiering genom vilket medel för elektronisk identifiering utfärdas till en fysisk eller juridisk person eller en fysisk person som företräder en juridisk person,*

*6) **förlitande part** en fysisk eller juridisk person som förlitar sig på en elektronisk identifiering eller betrodda tjänster,*

*16) **betrodd tjänst** en elektronisk tjänst som vanligen tillhandahålls mot ekonomisk ersättning och som består av*

a) skapande, kontroll och validering av elektroniska underskrifter, elektroniska stämplar eller elektroniska tidsstämplingar, elektroniska tjänster för rekommenderade leveranser och certifikat med anknytning till dessa tjänster, eller

b) skapande, kontroll och validering av certifikat för autentisering av webbplatser, eller

c) bevarande av elektroniska underskrifter, stämplar eller certifikat med anknytning till dessa tjänster,

*17) **kvalificerad betrodd tjänst** en betrodd tjänst som uppfyller tillämpliga krav i denna förordning,*

*20) **kvalificerad tillhandahållare av betrodda tjänster** en tillhandahållare av betrodda tjänster som tillhandahåller en eller flera kvalificerade betrodda tjänster och som beviljats status som kvalificerad av tillsynsorganet,*

Bilagan till EU Kommissionens förordning om tillitsnivåer för elektronisk identifiering [4] avsnitt 1.

*2) med **autentiseringsfaktor** avses en faktor som bekräftas vara bunden till en person och som tillhör någon av följande kategorier:*

a) med ”innehavsbaserad autentiseringsfaktor” avses en autentiseringsfaktor som personen måste kunna visa att den innehar,

b) med ”kunskapsbaserad autentiseringsfaktor” avses en autentiseringsfaktor som personen måste kunna visa att den har kunskap om.

c) med ”egenskapsbaserad autentiseringsfaktor” avses en autentiseringsfaktor som utgår från en kroppslig egenskap hos en fysisk person, som denne måste kunna visa att den har,

*3) med **dynamisk autentisering** avses en elektronisk process som använder kryptering eller andra metoder för att på begäran skapa ett elektroniskt bevis för att en person har kontroll över eller är i besittning av identifieringsinformationen, och som ändras vid varje autentisering mellan personen och det system som kontrollerar personens identitet,*

*4) med **ledningssystem för informationssäkerhet** avses en uppsättning processer och förfaranden avsedda att hantera godtagbara risknivåer förknippade med informationssäkerhet.*

Kapitel 2 i föreskriften Krav på informationssäkerhet i identifieringstjänst

4.4 Bestämmelse 4 Ledningssystem för informationssäkerhet hos leverantörer av identifieringstjänster

4.4.1 4.1 Standard för ledning avseende informationssäkerheten

Bestämmelsen innehåller allmänna bestämmelser om vilka faktorer som ska beaktas vid ledning avseende informationssäkerheten i identifieringssystem. Med tillhandahållande av en identifieringstjänst avses hela identifieringssystemet som omfattar helheten av hela identifieringstjänsten.

I 8 § 1 mom. 5 punkten i autentiseringslagen finns bestämmelser om ledning avseende informationssäkerhet och hänvisningar till bland annat avsnitt 2.4.3 i EU:s förordning om tillitsnivåer för elektronisk identifiering. Avsnitt 2.4.3 i bilaga 1 till EU:s förordning om tillitsnivåer för elektronisk identifiering förutsätter *att det finns ett effektivt ledningssystem för informationssäkerhet för hantering och kontroll av informationssäkerhetsrisker.*

Genom bestämmelse 4.1 preciseras kraven i autentiseringslagen och EU:s förordning om tillitsnivåer för elektronisk identifiering. Åtminstone standard ISO/IEC 27001 [11] är en allmänt känd och giltig standard för ledning avseende informationssäkerhet. En annan standard eller en kombination av standarder kan också användas under förutsättning att standarden verkligen gäller ledning avseende informationssäkerhet. Standarden kan vara en internationell standard, som ISO, men också en nationell standard, som KATAKRI [12].

Ordalydelsen i bestämmelsen ändras så att den eller de valda standarderna för ledning av informationssäkerheten måste följas, inte bara användas. Detta innebär en lätt skärpning av kravet. Syftet är att lyfta fram betydelsen av engagemang hos ledningen för leverantören av en identifieringstjänst samt betydelsen av upprätthållande av ett system och en process för ledning av informationssäkerheten.

Inte heller på hög tillitsnivå definieras certifiering som obligatorisk, men förverkligandet av och effektiviteten i ledningen av informationssäkerheten bedöms genomgående strikt enligt en hög kravnivå. Ledningen avseende informationssäkerheten ska utan undantag vara heltäckande, konsekvent och aktiv.

4.4.2 Bestämmelse 4.2 Omfattning av ledningen av informationssäkerheten

I bestämmelse 4.2 uppräknas de delområden av verksamheten som ledningen av informationssäkerheten ska omfatta. I preciseringen av kraven har man använt grupperingen på högre nivå av kraven i ISO/IEC 27001.

Bestämmelsen har inte ändrats. Kraven motsvarar ganska långt 8 § 2 mom. om ledning av informationssäkerhet i den föreskrift som var i kraft redan före 2016.

Ledningen av informationssäkerhet ska vara heltäckande, konsekvent, organiserad och systematisk samt följas upp kontinuerligt. I bestämmelsen preciseras vilka faktorer som åtminstone måste beaktas i ledningssystemet för informationssäkerhet.

Även underleverantörernas ledning av informationssäkerheten måste uppfylla kraven. De kan ställas i relation till hur kritisk den funktion som underleverantören producerar är i identifieringssystemet.

Gällande bedömningen av överensstämmelsen i ledningen av informationssäkerhet, se avsnitt 15 i föreskriften och dess motiveringar.

Härnäst beskrivs styckenas innehåll och deras relation till avsnitten i standarden ISO/IEC 27001 [11] bedöms. Kompletteringar har gjorts i tabellen jämfört med motiveringarna från 2016.

Avsnitt 4.2 i föreskriften och tillämpning	**ISO/IEC 27001**
1) *identifieringstjänsteleverantörens omvärld som en helhet* - Ledningssystemet för informationssäkerhet omfattar de väsentliga interna och externa tekniska, juridiska och administrativa krav och behov som påverkar identifieringssystemet. - I en identifieringstjänst ska man bland annat följa aktuella lagar och förordningar, såsom autentiseringslagen, föreskrift 72 och den allmänna dataskyddsförordningen.	4 organisationens omvärld
2) *styrning, organisering och administration av ledningen avseende informationssäkerheten* - Ledningssystemet för informationssäkerhet omfattar styrningen, organisationen och upprätthållandet av ledningen, som dokumenteras i informationssäkerhetspolicyn eller motsvarande styrdokument. - Man har en aktuell informationssäkerhetspolicy eller motsvarande styrdokument som godkänts av ledningen. Säkerhetsprinciperna och policyerna är heltäckande och ändamålsenliga i förhållande till organisationen och de objekt som ska skyddas. - Personalens och underleverantörernas ansvar i fråga om informationssäkerhet har beskrivits.	5 ledarskap 9.2 intern kvalitetsrevision 9.3 ledningens syn 10 förbättring av ledningssystem A.5.1.1 Informationssäkerhetspolicyer A.6.1.1 Roller och ansvar för informationssäkerhet A.15.1.1 Informationssäkerhetspolicy för leverantörsrelationer
3) *hantering av informationssäkerhetsrisker vid tillhandahållande av en identifieringstjänst* - Ledningssystemet för informationssäkerhet omfattar hantering av de informationssäkerhetsrisker	6 planering

som anknyter till tillhandahållandet av identifieringstjänsten. - Riskhantering är en regelbunden, kontinuerlig och dokumenterad process. - De identifierade riskerna klassificeras och prioriteras. - Genom riskhanteringsprocessen identifieras risker som berör informationens konfidentialitet, integritet och tillgänglighet. - Riskhanteringsprocessen och dess resultat används för att planera säkerhetsfunktioner för identifieringstjänsten/identifieringssystemet. - Jämför tillämpningsanvisningen för eIDAS-förordningen om tillitsnivåer: *En allmän princip för riskhanteringen är att organisationen själv måste välja vilken risknivå den anser godtagbar. Genom kravet i avsnitt 2.4 ändras denna allmänna princip, eftersom det föreskriver att organisationens säkerhetsåtgärder ska ställas i relation till riskerna på respektive nivå.* - I bestämmelse 6.1 i föreskriften fastställs närmare krav för bedömningen av riskerna i identifieringsmedlet	
4) *resurser för informationssäkerheten, kompetens, personalens medvetenhet om informationssäkerheten, kommunikation och dokumentation samt administration av dokumenterad information* - Systemet för hantering av informationssäkerheten omfattar resurstilldelning för informationssäkerhet, behörighetskrav, personalens medvetenhet om informationssäkerhet, kommunikation och dokumentation samt hantering av dokumenterad information. - Alla som deltar i uppgifter i anknytning till elektronisk identifiering ska ha tillgång till och känna till de aktuella anvisningarna och rutinerna för informationssäkerhet. - Säkerhetsutbildningen för personalen är regelbunden och dokumenteras. Utbildningens effektivitet följs upp. - Som ett typiskt exempel på hantering av behörighetskraven för personalen hos en leverantör av ett identifieringsverktyg kan man nämna inskolning i kontroll av äktheten hos pass och identitetskort vid	7 stödfunktioner

inledande identifiering av personer som ansöker om identifieringsverktyg eller i informationssäkerhetsrutiner i hantering av ett identifieringssystem på distans.	
5) planering och styrning av tillhandahållandet av en identifieringstjänst för att informationssäkerhetskraven ska kunna uppfyllas - I ledningssystemet för informationssäkerhet sköter man planeringen och styrningen av tillhandahållandet av identifieringstjänsten så att de informationssäkerhetskrav som ställs på identifieringstjänsten uppfylls. - Kraven på identifieringstjänster (autentiseringslagen, EU:s förordning om tillitsnivåer för elektronisk identifiering och ämbetsverkets föreskrift 72) har beaktats i ledningssystemet.	8 verksamhet A.18.1.1 överensstämmelse/efterlevnad av krav i lagstiftningen och avtal: specificering av de lagstadgade och avtalsmässiga krav som ska tillämpas
6) *bedömning av effektivitet och funktion i ledningen avseende informationssäkerheten* - Ledningssystemet för informationssäkerhet omfattar regelbunden bedömning av effektiviteten och funktionen i ledningen av informationssäkerheten, - det vill säga hur stor effekt ledningen avseende informationssäkerheten har på de faktorer, processer och problem som inverkar på informationssäkerheten i identifieringssystem.	9.1 uppföljning, mätning, analys, bedömning

4.4.3 Riskhanteringsmodell och -process

Den riskhantering som avses i bestämmelse 4.2 3) måste omfatta riskerna i hela identifieringssystemet. Skyldigheten omfattar också riskerna i de identifieringsverktyg som beviljats inom ramen för systemet, det vill säga identifieringsmedlet. I bestämmelse 6.1 definieras särskilda krav på hot- och riskbedömning för ett identifieringsmedel samt sådant som åtminstone måste beaktas i bedömningen.

Föreskriften tar inte ställning till vilken modell som ska användas i riskhanteringen eller vilken standard den ska följa. I riskbedömningar för såväl hela identifieringssystem som i synnerhet identifieringsmedel enligt bestämmelse 6 kan man använda samma standard eller verksamhetsmodell som valts av leverantören av identifieringstjänsten.

I riskbedömningen kan man använda relevanta standarder. Föreskriften definierar inte en viss standard som obligatorisk eller som referensobjekt. I riskhanteringen kan man använda exempelvis följande standarder eller anvisningar:

- SFS-ISO 31000:2018 [13]
- ISO/TR 31004, Risk management – Guidance for the implementation of ISO 31000, and International Standard/ISO/TR 31004:fi [14]

- SFS-EN IEC 31010:2019, ISO/IEC 31010, Risk management – Risk assessment techniques, developed jointly with the International Electrotechnical Commission/ [15]

- ISO 27005 [16] https://en.wikipedia.org/wiki/ISO/IEC_27005

- VAHTI Riskhanteringsanvisning, Finansministeriets publikationer 22/2017 [17] https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/80013/VM_22_2017.pdf?sequence=1&isAllowed=y

- NIST Risk Management Framework (RMF) [18] https://csrc.nist.gov/projects/risk-management/about-rmf

- I synnerhet vid bedömningen av förverkligandet av identifieringsmedel eller krypteringspraxis kan man även använda standarder, såsom FIPS 140-3 Security Requirements for Cryptographic Modules [19] https://csrc.nist.gov/publications/detail/fips/140/3/final

Som checklista för riskhanteringsmodellen kan man även använda följande, ur källan KATAKRI 2020 [12], T-03:

1) *Hanteringen av informationssäkerhetsrisker är en del av organisationens verksamhet och övriga riskhantering.*

2) *Genom hanteringen avinformationssäkerhetsrisker säkerställer man tillräckliga informationssäkerhetsåtgärder för att skydda säkerhetsklassificerade uppgifter.*

3) *Vid bedömning och analys av informationssäkerhetsrisker ska man använda en metod för produktion av information som är lämplig för funktionen och begriplig för beslutsfattandet.*

4) *Tillräckligt många experter deltar i hanteringen av informationssäkerhetsrisker.*

5) *I hanteringen av informationssäkerhetsrisker har man beaktat de risker som orsakas av berörda parter och leveranskedjor. Jfr risker som anknyter till leveranskedjorna för säkerhetskritiska anordningar och program (jfr I-01, I-12 och I-13).*

6) *Resultaten av bedömningen och analysen av informationssäkerhetsrisker används i planeringen och genomförandet av informationssäkerhetsåtgärder för säkerhetsklassificerade uppgifter, bedömning av effekterna av säkerhetstillbud samt i hanteringen av förändringar och till tillämpliga delar i upphandlingsförfaranden.*

7) *Informationssäkerhetsåtgärderna dimensioneras enligt riskerna med beaktande av bland annat informationens säkerhetsklass, omfång, form, klassificeringsgrund och förvaringslokaler i förhållande till de bedömda riskerna.*

8) *Organisationen har till centrala delar dokumenterat de tillsyns- och säkerhetsåtgärder som ska tillämpas samt den riskbedömning som utgör grunden för dem.*

Riskhanteringsprocessen bör omfatta de processer som beskrivs i ISO31000-standarden, där man beaktar (t.ex. SFS-ISO 31000:2018, sidan 14) [13]

1) *Omfattning, verksamhetsmiljö och kriterier*

2) *Riskbedömning*
   - *Identifiering av risker*
   - *Riskanalys*
   - *Bedömning av riskernas betydelse*
3) *Hantering av riskerna*
4) *Kommunikation och informationsutbyte*
5) *Inspelningar och rapporter*
6) *Uppföljning och granskning*

4.4.4 Bestämmelse 4.1, övervägda alternativ

År 2016 övervägdes vilka standarder som kan användas som referens i föreskriften. Man kom då fram till att ISO 27001 är den enda standarden som är tillräckligt omfattande. I utvärderingarna har det i praktiken kommit fram att åtminstone finansbranschens standarder (såsom PCI-standarderna, PCI DSS [20]) används som en del av hanteringen av informationssäkerheten.

Ämbetsverket bedömer att det fortfarande inte har lagts fram några relevanta heltäckande alternativ till ISO 27001. Den är inte det enda alternativet, men verkar vara den enda standard som används allmänt oberoende av bransch uttryckligen för hantering av informationssäkerhet.

I responsen i enkäten om behovet av ändringar i föreskriften föreslogs att föreskriftens ordalydelse skulle skärpas eller preciseras så att efterlevnad av standarden eller certifiering krävs. Transport- och kommunikationsverket bedömer att ett ovillkorligt certifieringskrav skulle vara ekonomiskt belastande och lämpa sig dåligt för en situation där hanteringen av datasäkerheten sköts genom en kombination av flera standarder.

4.5 Bestämmelse 5 Krav på informationssäkerhet i identifieringssystem

4.5.1 Allmänt

I bestämmelse 5 preciseras de åtgärder som behövs för förverkligandet av informationssäkerheten i hela identifieringssystemet.

Allmänna bestämmelser om kraven finns i 8 § 1 mom. 4 punkten i autentiseringslagen, som innehåller hänvisningar till avsnitten 2.2.1, 2.3.1 och 2.4.6 i bilagan till förordningen om tillitsnivåer för elektronisk identifiering [4].

Identifieringstjänster av olika storlek samt nykomlingar. Kraven på identifieringssystem och identifieringsmedel berör identifieringstjänstleverantörer i alla storlekar och med olika resurser, det vill säga leverantörer av identifieringsverktyg och till tillämpliga delar identifieringsförmedlingstjänster. Syftet med föreskriftens krav är att förbättra säkerheten, men även att förbättra regleringens förutsägbarhet för att underlätta identifieringstjänsternas verksamhet. Tydliga krav skapar enligt ämbetsverkets bedömning också inbördes förtroende för informationssäkerheten hos nuvarande och kommande identifieringstjänster i förtroendenätet.

Förmåga till skydd mot informationssäkerhetshot. Enligt avsnitt 2.3.1 i förordningen om tillitsnivåer för elektronisk identifiering

> *Autentiseringsmekanismen genomför säkerhetskontroller för att verifiera medlet för elektronisk identifiering, varför det är högst osannolikt att exempelvis gissningar, tjuvlyssning, omspelning eller manipulation av kommunikation som görs av en angripare med måttlig angreppspotential ("moderate attack potential") kan underminera autentiseringsmekanismerna.*

På tillitsnivån hög måste säkerhetsåtgärderna dimensioneras för att skydda mot angrepp med hög (”high”) angreppspotential.

Enligt avsnitt 2.4.6 i förordningen om tillitsnivåer för elektronisk identifiering

> *1. Proportionella tekniska kontroller ("technical controls") ska finnas för att hantera riskerna för tjänsternas säkerhet, och för att skydda de behandlade uppgifternas sekretess, integritet och tillgänglighet.*

Avsnitt 2.4.6 i förordningen om tillitsnivåer i elektronisk identifiering innehåller också bestämmelser om skydd av elektroniska kommunikationskanaler mot avlyssning, manipulation och omspelning, om förmågan att agera om risknivån förändras eller vid incidenter och säkerhetsöverträdelser och om informationssäkerheten i alla medel.

Informationssystem-, datakommunikations- och användningssäkerhet. I bestämmelserna 5.2–5.4 preciseras datakommunikations-, informationssystem- och användningssäkerheten, så att den informationssäkerhet som krävs enligt regelverket uppnås. Preciseringarna baserar sig på den indelning i datakommunikations-, informationssystem- och användningssäkerhet som används allmänt i fråga om säkerhet i informationssystem. Dessa områden utesluter inte varandra, utan är snarare olika perspektiv på samma identifieringssystemhelhet.

Separation som informationssäkerhetsåtgärd Separation av personalens arbetsuppgifter, separation av fysiska arbetslokaler och -verktyg eller en eventuell separation av teknisk servicemiljö och servermiljöer från övrig produktion hör till de normala rutinerna. Tillräcklig separation antas förverkligas genom normal hantering, planering och auditering av informationssäkerhet, om ingenting annat separat fastställs om detta förutom kraven i bestämmelse 5.5.

Konsekvenser. Kraven i bestämmelse 5 ändras inte, men de förtydligas. Bestämmelserna har preciserats och exempel på tillämpning i bedömningen och tillsynen av identifieringstjänsters överensstämmelse har lagts till i grunderna utifrån samlade erfarenheter och tillämpningspraxis.

Syftet med ändringarna är att förbättra identifieringssystemens säkerhet. Kraven är inte tekniskspecifika, och har därför inga effekter på utvecklingen av identifieringstjänsternas egenskaper.

Övriga metoder för styrning

Anvisning. I bedömningsanvisningen 211/2019 preciseras kraven på utvärdering av informationssäkerhet.

Rekommendation. I enkäten om behovet av ändringar i föreskriften efterfrågades en testningstjänst som skulle tillhandahållas av ämbetsverket. Ämbetsverket har dock inga fastställda operativa uppgifter i tillsynen av säker elektronisk identifiering, såsom anskaffning och upprätthållande av en testningstjänst. Utarbetande av testningsrekommendationer för testfunktioner som tillhandahålls av identifieringstjänsterna själva skulle vara möjligt inom förtroendenätet.

Samreglering. Informationssäkerhetsnivån definieras i regleringen och tillsynen. Tillhandahållare av tjänster för stark autentisering har möjlighet att utbyta information om säkerhetshot och -åtgärder utan att hindras av sekretessbestämmelserna.

Styrning genom information. Inga anmärkningar.

4.5.2 Identifieringssystemet som helhet (arkitektur och underleverantörer)

Med identifieringssystem (engl. eID scheme) avses ett system inom vilket metoder för elektronisk identifiering, det vill säga identifieringsverktyg, beviljas och upprätthålls för användarna. Ett identifieringssystem omfattar identifieringstjänstleverantörens tekniska system, hantering av informationssäkerhet och andra angivna tillförlitlighetskrav. Identifieringssystemet omfattar också alla delar och funktioner som skaffats från underleverantörer, som anknyter till produktionen av identifieringstjänsten. Termen i autentiseringslagen är *system för elektronisk identifiering*.

Ett identifieringssystem inkluderar bland annat följande:
- Datorhallar och andra lokaler
- servrar och programvara för identifieringstransaktioner
- systemkomponenter för identifiering
- förbindelser, nätslussar och kopplingar mellan delarna i identifieringssystemet, inklusive administratörsförbindelser
- rutiner för skydd av förbindelserna, gränssnitt mellan systemets delar och andra faktorer – inklusive säkerhetskontroller för kontakter till utomstående aktörer
- informationssäkerhetskomponenter i nätverket, såsom brandväggar
- informationsresurser

Underleverantörer. Underleverantörer behandlas inte separat i föreskriften. Tillhandahållaren av identifieringstjänsten ansvarar enligt 13 § i autentiseringslagen för att de tjänster som den använder via underleverantörer uppfyller kraven. I förverkligandet av ett identifieringssystem och ett identifieringsmedel används vanligen underleverantörer. I Transport- och kommunikationsverkets bedömningsanvisningar för elektroniska identifieringstjänster 211/2019 O behandlas underleverantörer med tanke på bedömning av överensstämmelse [21].

Om man i ett identifieringssystem använder produktifierade komponenter eller produkter från molntjänster (exempelvis Amazon Web Services, Google, Microsoft Azure), gäller kraven på identifieringssystem dessa komponenter, och de måste också inkluderas i bedömningen av överensstämmelse. I ett identifieringssystem får man endast använda komponenter som uppfyller kraven och vars överensstämmelse kan säkerställas.

4.5.3 Bestämmelse 5.1.1 Identifieringssystemets skyddsförmåga

Bestämmelse 5.1.1 är ny. Där preciseras kravnivån för helheten av identifieringssystemets säkerhetsåtgärder och tekniska inställningar.

Enskilda krav för tillitsnivåerna väsentlig och hög har i regel inte definierats separat i föreskriften. Kravnivån för de säkerhetsåtgärder som förutsätts enligt avsnitt 2.4.6 i förordningen om tillitsnivåer för elektronisk identifiering, det vill säga tekniska kontroller, fastställs däremot enligt förmågan till skydd mot angreppspotential enligt avsnitt 2.3.1 i förordningen om tillitsnivåer. Kravet gäller hela identifieringssystemets skyddsförmåga och därmed de delfaktorer inom datakommunikations-, informationssystem- och användningssäkerhet som preciseras i bestämmelserna 5.2–5.4.

För hot- och riskbedömningen fastställs inga närmare kriterier och ingen standard som ska följas. Den materiella bedömningen ska basera sig på goda kunskaper om branschen samt på uppföljning av hot, sårbarheter och den tekniska utvecklingen.

Se tillämpningsanvisningen för förordningen om tillitsnivåer, LOA Guidance[2] [22], avsnitt 2.3.1

> *De termer som används för de olika angreppspotentialerna på tillitsnivån är "förhöjd/grundläggande" (enhanced-basic), "måttlig" (moderate) och "hög" (high). Dessa termer har lånats från standarderna ISO/IEC 15408 "Information technology – Security techniques – Evaluation criteria for IT security" [23] och ISO/IEC 18045 "Information technology – Security techniques – Methodology for IT security evaluation" [24]. Standardernas text kan läsas fritt på adressen www.commoncriteriaportal.org/cc (CCPART1-3 motsvarar standarden ISO/IEC 15408 och CEM standarden ISO/IEC 18045).*
>
> *I standarden ISO/IEC 15408-1 definieras angreppspotential som den arbetsmängd som ett angrepp [mot en mekanism] kräver, uttryckt som angriparens sakkunskap, resurser och motivation.*
>
> *I standarden ISO/IEC 18045 / bilaga B.4 till CEM ges anvisningar för hur man beräknar den angreppspotential som krävs för att utnyttja en viss svaghet i en autentiseringsmekanism.*
>
> *Uppfyllandet av kraven i genomförandeförordningen förutsätter en bedömning av tåligheten mot eventuella angrepp.*
>
> *I bedömningen ska man beakta relevanta hot. I standarden ISO 29115 [25] nämns exempelvis följande: gissningar via och utanför nätet, omspelning av identifieringsuppgifter, nätfiske, avlyssning, replay-attack, sessionskapning, man-i-mitten-attack, stöld av identifierande uppgifter, spoofing-attack och att utge sig för att vara någon annan.*

4.5.4 Bestämmelse 5.1.2 Relationen mellan krypteringskraven i bestämmelse 5 och 7

Bestämmelse 5.1.2 är delvis ny. I den tidigare föreskriften angavs det gällande *säkerheten i informationssystem* att man måste använda krypteringslösningar som rekommenderas internationellt eller nationellt *till andra delar vad som föreskrivs i 7 §.* Kravet på användning av internationellt eller nationellt rekommenderade krypteringslösningar har också lagts till för datakommunikations- och användarsäkerheten, och relationen till krypteringslösningarna enligt bestämmelse 7 definieras för alla krav i bestämmelse 5 i bestämmelse 5.1.2.

I avsnitt 7 i föreskriften anges särskilda krypterings- eller skyddskrav för vissa datakommunikationsförbindelser och meddelanden. Kravet enligt avsnitt 5 i föreskriften gäller allmänt andra förbindelser och element såsom exempelvis interna element i identifieringssystemet, de uppgifter som förvaras samt förbindelserna till underleverantörernas system. Kravet omfattar såväl 5.2 datakommunikationssystem och 5.3 datasystem som 5.4 operation. Även i dessa rekommenderas att man till tekniskt tillämpliga delar använder de lösningar som fastställs i bestämmelse 7, men skyddet kan också förverkligas genom andra åtgärder.

4.5.5 Bestämmelse 5.2 Datakommunikationssäkerhet

Bestämmelse 5.2 motsvarar ganska långt föreskriftens tidigare ordalydelse i 5.1 § 1 stycket. Preciseringar har gjorts i bestämmelsen.

Utöver de krav som anges i bestämmelse 5.2 anges i bestämmelse 14 om ett datakommunikationsprotokoll och i bestämmelse 7–9 om skydd av datakommunikation och meddelanden mellan identifieringstjänster samt mellan identifieringstjänster och

[2] LOA Guidance i sin helhet har inte översatts till svenska. Översättning har gjorts endast här.

de ärendehanteringstjänster som förlitar sig på dem. Säkerheten i förbindelsen mellan identifieringsverktygets användare och leverantören av identifieringsverktyget ingår i kraven på autentiseringsmekanismen i bestämmelse 6.

5.2.a) säkerhet i nätstrukturen

Genom säkerheten i nätstrukturen ser man till att *elektroniska kommunikationskanaler som används för att utbyta personuppgifter eller känslig information skyddas mot avlyssning, manipulation och omspelning.*

Nätets struktur ska dokumenteras. Identifieringssystemets anordningar och system för datatrafik har identifierats och dokumenterats. Säkerheten i strukturen gäller datakommunikationsförbindelser mellan identifieringssystemets delar och deras skyddsrutiner. Den berör nätområden med olika säkerhetsnivåer samt filtrerings- och tillsynssystem mellan dem. Kravet på strukturell säkerhet gäller också alla relevanta datakommunikationsförbindelser till underleverantörer (infrastruktur, programvaror, användningstjänster, kortfabrik etc.).

5.2.b) indelning av datakommunikationsnätet i zoner

Målet med kravet är att minska de risker som orsakas genom datakommunikationsförbindelserna för nätverkens integritet, sekretess och användbarhet.

Indelningen i zoner innebär bland annat att produktionsnätverket, underhålls- och administrationsnätverket samt det övriga kontorsnätverket ska vara separata från varandra. Det ska också finnas en utvecklingsmiljö som är separat från produktionen.

5.2.c) filtreringsregler enligt principen om behovsenlig behörighet

Principen om behovsenlig behörighet innebär att alla förbindelser som inte är nödvändiga för verksamheten ska nekas eller stängas. Produktionsnätets förbindelser till det offentliga nätet ska vara riskbaserade förbindelser som endast möjliggör tjänstens funktioner.

5.2 d) administration av filtrering och kontrollsystem

Inga exempel på tillämpningen.

5.2.e) säkra administratörsförbindelser

Preciseringen ”säkra” har lagts till i bestämmelsen.

Administrationsförbindelserna kan vara såväl organisationsinterna som externa kommunikationsförbindelser. Den informationshanteringsmiljö som används för administration ska separeras från andra miljöer.

Se även avsnitt 5.5 i föreskriften.

5.2.f) *nationellt eller internationellt rekommenderade krypteringslösningar*

Gällande källor till rekommenderade krypteringslösningar, se avsnitt 4.7.5 i denna motiveringspromemoria.

4.5.6 Bestämmelse 5.3 Säkerhet i informationssystem

Bestämmelse 5.3 motsvarar ganska långt föreskriftens tidigare ordalydelse i 5.1 § stycke 2. Preciseringar har gjorts i bestämmelsen.

5.3.a) hantering av behörigheter enligt principen om behovsenlig behörighet

Preciseringen ”enligt principen om behovsenlig behörighet” har lagts till i bestämmelsen.

Principen om behovsenlig behörighet innebär att behörigheter endast ska beviljas utifrån informationssystemets klassificering och användarens uppgifter. Med hjälp av hantering av behörigheter ska man på ett systematiskt och dokumenterat sätt begränsa tillgången till information och miljöer där information hanteras. Överflödiga användarbehörigheter ska tas bort regelbundet.

Man måste vara särskilt noggrann med definitionen av administratörsrättigheter, och system- och transaktionsloggarnas integritet ska säkerställas.

I definitionen av administratörsbehörigheterna ska man använda separation av system och säkerställande av loggarnas oföränderlighet samt andra ändamålsenliga metoder.

5.3.b) individuell identifiering av systemanvändarna

Preciseringen ”individuell” har lagts till i bestämmelsen. Användaruppgifterna måste vara personliga och får inte användas gemensamt.

Genom identifieringen säkerställer man att endast rätt användare kommer in i systemen och att transaktionerna kan spåras.

Användarna av identifieringssystemets datasystem måste identifiera sig med metoder som är kända och anses säkra. I regel ska man använda identifiering som baserar sig på flera faktorer (*2FA dvs. 2-factor-authentication, MFA dvs. multi-factor-authentication*). Om användarnamn och lösenord som helhet utifrån andra skyddsmetoder bedöms vara tillräckligt i något sammanhang, ska lösenorden vara tillräckligt starka.

5.3.c) härdande av system

Med härdande av system avses att man i identifieringssystemet använder endast de tjänster, funktioner, processer, apparater och komponenter som är nödvändiga för dess funktion.

Användningen av dem ska definieras så att man har avlägsnat alla onödiga rättigheter och funktioner från installationen. En härdad installation innehåller endast sådana komponenter och tjänster samt användar- och processrättigheter som är nödvändiga för att uppfylla funktionskraven och säkerställa säkerheten.

5.3.d) skydd mot skadliga program

I ett identifieringssystem måste man sörja för upptäckt, förebyggande, förhindrande och åtgärdande av skador och hot som orsakas av skadliga program.

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

Preciseringen ”förmågan och en process för att” har lagts till i bestämmelsen.

Bestämmelsen förutsätter alltså att det finns ett på förhand fastställt förfarande som följs vid spårningen och åtgärdandet av eventuella säkerhetsavvikelser.

De klassificeringar som beskrivs i nästa avsnitt ingår i förmågan att spåra händelser.

Förmågan till spårning förutsätter att identifieringssystemets klockslag upprätthålls på ett tillförlitligt sätt. Klockslaget behövs för att på ett tillförlitligt sätt visa transaktionstider. Med klockslagets tillförlitlighet avses en tillförlitlig tidskälla och tillräckligt strikt feltolerans. Den rekommenderade feltoleransen är 0,5 sekunder.

5.3.f) *förmågan att upptäcka avvikelser och en process för att åtgärda dem*

I föreskriften har uttrycket ”återhämtning” ersatts med uttrycket ”process för att åtgärda dem”.

Enligt föreskriften förutsätts att det finns förmåga och på förhand fastställda processer för att upptäcka avvikelser i identifieringssystemet.

I definitionerna ska man beakta hur kritiska komponenterna och processerna i datakommunikationsförbindelserna och informationssystemen är samt klassificeringen av dem samt att händelser som påverkar säkerheten ska kunna spåras även i efterhand.

Observationsförmåga förutsätter att händelseloggar om systemets funktion samt om händelser och avvikelser som påverkar informationssäkerheten samlas in och sparas i identifieringssystemet. För att upptäcka säkerhetstillbud och säkerhetsincidenter krävs det att identifieringssystemets funktion, förändringar och händelseloggar övervakas.

Loggarnas integritet säkras bland annat genom åtkomstkontroll och användningsrättigheter, skydd av miljön och vid behov genom att flytta bort logguppgifter från målsystemet. Separation av personalens arbetsuppgifter behövs åtminstone för att en och samma person inte ska kunna skapa ett identifieringsverktyg och administrera logguppgifter som hänför sig till skapande och införande av identifieringsverktyg.

Processen för åtgärdande innebär att alla avvikelser och störningar i identifieringssystemet behandlas och analyseras och deras allvarlighet klassificeras systematiskt enligt fastställda förfaranden och avvikelserna åtgärdas på det sätt som allvarlighetsklassificeringen kräver.

5.3.g) *internationellt eller nationellt rekommenderade krypteringslösningar*

Gällande källor till rekommenderade krypteringslösningar, se avsnitt 4.7.5 i denna motiveringspromemoria.

4.5.7 Bestämmelse 5.4 Säkerhet vid användning

5.4.a) omsorgsfull hantering av förändringar

Ordet ”omsorgsfull” har lagts till i bestämmelsen.

Kravets syfte är att förebygga att ändringar på ett identifieringssystem orsakar fel i fråga om informationssäkerhet eller användbarhet. Ändringar är ofta brådskande, och deras effekter kan återspeglas i många detaljer i systemet. Därför måste man planera dem omsorgsfullt, standardisera processerna och reservera tillräckligt med tid för förändringarna. Granskningar och tester är en del av en tillförlitlig förändringsprocess. Både processerna och de ändringar som gjorts bör dokumenteras, så att orsakerna till eventuella fel kan spåras. I korrekt dokumentation sparas i identifieringssystemets administrationsloggar uppgifter om ändringar i identifieringssystemet, och loggarna separeras från andra loggar och man sörjer för deras integritet.

5.4 b) *en behandlingsmiljö och lagring för sekretessbelagt material som baserar sig på klassificeringen av informationen*

”Som baserar sig på klassificeringen av informationen” och ”lagring” har lagts till i bestämmelsen.

Skyddet av uppgifter som förvaras har överförts till denna föreskrift från 7 § 4 mom., som löd: *Man ska sörja för integriteten och sekretessen för uppgifter som lagras i identifieringssystem. Om skyddet av uppgifterna endast baserar sig på kryptering, tillämpas kraven på underskrift, symmetrisk kryptering och hashfunktioner i 1 mom.*

En grundförutsättning för behandling av informationen är en klassificering av informationen och materialen, utifrån vilken man klassificerar informationssystemen och de funktioner som de möjliggör. I klassificeringen av system ska man beakta hela livscykeln för den information som skyddas.

I klassificeringen ska man beakta exempelvis affärshemligheter, säkerhetsarrangemang och loggar. Vidare ska man beakta personuppgifter och de kryptografiska hemligheter som anknyter till beviljandet av identifieringsmedel.

Säkerhetsåtgärderna för hantering och förvaring av information ska dimensioneras med beaktande av bland annat informationens klassificeringsgrund, mängd, form och förvaringslokaler i förhållande till det bedömda hotet. Den förvarade informationens integritet och sekretess ska skyddas genom säkerhetsåtgärder såsom åtkomstkontroll och kryptering. Exempel på uppgifter som ska skyddas särskilt noggrant är nycklar som används för kryptering eller underskrift eller underskriftsnycklar för rotcertifikat.

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

”Skydd mot hot i distansanvändningsmiljön” har lagts till i bestämmelsen.

I detta avsnitt finns inga exempel på tillämpningen. Se avsnitt 5.5 i föreskriften.

5.4 d) *hantering av programutveckling och sårbarheter i programvara*

Preciseringen ” programutveckling” har lagts till i bestämmelsen.

I föreskriften förutsätts att identifieringstjänsten har ett förfarande för att följa upp allmänna sårbarheter, och det ska omfatta den programvara som påverkar identifieringssystemets säkerhet.

I programvara som används i identifieringssystemet ska man följa principerna för säker programmering. Man ska också beakta säkerheten i utvecklingsmiljön.

Kravet på programvarusäkerhet omfattar exempelvis identifieringsapplikationer och programbibliotek.

Hantering av sårbarheter innebär uppföljning av sårbarheter i program samt i krypteringsalgoritmer och -metoder, följande av meddelanden samt automatiska och regelbundna kontroller av programvara som används i systemen både i externa och interna nätverk.

Jfr PiTuKri, avsnitt KT-04 om hantering av sårbarheter, [26] Traficoms publikation 21/2021 Säkerhetskriterier för molntjänster (PiTuKri) https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Traficom_PiTuKri_2020_SE_210506_WEB.pdf

Tillförlitliga metoder för hantering av sårbarheter i programvaran förverkligas för molntjänstens hela livscykel.

Man bör särskilt beakta följande:

a) Molnleverantören följer med myndigheternas, maskin- och programtillverkarnas och motsvarande instansers informationsbrev om säkerhet och utför kontrollerad installation av de säkerhetsuppdateringar som bedöms vara nödvändiga baserat på en riskanalys (jfr MH-01).

b) En automatisk systemkontroll för att upptäcka kända sårbarheter ska köras minst varje månad. Om man har avvikit från de planerade inställningarna eller den planerade säkerhetsuppdateringsnivån ska orsakerna analyseras och avvikelserna rättas till eller dokumenteras i enlighet med hanteringsprocessen för incidenter (se TJ-04) (se TJ-04).

Sårbara algoritmer och krypteringsmetoder. I beredningen av bestämmelse 7 tillsammans med berörda parter har en fråga lyfts om hur tillämpningen av avsnitt 7 påverkas ifall algoritmer eller metoder som listats som godkända i föreskriften blir sårbara och detta leder till att man måste sluta använda dem.

Enligt 5.4 d) har identifieringstjänsterna möjlighet och skyldighet att hantera sårbarheter. Ett ändamålsenligt sätt att beakta sårbarheter är att följa informationskanaler som berör dem och på eget initiativ avstå från att använda sårbara metoder.

Ämbetsverkets uppfattning är att krypteringsalgoritmer och metoder inte blir sårbara plötsligt, utan att det vanligen är fråga om en utveckling som tar flera år eller till och med decennier. Detta gör det möjligt att ändra föreskriften vid behov, men om föreskriften inte hinner ändras i en oväntad situation kan ämbetsverket styra reaktionen på sårbarheter genom rådgivning.

5.4.e) *säkerhetskopiering*

Syftet med säkerhetskopiering är att se till att information och system återställs vid en störning och att informationen kan spåras vid behov.

Säkerhetskopieringen måste skötas systematiskt och med hänsyn till informationens klassificering och livscykel. Vid förvaringen måste man beakta att den fysiska placeringen ska separeras från det egentliga systemet.

5.4.f) *nationellt eller internationellt rekommenderade krypteringslösningar*

Gällande källor till rekommenderade krypteringslösningar, se avsnitt 4.7.5 i denna motiveringspromemoria.

4.5.8 Bestämmelse 5.5 Administratörs- och distansförbindelser i identifieringssystemets produktionsnät

I bestämmelse 5.5 preciseras kraven på terminaler och distansförbindelser som används vid hantering på distans på tillitsnivåerna väsentlig och hög. Bestämmelsen motsvarar 5 § 2 momentet i den tidigare föreskriften.

Genomförandet av systemet och dess kontroller måste beroende på tillitsnivån anpassas till angreppspotential på måttlig eller hög nivå.

Anställdas terminalenheter som tillåter åtkomst till ledningssystem kan lätt utgöra en informationssäkerhetsrisk om inte särskild uppmärksamhet fästs vid det.

På tillitsnivån väsentlig krävs inte att terminalen avskiljs, men på tillitsnivån hög krävs antingen en dedikerad terminal eller virtualiserad terminering eller en lösning som baserar sig på kvm-principen (fjärrskrivbord).

Internet och kontorsnät anses vara nätverk som saknar förtroende, om inte kontorsnätet omfattas av bedömning av överensstämmelse.

Kraven på *tillitsnivån väsentlig* är sedvanliga och kan täckas genom att tillämpa kraven i t.ex. standarden ISO 27001. Överföringskanalen ska alltså vid fjärranvändning vara skyddad och de risker som kontorsnätet kan orsaka måste beaktas.

På tillitsnivån hög kan kraven genomföras åtminstone så att arbetsstationer som är i fjärranvändning nekas åtkomst till organisationens övriga tjänster, såsom e-post, och att möjligheten att använda andra funktioner än de som är nödvändiga för användning av administrationsnätet tas bort från arbetsstationen. I praktiken betyder detta alltså att det behövs en separat arbetsstation för administration.

Helhetsbedömningen på tillitsnivån hög betyder att man, om man använder en annan än en sådan härdad arbetsstation som beskrivs ovan, vid genomförandet ska beakta separation av produktionssystemet och övriga arrangemang med vilka informationssäkerhetshot kan hanteras. I princip förutsätter det en virtuell terminering eller en lösning som baserar sig på kvm-principen (keyboard, video, mouse; fjärrskrivbord).

Det väsentliga är vad man gör med den terminalenheten som tar virtuell kontakt och därför är t.ex. en two-factor VPN-förbindelse till ett virtuellt skrivbord inte ensam en lösning. Det är inte heller tillräckligt att man använder antivirusprogram och webbproxy.

Vid överföring av nödvändiga filer från en terminalenhet till en annan ska man också ta hänsyn till risk för skadliga program bl.a. genom att endast använda tillförlitliga källor och säkerställa informationssäkerheten (integriteten) med alla nödvändiga metoder.

4.5.9 Bestämmelse 5, övervägda regleringsalternativ

4.5.9.1 Krav för tillitsnivån hög

I enkäten om behovet av ändringar i föreskriften önskade en del av respondenterna att de tekniska kraven för tillitsnivåerna väsentlig och hög skulle definieras detaljerat i föreskriften. Man fick dock inga förslag på krav där preciseringar särskilt skulle behövas.

Ämbetsverket anser att det inte är möjligt att precisera kraven för tillitsnivåerna i föreskriften, eftersom ett identifieringssystem inkluderar många delfaktorer. En detaljerad definition är inte ändamålsenlig, eftersom de tekniska genomförandena och hoten förändras hela tiden.

Man har i stället förtydligat och preciserat i föreskriften hur alla säkerhetsåtgärder ska ställas i relation till angreppspotentialen enligt tillitsnivån.

4.5.9.2 Separationskrav som informationssäkerhetsåtgärd

I beredningen av föreskriften år 2021 har man inte noterat grunder eller behov för att fastställa nya separationskrav.

Separation som informationssäkerhetsåtgärd I beredningen av föreskriften bedömdes år 2016 om någon av följande åtgärder är nödvändig på grund av kraven på

informationssäkerhet: separation av personalens arbetsuppgifter, separation av fysiska arbetslokaler och -verktyg eller en eventuell separation av teknisk servicemiljö och servermiljöer från övrig produktion.

I konsekvensbedömningen kom man då fram till att detaljerna gällande separationen i huvudsak skulle överföras till hanteringen, planeringen och auditeringen av informationssäkerheten. I konsekvensbedömningen ansåg man år 2016 att separation av personalens arbetsuppgifter behövs åtminstone för att en och samma person inte ska kunna skapa ett identifieringsverktyg och administrera logguppgifter som hänför sig till skapande och införande av identifieringsverktyg. Detta antogs förverkligas redan genom normal ledning, planering och kvalitetsrevision av informationssäkerheten och behöver därför inte bestämmas särskilt.

Fastställandet av säkerhetskrav för arbetsstationer som används i administrations- och kontorsnät väckte i beredningen år 2016 så många frågor att kraven förtydligades i föreskriftens 5 § 2 mom. och i tillämpningsanvisningen för motiveringspromemorian. De behålls som sådana i föreskriften och motiveringarna.

4.5.10 Tillförlitlighet hos klockslaget i identifieringssystemet

Motiveringspromemorian till föreskrift 72 har innehållit en rekommendation om tillförlitligheten hos klockslaget i identifieringssystem (föreskriftens motiveringspromemoria 2016/2018 avdelning C, avsnitt 1).

I beredningen av föreskriften har man övervägt att ta bort rekommendationen gällande feltolerans i identifieringssystemets tidskälla och klockslag, eftersom tillämpningen av den inte har tagits upp i styrningen och tillsynen av identifieringstjänster eller i responsen från berörda parter.

Identifieringssystemets klockslag är dock en del av allmänt gott underhåll av datakommunikations- och informationssystem, så detta behålls i motiveringarna, men omnämnandena flyttas till avsnittet om informationssystemsäkerhet i identifieringssystem.

> *Rekommendation MPS72 (samma 2.11.2016 och 14.5.2018) avdelning C avsnitt 1*
>
> *Leverantören av identifieringstjänster bör skaffa sig en tillförlitlig tidskälla med vilken leverantören synkroniserar klockslaget i sitt system. Klockslaget behövs för att på ett tillförlitligt sätt visa transaktionstider. Den rekommenderade feltoleransen är 0,5 sekunder. Synkronisering mellan aktörer behövs troligen inte.*
>
> *Frågan omfattas av rekommendationen ITU-R TF.1876 (03/2010) Trusted time source for time stamp authority* [27].
>
> *Möjliga tidskällor är exempelvis VTT:s/MIKES NTP eller PTP, av vilka den sistnämnda har tillgänglighetsgaranti. Det finns också andra alternativ.*

4.6 Bestämmelse 6 Krav på informationssäkerhet i identifieringsmedel

4.6.1 Bestämmelse 6.1 Identifieringsmedlets egenskaper och skyddsförmåga

4.6.1.1 Bestämmelse 6.1.1 Specificerad riskbedömning

Bestämmelsen är ny.

I bestämmelse 6.1.1 preciseras säkerhetskraven på den helhet som utgörs av identifieringsmedlets autentiseringsfaktorer och autentiseringsmekanism. Föreskriften kompletteras med krav på särskild riskbedömning och faktorer som ska beaktas där. Hot som berör autentiseringsfaktorer och autentiseringsmekanismer ska bedömas

separat. Identifieringsmedlet, det vill säga de autentiseringsfaktorer och säkerhetsåtgärder som används i det, ska planeras så att helheten skyddar mot de hot som bedömts finnas.

Ämbetsverket bedömer att en sådan modell är tillräckligt flexibel för olika identifieringsmedel och autentiseringsfaktorer och beaktar identifieringsmedlets säkerhetskontroller som helhet. Ämbetsverkets eventuella tillsynslösningar skulle basera sig på en noggrann bedömning av identifieringstjänstens risker, vid vilken man också beaktar effekterna av säkerhetskontroller.

Enligt den respons från berörda parter som man fått i beredningen fungerar ett riskorienterat tillvägagångssätt, men det är bra att ge anvisningar för vad som ska bedömas och med vilka metoder, så att godtagbarheten i den kvarstående risken blir så lätt att förutse som möjligt. I den valda regleringsmodellen preciseras kraven på riskbedömningen och de delfaktorer som ska beaktas i den. Tillämpningen behandlas i de följande avsnitten.

Övergångstid. Ämbetsverket anser utifrån respons från berörda parter att det inte behövs någon övergångstid för kravet, utan att kravet på utarbetande av en bedömning kan träda i kraft när den ändrade föreskriften träder i kraft.

Konsekvenser. Ämbetsverket bedömer att ett krav på en riskbedömning är en naturlig del av produktionen av en informationsteknisk tjänst av typen identifieringstjänst och en del av det fastställda kravet på hantering av informationssäkerheten. Ett särskilt krav i föreskriften kan precisera kraven gällande bedömning och utöka kraven på dokumentation. Ämbetsverket bedömer att kravet främjar en säker utveckling av identifieringsmedel och ger en motiverad grund för ämbetsverkets eventuella tillsynsåtgärder.

Alternativa regleringssätt. Som alternativ till avsnitt 6.1.1 har ämbetsverket bedömt regleringsmodeller där föreskriften skulle definiera specifika krav på autentiseringsfaktorer eller definiera krav på identifieringssystemets skyddsförmåga. Specifik reglering för olika autentiseringsfaktorer skulle på grund av autentiseringsfaktorernas mångsidighet och utveckling inkludera många detaljer som det enligt ämbetsverkets bedömning inte är möjligt eller ändamålsenligt att försöka täcka på bestämmelsenivå. Inte heller hoten mot identifieringsmedlens säkerhet eller säkerhetsåtgärderna för att skydda sig mot hoten är helt specifika för typen av autentiseringsfaktor. Man kan tänka sig indikatorer för skyddsförmågan eller andra slags preciseringar i föreskriften.

Övriga metoder för styrning.

De ändrade kraven beaktas i *bedömningsanvisningarna för identifieringstjänster*.

Gällande *samregleringen* anser ämbetsverket att gemensamma säkerhetshot kan behandlas i samarbetsgruppens informationsutbyte enligt autentiseringslagens 16 §. Enligt 12 a § i autentiseringslagen är det förbjudet att inom förtroendenätet använda information som fåtts från konkurrenter för andra än de syften för vilka de getts till leverantören av identifieringstjänsten.

Rekommendation eller informationsstyrning. Inga anmärkningar.

Tillsyn. En riskbedömning för identifieringssystemet och som en del av detta identifieringsmedlet är ett sedan tidigare gällande krav, så ingen övergångstid krävs. Riskbedömningen har dock inte nödvändigtvis utarbetats och dokumenterats med denna noggrannhet. Ämbetsverket bedömer separat om man ska övervaka utförandet av bedömningen och dess resultat när föreskriften trätt i kraft, exempelvis genom en

tillsynsenkät under 2022, eller först som en del av den regelbundna tidsbundna bedömningen av överensstämmelse som görs vartannat år, nästa gång år 2023, så att tillsynen i praktiken sker år 2024. Det särskilda kravet på bedömning gäller i vilket fall som helst förändringar i identifieringsmedel som anmäls till ämbetsverket efter ikraftträdandet. Det kan också komma att övervakas från fall till fall i störningssituationer.

4.6.1.2 Hot som bör beaktas i riskbedömningen

De hot som ska beaktas i hotbedömningar baserar sig på god branschkännedom, information som samlas in vid administrationen av identifieringstjänsten, konfidentiell information som fås i förtroendenätets samarbetsgrupp samt allmänt tillgänglig information om informationssäkerhetshot och sårbarheter.

Tillämpningsanvisningen för förordningen om tillitsnivåer, LOA Guidance [22], avsnitt 2.3.1:

> *I bedömningen ska man beakta relevanta hot. I standarden ISO 29115 nämns exempelvis följande: gissande via nätet och utanför nätet, omspelning av identifierande uppgifter, fiske efter information, avlyssning, replay-attack, sessionskapning, man-i-mitten-attack, stöld av identifierande uppgifter, spoofing-attack och att utge sig för att vara någon annan.*

Beroende på identifieringsverktygets och -mediets egenskaper hör åtminstone följande hot och kombinationer av hot som nämns i ISO 29115-standarderna och -anvisningarna NIST 800-63B Digital Identity Guidelines, Authentication and Lifecycle Management (https://pages.nist.gov/800-63-3/sp800-63b.html) till dem som bör beaktas

ISO 29115 Information technology — Security techniques — Entity authentication assurance framework [25]

- Online guessing/gissning med förbindelse
- Offline guessing/gissning utan förbindelse
- Credential duplication/kopiering av inloggningsuppgifter
- Phishing/nätfiske, snokande
- Eavesdropping/avlyssning
- Replay attack/omspelningsattack
- Session hijacking/kapning av session
- Man-in-the-middle/man-i-mitten -attack
- Credential theft/stöld av inloggningsuppgifter
- Spoofing/bedrägeri, att utge sig för att vara någon annan, att utge sig för att vara någon annan genom att förfalska information
- Masquerading/angrepp med falsk identitet

NIST 800-63B Digital Identity Guidelines, Authentication and Lifecycle Management [28]

- Assertion Manufacture or Modification/assertion/skapande av en falsk försäkran eller ändring av en försäkran
- Theft/stöld
- Duplication/kopiering
- Eavesdropping/avlyssning
- Offline Cracking/intrång utan förbindelse
- Side Channel Attack/attack via en sidokanal
- Phishing or Pharming/nätfiske/omdirigering av webbplats
- Social Engineering/manipulation av användaren
- Online guessing/gissning med förbindelse
- Endpoint Compromise/äventyrande av terminal
- Unauthorized Binding/olovlig anslutning/sammankoppling

4.6.1.3 Typiska hot mot autentiseringsfaktorer

Härnäst ges exempel på hot som är specifika för olika typer av autentisering. Listan är inte heltäckande, utan ger exempel.

Innehavsbaserad autentiseringsfaktor. Tillämpningsanvisningen för förordningen om tillitsnivåer, LOA Guidance [22], avsnitt 1. (2)(a):

> *Typiska attacker mot innehavsbaserade autentiseringsfaktorer är stöld, omspelning eller förfalskning (ändring) samt attacker mot bevis för innehav vid tidpunkten för autentiseringen.*

Tryckt lista med koder. Kopiering, nätfiske, stöld, att utge sig för att vara måltjänsten

SMS OTP. Skadliga program i terminalen, byte av SIM-kort, bristfälligt skydd av SMS-nätslussar, kringgående av telefonlåsningar (SMS syns på skärmen på en låst telefon), nätfiske/bedrägeriwebbplatser, en aktör som utger sig för att vara måltjänsten

Kodkalkylator. Attack via sidokanal (side channel attack), stöld, nätfiske/bedrägeriwebbplatser.

Identifieringsapp. Skadliga program i terminalen, stöld och spionage på faktor som baserar sig på information (exempelvis genom tjuvtittande) eller en dålig biometrisk sensor, kapning av session, en aktör som utger sig för att vara måltjänsten, aktivering eller olovlig koppling av identifieringsapplikation med hjälp av nätfiske

Autentiseringsfaktor som baserar sig på information. Tillämpningsanvisningen för förordningen om tillitsnivåer, LOA Guidance, avsnitt 1. (2)(b):

> *Typiska attacker mot kunskapsbaserade autentiseringsfaktorer är gissande, nätfiske (phishing), avlyssning eller omspelning. Det är typiskt för kunskapsbaserade autentiseringsfaktorer att den person som använder en metod för elektronisk identifiering inte nödvändigtvis ens lägger märke till en attack. Exempel: angrepp som baserar sig på rå styrka eller användning av ordbok, som riktar sig mot lösenord vars entropi är svag och för vilka man inte räknar antalet nya försök; lösenord som kopierats ut brev eller e-postmeddelanden utan att innehavaren eller verifieraren upptäckt det.*

Lösenord/lösenfras. Gissande, utredning, stöld, nätfiske/bluffsidor.

PIN-kod. Gissande, utredning, stöld, nätfiske/bluffsidor.

Faktorer som baserar sig på antagen kunskap (par av frågor och svar). Gissande, utredning, stöld, nätfiske/bluffsidor.

Egenskapsbaserad autentiseringsfaktor Tillämpningsanvisningen för förordningen om tillitsnivåer, LOA Guidance, avsnitt 1.(2)(c):

> *I egenskapsbaserade autentiseringsfaktorer bör det finnas variation även mellan personer med likadana egenskaper, så att identifiering av personen är möjlig; exempel är fingeravtryck, handavtryck, blodkärlen i handflatan, ansiktet, handens geometri och ögats iris. Vid användning av biometriska faktorer är det viktigt att se till att den person som autentiseringsfaktorn anknyter till är fysiskt närvarande på platsen för autentiseringen. På detta sätt minskar man risken för bedrägeri eller omspelning.*

Fingeravtryck. Relativt låg FAR (False Acceptance Rate) på grund av det tekniska genomförandet, kopiering (från ytor, fotografier), skadeprogram, är användaren omedveten.

Ansikte. Relativt låg FAR (False Acceptance Rate) på grund av det tekniska genomförandet, presentationsangrepp.

Baserade på kontinuerlig mätning. Inga anmärkningar.

4.6.1.4 Autentiseringsmekanism

Med autentiseringsmekanism avses de tekniska åtgärder genom vilka man verifierar att användaren innehar, känner till eller har egenskaper som utgör de autentiseringsfaktorer för identifieringsverktyget som är kopplade till användaren. För stark autentisering kräver regelverket dynamisk autentisering, det vill säga att varje identifieringssession måste vara unik och inte får vara möjlig att upprepa.

Som exemplen nedan visar kan hot som berör autentisering inte på ett exakt sätt skiljas från hot som berör autentiseringsfaktorer. De särskilda hoten i autentiseringen anknyter enligt ämbetsverkets bedömning och i ljuset av tillämpningsanvisningen för förordningen om tillitsnivåer åtminstone till datakommunikation.

Tillämpningsanvisningen för förordningen om tillitsnivåer, LOA Guidance [22], avsnitt 1.(3):

> *Det primära syftet med dynamisk autentisering är att minska risken för exempelvis ma-i-mitt -attacker eller risken för att verifieringsuppgifterna från ett tidigare sparat autentiseringstillfälle används på nytt. Här ingår exempelvis följande:*
>
> - *replay-angrepp, det vill säga att autentiseringsuppgifter kapas och används på nytt i en annan autentiseringssituation*
> - *vissa typer av sessionskapningar, exempelvis fall där man helt eller delvis byter två eller flera samtidiga autentiseringssituationer.*
>
> *Man bör komma ihåg att autentisering som baserar sig på flera faktorer inte är detsamma som dynamisk autentisering. I autentisering som baserar sig på flera faktorer krävs inte att autentiseringen sker dynamiskt (exempel är PIN-kod och fingeravtrycksuppgifter), så ett sådant autentiseringssätt kan vara mer sårbart för replay-angrepp än dynamisk autentisering.*
>
> *Dynamisk autentisering kan ske med hjälp av en autentiseringsfaktor (exempelvis en engångsnyckel som fås från enheten) eller en autentiseringsmekanism (exempelvis en dynamisk fråga i utmaning-svar-autentisering).*
>
> *Exempel på dynamiska autentiseringssätt:*
>
> - *ett smartkort som en person innehar, på vilket det finns en privat nyckel som verifieras med en utmaning-svar-metod*
> - *protokoll som baserar sig på tillfälliga Diffie-Hellman-nycklar och ger en ett autentiseringsmedel (exempelvis PACE), tillfällig bildning (nonce), en tidsstämpel och/eller en sifferserie av engångskaraktär.*
> - *protokoll som baserar sig på statiskt bildade tillfälliga DiffieHellman-nycklar, om den förlitande parten ger en tillfällig nyckel (exempelvis utvidgad passerkontroll)*

- *dynamiskt bildade tillträdeskoder för engångsbruk (exempelvis OTP-koder) eller protokoll för utmaning och svar, där engångskoden har producerats tidigare och delats utanför filen och där koden väljs dynamiskt i samband med autentiseringen (exempelvis OTP-kort).*

Om en persons privata nyckel har lagrats som distanstjänst (centraliserat exempelvis på en HSM-enhet som används av en leverantör av identifieringsuppgifter), måste det autentiseringssätt som krävs för användning av den privata nyckeln också vara dynamiskt.

Tillämpningsanvisningen för förordningen om tillitsnivåer, LOA Guidance, avsnitt 2.3.1:

I bedömningen av tåligheten mot angrepp bör man beakta hela autentiseringsmekanismen, även de risker som hänför sig till verifieringen av innehavet av metoden för elektronisk identifiering.

Exempel:

- *Vid tillitsnivån hög räcker det inte med att smartkortet skyddar krypteringsnyckeln mot förfalskningsförsök med hög allvarlighetsnivå, utan även krypteringsprotokollet ska skydda verifieringen av innehavet av nyckeln från förfalsknings- eller omspelningsförsök med hög allvarlighetsnivå.*

- *När det är fråga om en lösenordsidentifierare för engångsbruk där man bildar ett engångslösenord som levereras i en skyddad kanal (exempelvis TLS), påverkas styrkan i en faktor som baserar sig på innehav av identifierarens styrka och den skyddade kanalens styrka.*

- *För tidsbaserad bildare av engångslösenord är verifieringsmekanismen för innehav skickande av det bildade engångslösenordet till verifieraren. Styrkan hos denna mekanism begränsas bland annat av engångslösenordets längd, lösenordets giltighetstid och leveranssättets tillförlitlighet.*

4.6.1.5 Säkerhetsåtgärder

Innehavsbaserad autentiseringsfaktor. Tillämpningsanvisningen för förordningen om tillitsnivåer, LOA Guidance [22], avsnitt 1.(2)(a):

En central säkerhetsegenskap i en innehavsbaserad autentiseringsfaktor (exempelvis ett identifikatorverktyg) är att den specifikt innehas av ägaren. Det förutsätter att kopiering av en autentiseringsfaktor till en tredje part är så svårt och osannolikt att denna risk är obetydlig. Tillitsnivån påverkas av tåligheten mot kopieringförsök.

Exempel: asymmetriska (privata) krypteringsnycklar, privata nycklar som sparats på en särskild enhet (exempelvis ett smartkort), programidentifierare, specifika identifierare (exempelvis SIM-kortet i en mobiltelefon) eller enheter som använder ett engångslösenord (exempelvis en RSA-identifierare eller ett lösenord på ett papperskort.

Tryckt lista med koder. Anvisningar för användaren

SMS OTP. Onåbara för identifieringstjänsten; säkrande av SMS-nätsluss, process för byte av SIM-kort/eSIM. Anvisningar för användaren, visning av den förlitande partens namn för användaren i webbläsargränssnittet

Kodkalkylator. Certifiering, användning av certifierade chips/tekniska lösningar som är motståndskraftiga mot angrepp via sidokanaler, anvisningar för användaren, visning av den förlitande partens namn för användaren i webbläsargränssnittet

Identifieringsapp. Kriterierna i bilaga C till bedömningsanvisningen för identifieringstjänster 211/2019, visning av en identifierare för sessionen för användaren (*session binding*), förmedling av den förlitande partens namn till applikationen, anvisningar för användaren. För att säkerställa innehavet ska man vid aktivering/ikoppling av en ny identifieringsapplikation (instans) beakta att användaren måste informeras via en annan kanal och med bekräftade kontaktuppgifter.

Autentiseringsfaktor som baserar sig på information. Tillämpningsanvisningen för förordningen om tillitsnivåer, LOA Guidance, avsnitt 1.(2)(b):

> *Om information används som autentiseringsfaktor bör man göra det så svårt som möjligt för motparten att gissa informationen i fråga (antingen slumpmässigt eller genom rå kraft/beräkningseffektivitet).*
>
> *Exempel: när informationen är ett lösenord förutsätter ett bra tillvägagångssätt en lämplig lösenordspraxis (se exempelvis BSI IT-Grundschutz-guiden S.2.11 "Provisions concerning the use of passwords" samt NIST 800-63-2, bilaga A, punkterna "Single Token Authentication" och "Password Entropy").*

Lösenord/lösenfras. Anvisningar för användarna, krav på mångsidig sekretess, begränsning av antalet inkorrekta försök

PIN-kod. Anvisningar för användarna, längdkrav, användning av säkerhetsmetoder som erbjuds av applikationen/plattformen i inmatningsskedet, begränsning av antalet inkorrekta försök

Faktorer som baserar sig på antagen kunskap (par av frågor och svar). Anvisningar för användarna, flera par av frågor och svar, frågorna får inte basera sig på information som fås ur andra register eller källor.

Egenskapsbaserad autentiseringsfaktor Tillämpningsanvisningen för förordningen om tillitsnivåer, LOA Guidance, avsnitt 1.(2)(c):

> *I egenskapsbaserade autentiseringsfaktorer bör det finnas variation även mellan personer med likadana egenskaper, så att identifiering av personen är möjlig; exempel är fingeravtryck, handavtryck, blodkärlen i handflatan, ansiktet, handens geometri och ögats iris.*
>
> *Vid användning av biometriska faktorer är det viktigt att se till att den person som autentiseringsfaktorn anknyter till är fysiskt närvarande på platsen för autentiseringen. På detta sätt minskar man risken för bedrägeri eller omspelning.*

I bilaga C till bedömningsanvisningarna för identifieringstjänster 211/2019 finns kriterier för användning av biometriska autentiseringsfaktorer i anslutning till en mobilapplikation. I säkerhetsåtgärderna måste man beakta både applikationens och apparatens egenskaper.

I fråga om faktorer som baserar sig på en *egenskap* måste man försöka bedöma förmågan hos terminalens sensorer och förverkligandet av jämförelsealgoritmerna. Allmänt använda termer, såsom FAR (False Acceptance Rate) och FRR (False Rejection Rate) är indikatorer som används i dagsläget. Den viktigaste av dessa är False Acceptance Rate, som syftar på sannolikheten för att få ett godkänt svar för fel person. Antalet nya försök ökar sannolikheten för att få ett godkänt svar för fel person, så i en faktor som baserar sig på en egenskap måste man även beakta denna effekt genom att begränsa antalet försök. De godkända FAR-värdena ska basera sig på en riskbedömning.

Koder för tillämpningar som baserar sig på egenskaper kan studeras och testas på webbplatsen för NISTs projekt Face Recognition Vendor Test (FRVT) [29], https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt

Det bör noteras att leverantören av identifieringstjänsten i allmänhet inte kan påverka dessa faktorer när man använder terminalens egna gränssnitt. Leverantören av identifieringstjänsten kan närmast utreda och följa upp kvaliteten hos sådana funktioner som den tar i bruk i sitt eget identifieringsmedel.

Exempellista över möjliga säkerhetsåtgärder
- Begränsning av sessionens längd
- Maximalt antal felaktiga försök
- Lösenordets längd och slumpmässighet
- Krav på flera autentiseringsfaktorer
- Toleransgräns för falska positiva (fingeravtryck, ansikte, andra biometriska faktorer)
- Kryptering
- Hantering av hemligheter och säkerhet vid lagring
- Förhindrande av kopiering
- Information till innehavaren av identifieringsverktyget

4.6.1.6 Riskbedömning och angreppspotential

Riskhanteringen är en del av den hantering av risker för identifieringstjänstens informationssäkerhet som krävs enligt bestämmelse 4.2 stycke 3, så identifieringstjänsterna antas redan använda någon riskhanteringsmodell. Krav och eventuella standarder för riskhanteringen behandlas ovan i motiveringarna till bestämmelse 4.

Identifieringsmedlets risktolerans och toleransen för kvarstående risk måste ställas i relation till kravet på skyddsförmåga mot en angreppspotential på en viss nivå.

I tillämpningsanvisningarna för förordningen om tillitsnivåer för elektronisk identifiering nämns två standarder som referens för bedömning av allvarligheten i ett angrepp enligt följande:

Tillämpningsanvisningen för förordningen om tillitsnivåer, LOA guidance [22], avsnitt 2.3.1:

> *De autentiseringsmekanismer som används i autentiseringsskedet kan inte helt förhindra alla angrepp, utan de kan endast stå emot angrepp på vissa säkerhets- eller tillitsnivåer. Det vanliga sättet att mäta vilken tålighet olika mekanismer ger är att ordna mekanismerna enligt hur väl de klarar angrepp av olika allvarlighet (dvs. angriparens kraft).*
>
> *De termer som används för de olika angreppspotentialerna på tillitsnivån är "förhöjd/grundläggande" (enhanced-basic), "måttlig" (moderate) och "hög" (high). Dessa termer har lånats från standarderna ISO/IEC 15408 "Information technology – Security techniques – Evaluation criteria for IT security"* [23] *ja ISO/IEC 18045 "Information technology – Security techniques – Methodology for IT security evaluation"* [24]*. Standardernas text kan läsas fritt på adressen www.commoncriteriaportal.org/cc (CCPART1-3 motsvarar standarden ISO/IEC 15408 och CEM standarden ISO/IEC 18045).*
>
> *I standarden ISO/IEC 15408-1 definieras angreppspotential som den arbetsmängd som ett angrepp [mot en mekanism] kräver, uttryckt som angriparens sakkunskap, resurser och motivation.*

I standarden ISO/IEC 18045 / bilaga B.4 till CEM ges anvisningar för hur man beräknar den angreppspotential som krävs för att utnyttja en viss svaghet i en autentiseringsmekanism.

Uppfyllandet av kraven i genomförandeförordningen förutsätter en bedömning av tåligheten mot eventuella angrepp.

4.6.1.7 Bestämmelse 6.1.2 Autentiseringsfaktorernas oberoende

Bestämmelse 6.1.2 kompletteras med ett preciserat krav på identifieringsmedlets egenskaper och säkerhetsåtgärder för att säkerställa autentiseringsfaktorernas oberoende.

Faktorernas oberoende är en nödvändig säkerhetsåtgärd i synnerhet om olika faktorer används i samma terminal, exempelvis en smarttelefon. Det praktiska förverkligandet av separationen och eventuella säkerhetsåtgärder beror på medeln.

4.6.1.8 Bestämmelse 6.1.3 Krypteringskrav på identifieringsmedel och autentisering

I bestämmelse 6.1.3 preciseras krypteringskraven på identifieringsmedel och autentiseringsmekanismer. Bestämmelsen motsvarar bestämmelse 5.1.2, som definierar hela identifieringssystemets krypteringstekniska kvalitet.

I övrigt finns bestämmelser om kryptering av datakommunikation mellan identifieringstjänster och förlitande parter i bestämmelse 7 och bestämmelser om skydd av meddelanden i bestämmelse 9.

I bestämmelse 6.1.3 preciseras skyddskraven enligt avsnitt 6.1.1 för krypteringslösningarnas del. Enligt bestämmelsen ska man använda lösningar som rekommenderas internationellt eller nationellt. I fastställandet och valet av krypteringslösningar måste man beakta riskbedömningen, precis som vid andra skyddsåtgärder. För datakommunikationens del utgår man i krypteringslösningarna från algoritmerna, förfarandena och värdena enligt bestämmelse 7. Med uttrycket till tekniskt tillämpliga delar avses tekniskt tillämpliga delar i allmänhet. Beaktande av riskbedömningen innebär att andra säkerhetsåtgärder till helheten sett endast delvis kan utgöra en grund för att tillämpa lösningarna enligt bestämmelse 7.

Krypteringsmetoder som är allmänt kända för att vara tillförlitliga ska användas i anslutning till identifieringsverktyg vid

- skapande och upprätthållande av innehavarspecifika hemligheter,
- skydd av en innehavarspecifik hemlighet (vanligen en privat nyckel) i en terminal eller ett bakgrundssystem
- alla funktioner som påverkar identifieringsmedlets integritet och sekretess

Krypteringskraven i bestämmelse 6 på datakommunikation enligt bestämmelse 7 gäller

datakommunikationen mellan identifieringsverktyget som användaren innehar och identifieringssystemet, det vill säga autentiseringen av innehavaren av identifieringsverktyget till de delar som meddelandena inte berörs av kraven på skydd av meddelanden enligt bestämmelse 9. Jämfört med den kryptering av meddelanden som föreskrivs i bestämmelse 9 avser bestämmelse 6.1.3 exempelvis de utmaning-svar-meddelanden som används i verifieringen mellan identifieringsverktygets innehavares och identifieringsverktygets leverantörs system.

- Exempel från bedömningsanvisningen 211/2019 [21], bilaga C på särskilda kriterier för mobilidentifieringslösningar: hard fail certificate pinning mellan mobilapplikationens applikation och bakgrundssystem.

En mobilapplikation som är en del av användarens identifieringsverktyg är i nutida identifieringsmedel i kontakt med identifieringsverktygets leverantörs bakgrundssystem. Om informationssäkerheten för detta föreskrivs i bestämmelse 6. I identifieringsmedel som använder smartkort har användarens verktyg kontakt med identifieringsverktygsleverantörens kortläsarapplikation, som är en del av identifieringssystemet.

Om identifieringsmedlen utvecklas exempelvis enligt modellerna för autonom identitet (Self Sovereign Identity) så att en applikation i användarens terminal (en s.k. plånboksapplikation, wallet) förmedlar identifieringsmeddelanden eller bekräftelser av attribut till förlitande parter, kräver uppfyllandet av kraven sannolikt en ny granskning. Samtidigt blir det sannolikt aktuellt att bedöma ansvaren och förfarandena för verifiering av parterna.

4.6.2 Bestämmelse 6.2 Särskilda säkerhetsåtgärder

4.6.2.1 Bestämmelse 6.2.1 Visning av identifierande information om ärendetransaktionen för användaren (session binding)

Kravet är nytt.

Med identifierande information om en identifieringstransaktion eller ärendetransaktion avses vilken teckensträng, bild eller annan information som helst som visas för användaren av identifieringsverktyget både i identifieringsverktyg och i en ärendehanteringstjänsts applikation eller webblåsarsession (session binding). Med hjälp av informationen kan användaren lätt koppla ihop identifieringsbegäran med ärendetransaktionen. Syftet är att göra det möjligt för användaren av identifieringsverktyget att inte bekräfta eventuella felaktiga eller bedrägliga identifieringsbegäranden.

Kravet gäller naturligtvis endast identifieringsmedel med egen skärm. Exempelvis i kodkalkylatörer är visning i allmänhet inte tekniskt möjlig. Förfarandet har beaktats i kriterierna för mobilapplikationer i bilaga C till bedömningsanvisningen för elektroniska identifieringstjänster 211/2019 (”binding message”).

Informationen som visas kan ha många olika former, såsom teckensträngar, meningar, bilder eller QR-kod. Läsbarheten och begripligheten måste dock beaktas, så att användaren lätt kan associera ärendetransaktionen och identifieringsbegäran med varandra.

I visningen av transaktionens beteckning bör man beakta tillgänglighetskraven i lagen om tillhandahållande av digitala tjänster (306/2019) [30].

Bestämmelsen tar inte ställning till om det är identifieringsförmedlingstjänsten eller leverantören av identifieringsverktyget som är skyldig att visa informationen.

Övergångstid, se bestämmelse 24

4.6.2.2 Bestämmelse 6.2.2 visning av den förlitande partens namn för användaren (SP-name)

Kravet är nytt.

Med information om den förlitande parten avses den ärendehanteringstjänst till vilken bekräftelsen av identifieringen skickas. Föreskriftens syfte är att när namnet på den ärendehanteringstjänst i vilken bekräftelsen på identifiering har begärts och dit den är på väg visas för användaren, har användaren möjlighet att upptäcka och avstå från att bekräfta en eventuell felaktig eller bedräglig identifieringsbegäran.

Detta bidrar till att minska risken för att användaren vilseleds i fråga om vilken ärendehanteringstjänst han eller hon identifierar sig i.

Precis som den identifierande informationen om identifieringsbegäran enligt bestämmelse 6.2.1, kan även informationen om den förlitande parten visas endast i ett sådant identifieringsverktyg som har en skärm.

Genomförandet av identifieringstransaktioner och vilken part i identifieringskedjan som informerar användaren varierar, så det är inte ändamålsenligt att ge bindande föreskrifter för om identifieringsförmedlingstjänsten eller leverantören av identifieringsverktyget ska visa informationen för användaren. I fastställandet av visningen av informationen bör man så komplett som möjligt beakta alla skeden där det är möjligt att visa informationen för användaren. Väsentliga är i synnerhet de skeden i identifieringsprocessen och de användargränssnitt där åtgärder krävs av användaren, såsom fönster för val av identifieringsmedel, eventuella gränssnitt som föreslås av identifieringsförmedlingstjänsten, webbläsarbaserade gränssnitt eller identifieringspplikationer som tillhandahålls av leverantören av identifieringsverktyget eller annan del av identifieringsverktyget eller autentiseringen som möjliggör visning.

I visningen av ärendehanteringstjänstens namn bör man beakta tillgänglighetskraven i lagen om tillhandahållande av digitala tjänster (306/2019) [30].

Informationen definieras som obligatoriskt attribut i gränssnitt mellan ett identifieringsverktyg och en identifieringsförmedlingstjänst i bestämmelse 12.1. Informationen produceras av identifieringsförmedlingstjänsten. Attributet fastställdes redan tidigare, i SAML- och OpenID Connect-gränssnittsrekommendationerna [31, 32] (*ftn_spname*), som frivilligt och 2021 som obligatoriskt, så en del identifieringstjänster kan redan ha beredskapen definierad i gränssnitten.

Övergångstid se bestämmelse 24.

4.6.2.3 Bestämmelse 6.2.3 Samlad inloggning (SSO)

Bestämmelsen är ny.

Erbjudande av samlad inloggning är enligt ämbetsverkets tolkning möjligt i ljuset av autentiseringslagen, så länge en registrerad leverantör av en identifieringstjänst ansvarar för dess säkerhet, tillförlitlighet och överensstämmelse och överensstämmelsen i genomförandet har bedömts.

I bestämmelsen föreskrivs på en allmän nivå om faktorer som anknyter till hanteringen av säkerheten i identifieringsmedlet och autentiseringen, som i synnerhet gäller samlad inloggning. Hit hör åtminstone hantering av sessionernas längd, överföring av sessioner mellan förlitande parter samt avslutande av sessioner, det vill säga engångsutloggning.

I bestämmelse 6.2.3 föreskrivs att kravet enligt bestämmelse 6.2.2 på visning av den förlitande partens namn även gäller de specialsituationer där en identifieringstjänst erbjuder fler än en förlitande part identifiering av innehavaren av ett identifieringsverktyg genom samlad inloggning. För samlad inloggning kan man även använda termen federering.

För användarens del handlar samlad inloggning om att användaren överförs från en förlitande parts ärendehanteringstjänst till en annan förlitande parts ärendehanteringstjänst utan att autentisera sig på nytt, det vill säga utan att på nytt bevisa att han eller hon är den rätta innehavaren av ett starkt elektroniskt identifierings-

verktyg. Enligt bestämmelse 6.2.3 ska användaren vid överföringen ges information om att han eller hon är på väg att överföras till en annan tjänst och information om namnet på tjänsten i fråga, så som förutsätts i bestämmelse 6.2.2. Användaren ska ha möjlighet att godkänna eller avslå överföringen. Obs! Bestämmelse 12.1 4) gäller alltså endast den första förlitande parten. Logguppgifterna för en session som autentiserats genom samlad inloggning måste sparas.

Bestämmelsen tar inte ställning till om identifieringsförmedlingstjänsten eller identifieringsverktyget ska visa informationen för användaren.

Däremot bedömer ämbetsverket att visning av information om identifieringstransaktionen/ärendetransaktionen enligt bestämmelse 6.2.1 (sessions-id, *session binding*) inte är tekniskt möjlig i alla sessioner som är knutna till samlad inloggning, så detta krävs inte i andra än det första skedet i samlad inloggning, det vill säga autentiseringen.

Övriga metoder för styrning. Enkel inloggning har varit förknippad med många juridiska tolkningsfrågor samt informationsutbyte om tekniskt genomförande och säkerhet. Ämbetsverket har gett råd om tolkningar kring dessa frågor och arbetat med de tekniska frågorna tillsammans med identifieringstjänsterna. Detta arbete fortsätter och ämbetsverket överväger ändamålsenliga styrmedel när arbetet framskrider. På grund av identifieringstjänsternas hittills olika synsätt är de medel som närmast verkar vara ändamålsenliga ämbetsverkets *anvisningar, rekommendationer eller tolkningsriktlinjer*.

4.6.3 Bestämmelse 6.3 Koppling av ett identifieringsverktyg till en person

Bestämmelse 6.3.1 är ett grundläggande krav på att autentiseringsfaktorer i identifieringssystemet ska kopplas till innehavaren av identifieringsverktyget, som lagts till i föreskriften för tydlighetens skull.

Kopplingen är naturligtvis olika för olika autentiseringsfaktorer, då exempelvis hanteringen av PIN-koder eller biometriska faktorer skiljer sig från kopplandet av en app eller en kodkalkylator.

Bestämmelse 6.3.2 motsvarar kravet i 6 § i föreskriften från 2016, som preciserade vissa detaljer som hänför sig till tillämpningen vid skapande och beviljande av identifieringsverktyg. De gäller enstaka förfaranden närmast vid beviljande av identifieringsverktyg med vilka säkerställs att verktyget endast används av den verkliga innehavaren. Motsvarande krav har varit i kraft sedan före 2016 genom den tidigare föreskrift 8, men kravet gjordes mer flexibelt år 2016 så att det tillåter olika processer vid beviljande av identifieringsverktyg.

Kravet i bestämmelse 6.3.2 innebär att identifieringsverktyg i regel inte så att säga kan skapas på lager i väntan på eventuella kunder på så sätt att identifieringsverktyget är försett med personuppgifter. Den sökande ska alltså göra en inledande identifiering innan personuppgifterna kombineras med identifieringsverktyget.

Genom bestämmelse 6.3.2 möjliggörs även en sådan process där personuppgifterna kombineras med det ansökta verktyget redan innan den sökande har gjort en inledande identifiering enligt 17 § i autentiseringslagen. Detta kan vara behövligt till exempel om den sökandes inledande identifiering görs vid ett personligt besök och man vill sköta beviljandeprocessen på ett besök. Sådana behov finns av grundad anledning till exempel vid produktion av identifieringscertifikat som Myndigheten för digitalisering och befolkningsdata beviljar personer som befinner sig utomlands.

Tillämpning. Om personuppgifterna kombineras med identifieringsverktyget före inledande identifiering, ska man vid andra sök- och beviljandeprocesser använda säkerhetsåtgärder där man beaktar risken för felaktigt skapade identifieringsverktyg (med fel personuppgifter eller utan avsikt att ansöka om identifieringsverktyg) och risken för att identifieringsverktyget används innan den inledande identifieringen har gjorts. Riskerna kan minimeras genom att kontrollera saken i befolkningsdatasystemet innan personuppgifterna kombineras med verktyget, genom att tekniskt förhindra användningen av identifieringsverktyg före inledande identifiering och genom att kontrollera att de ansökta och beställda identifieringsverktygen motsvarar de levererade.

Som primära skyddsmetoder rekommenderar Transport- och kommunikationsverket att användning av identifieringsverktyget förhindras tekniskt med hjälp av en spärrlista tills alla förutsättningar för beviljande och leverans är uppfyllda. Ett återkallat certifikat får på basis av lagstiftningen inte tas i bruk igen, men detta förbud hindrar inte ett arrangemang där användning av ett certifikat som blivit anhängigt tekniskt är förhindrad och certifikatet aktiveras för användning efter det att den sökande har gjort en inledande identifiering.

Närmare bestämmelser om överlåtelse av identifieringsverktyg till sökande finns i 21 § i autentiseringslagen. Enligt 2.2.2 i EU:s förordning om tillitsnivåer förutsätter identifieringsverktyg på tillitsnivån hög dessutom en separat aktiveringsprocess.

I processen ska man naturligtvis också se till att inledande identifiering hänför sig till beviljande av identifieringsverktyg och att användaren är medveten om det. I detta sammanhang är det också möjligt att tillhandahålla andra tjänster, såsom mobilabonnemang eller banktjänster, och identifiera personen också för dem.

I samband med beviljandet av ett identifieringsverktyg och när verktyget kopplas till en person, rekommenderas det att man försöker kontrollera risken för olovlig koppling exempelvis genom att informera användaren via en annan kanal och använda bekräftade kontaktuppgifter.

4.6.4 Bestämmelse 6.4 Behandling av innehavarspecifika uppgifter i identifieringsmedlet

Genom kraven preciseras vissa detaljer som hänför sig till tillämpningen vid skapande och beviljande av identifieringsverktyg. De gäller enstaka förfaranden närmast vid beviljande av identifieringsverktyg med vilka säkerställs att verktyget endast används av den verkliga innehavaren. Om säkerheten i identifieringsmedlet och -systemet föreskrivs i 8 och 8 a § i autentiseringslagen.

Sådana hemliga uppgifter som avses i bestämmelsen är åtminstone en privat nyckel som hänför sig till identifieringsverktyget och en PIN-kod som behövs för att använda verktyget, ett lösenord eller ett template för en biometrisk autentiseringsfaktor.

Enligt bestämmelse 6.4.1 ska man säkerställa att hemliga uppgifter som hänför sig till ett identifieringsverktyg inte under några omständigheter röjs för personalen hos leverantören av identifieringstjänsten. Kravet var i kraft redan före den föreskrift som gavs 2016.

Ämbetsverket anser att kravet bör bevaras, eftersom man i beviljanderutinerna fortfarande då och då kommer att möta situationer där sekretessbelagda uppgifter såsom PIN-koder kan bli kända för tjänsteleverantörens personal under beviljandeprocessen.

Kravet i bestämmelse 6.4.2 tryggar att endast den som ansöker om (innehar) ett identifieringsverktyg vet eller kan använda de konfidentiella uppgifterna. Med detta säkerställs att ingen annan kan använda identifieringsverktyget.

Kravet innebär i praktiken att till exempel en PIN-kod för ett identifieringsverktyg inte i något skede får röjas för personalen på registreringsstället och att koden inte får förmedlas via sådana datasystem där den blir kopierad, till exempel e-post.

Jfr förordningen om tillitsnivåer för elektronisk identifiering [4]

> 2.2.1/2. *Metoden för elektronisk identifiering är planerad så att den kan antas användas endast om den innehas av den person som den tillhör.*
>
> 2.3.1/2. *Om personidentifieringsuppgifter lagras som en del av autentiseringsmekanismen är dessa uppgifter säkrade för att skydda mot förlust och från att den äventyras, inklusive offline-analys.*
>
> 2.4.6/3. *Tillgången till känsligt krypteringstekniskt material, som används för beviljande och autentisering av metoder för elektronisk identifiering, begränsas strikt till de uppgifter och tillämpningar som kräver sådan tillgång. Man måste säkerställa att sådant material aldrig sparas permanent som klartext. ...Känsligt krypteringstekniskt material, som används för att bevilja och autentisera metoder för elektronisk identifiering, är skyddade mot olovlig hantering.*

4.6.5 Övervägda regleringsalternativ, bestämmelse 6.1 Säkerhetskrav på identifieringsmedlet

I beredningen av bestämmelse 6.1 övervägde man hur man ska specificera säkra eller osäkra autentiseringsfaktorer och identifieringsmedlet som helhet. Alternativen har övervägts och bedömts enligt följande:

a) De autentiseringsfaktorspecifika kraven skulle preciseras i föreskriften

De möjliga autentiseringsfaktorerna som baserar sig på innehav, kunskap eller biometriska egenskaper är väldigt många och olika. För jämförelsens skull har man i PSD2-regelverket fastställt preciserade krav för respektive huvudtyp, exempelvis skydd av innehavsbaserade faktorer mot kopiering.

Sådan reglering skulle på grund av autentiseringsfaktorernas mångsidighet och utveckling inkludera många detaljer som det inte är möjligt eller ändamålsenligt att försöka täcka på bestämmelsenivå. Inte heller hoten mot identifieringsmedlens säkerhet eller säkerhetsåtgärderna för att skydda sig mot hoten är helt specifika för typen av autentiseringsfaktor.

Ett exempel på detta regleringssätt skulle vara att fastställa ett krav på förhindrande av innehavsbaserade autentiseringsfaktorers kopierbarhet och ett krav på att autentiseringsfaktorer som baserar sig på innehav ska basera sig på en kryptografisk hemlighet. Då skulle det vara tydligt att en kodlista av papper inte uppfyller kraven, och man borde i föreskriften även överväga en övergångstid för avslutande av användningen av kodlistor av papper eller stärkande av dem med någon tilläggsfaktor baserad på en kryptografisk hemlighet som skyddar mot kopiering.

I beredningen tillsammans med berörda parter har det framkommit att en del identifieringstjänster fortfarande tänker använda kodlistor av papper som en del av sitt identifieringsmedel, även om användningen av dem håller på att ersättas av mobilapplikationer och kodkalkylatorer. I beredningen har det lyfts fram att exempelvis tillägg av en SMS-bekräftelse till en identifieringstransaktion orsakar kostnader, vilket har kritiserats med tanke på det maximipris som fastställts för identifierings-

transaktioner i förtroendenätet mellan identifieringsverktyg och identifieringsförmedlingstjänster. Transport- och kommunikationsverket har inte kartlagt textmeddelandetjänsternas priser för identifieringstjänster.

b) Kraven på identifieringsmedlets skyddsförmåga skulle preciseras i föreskriften

Motståndskraften mot måttlig eller hög angreppspotential hos autentiseringsmekanismer i identifieringsmedel med tillitsnivån väsentlig respektive hög regleras i autentiseringslagen och förordningen om tillitsnivåer för elektronisk identifiering. I förordningen om tillitsnivåer nämns också typer av hot på bestämmelsens nivå.

Skyddsförmåga mot angreppspotential på måttlig eller hög nivå är en helhet som baserar sig på en kombination av autentiseringsfaktorernas olika säkerhetsegenskaper och identifieringsmedlets säkerhetsåtgärder samt på kontinuerlig uppföljning av föränderliga hot.

Man kan tänka sig att definiera indikatorer för skyddsförmågan eller andra slags preciseringar i föreskriften genom hänvisning till någon allmänt använd riskbedömningsstandard. I tillämpningsanvisningen för förordningen om tillitsnivåer nämns som referens för bedömningen av allvarligheten i ett angrepp *ISO/IEC 15408 "Information technology – Security techniques – Evaluation criteria for IT security"* [23] *ja ISO/IEC 18045 "Information technology – Security techniques – Methodology for IT security evaluation"* [24].

Ämbetsverket anser att det inte finns tillräckligt med kunskap om standardernas tillämplighet för alla identifieringsmedel, som skulle göra det motiverat att hänvisa till dem som förpliktande i föreskriften.

Däremot anser ämbetsverket att kraven på skyddsförmågan kan preciseras i föreskriften genom att lista delfaktorer som måste beaktas i bedömningen.

c) Kraven på hot- och riskbedömningar i identifieringsmedlen preciseras i föreskriften

I tillämpningsanvisningen för EU:s förordning om tillitsnivåer konstateras att de olika faktorerna ska väljas så att de bekämpar olika metoder för hot/angrepp och att man utöver själva faktorerna även bör beakta förfarandet för verifiering av faktorerna. I tillämpningsanvisningen finns också de standardhänvisningar som nämns i föregående avsnitt.

I denna regleringsmodell preciseras kraven på riskbedömningen och de delfaktorer som ska beaktas i den. Autentiseringsfaktorernas och autentiseringsmekanismens risker måste bedömas separat och identifieringsmedlets skyddsförmåga måste basera sig på en hot- och riskbedömning enligt tillitsnivån.

Ämbetsverket bedömer att en sådan modell är tillräckligt flexibel för olika identifieringsmedel och autentiseringsfaktorer och beaktar identifieringsmedlets säkerhetskontroller som helhet. Ämbetsverkets eventuella tillsynslösningar skulle basera sig på en noggrann bedömning av identifieringstjänstens risker, vid vilken man också beaktar effekterna av säkerhetskontroller.

Vid det första hörandet i en workshop den 10 mars 2021 betraktade aktörerna modellen som bra. Det föreslogs att tillämpningsanvisningarna skulle kompletteras med preciseringar utifrån någon allmänt använd riskbedömningsstandard, för att möjliggöra bedömningar av överensstämmelse. Det lyftes också fram att exempelvis metoder för att skydda mot nätfiske kan minska användarkomforten för användaren och att metoderna bör tas i bruk i alla identifieringsverktyg, så att konkurrensen blir

jämlik. Vidare lyftes det fram att riskerna varierar beroende på hur många som använder leverantörens identifieringsverktyg, och att det är mer lockande för kriminella att angripa en stor tjänsteleverantörs användare och medel.

4.6.6 Bestämmelse 6 och autentiseringslagens/förordningens om tillitsnivåer förenlighet med PSD2-reglerna

Om stark autentisering i bank- och betaltjänster finns bestämmelser i PSD2-direktivet [33] och i kommissionens genomförandeförordning som getts med stöd av den (EU) [34]. Nationella bestämmelser om betaltjänster finns i betaltjänstlagen [35].

Regleringen enligt eIDAS-förordningen och autentiseringslagen är däremot branschoberoende, det vill säga neutral i förhållande till i vilken bransch och tjänst identifieringen används.

Regleringen har hittills inte samordnats på EU-nivå.

Många starka elektroniska identifieringsmedel som är registrerade enligt autentiseringslagen används i Finland även för stark autentisering enligt reglerna för betaltjänster. Därmed uppstår frågan om reglernas krav är sinsemellan motstridiga och om samma identifieringsmedel kan erbjudas både för identifiering som är oberoende av verksamhetsområde och i betaltjänstverksamhet, som är föremål för särskilda regler.

År 2018 granskade Transport- och kommunikationsverket (dåvarande Kommunikationsverket) och Finansinspektionen reglernas tekniska kompatibilitet och begärde utlåtanden om bedömningen [36] från Finansinspektionens PSD2-samarbetsgrupp och Kommunikationsverkets eIDAS-arbetsgrupp. **Enligt bedömningen och utlåtandena noterades år 2018 inga hinder för användning av samma identifieringsmedel inom båda regelverken, så länge man alltid följer det striktare eller exaktare av två enskilda krav.**

Efter den gemensamma granskningen år 2018 har Finansinspektionen infört riktlinjen att tryckta listor med blankkoder inte uppfyller kraven i reglerna för betaltjänster utan någon ytterligare bekräftelse. I betaltjänster måste identifieringsmedel där en tryckt lista med koder är en autentiseringsfaktor kompletteras med någon annan faktor utöver kodlistan (och utöver en faktor som baserar sig på innehavarens kunskap eller egenskap). Många banker använder textmeddelande som tilläggsbekräftelse till kodlistan, så att användaren måste visa att han eller hon innehar både kodlistan och en telefonanslutning.

Inför förhandsenkäten om behov av ändringar i föreskriften sammanställde Transport- och kommunikationsverket år 2020 i form av tjänstearbete referensinformation om tillämpningen av förordningen om tillitsnivåer i elektronisk identifiering samt om tillämpningen av och tillämpningsanvisningarna för reglerna kring betaltjänster i syfte att identifiera skillnader mellan regelverken och bedöma skillnadernas konsekvenser. **Varken i jämförelsen eller i branschresponsen under 2020–2021 kom det fram några nya observationer eller andra väsentliga skillnader än bedömningen av tryckta kodlistor.**

4.7 Bestämmelse 7 Krypteringskrav på identifieringssystemets gränssnitt

4.7.1 Bestämmelse 7.1 krypteringsmetoder för datakommunikation

4.7.1.1 Allmänt

I bestämmelse 7.1 definieras krypteringen av datakommunikationen. Syftet är att säkerställa identifieringstransaktionernas integritet och sekretess på datakommunikationens nivå.

Kraven ska tillämpas mellan leverantörer av identifieringstjänster samt mellan leverantörer av identifieringstjänster och förlitande parter, det vill säga ärendehanteringstjänster. Kraven gäller datakommunikation i synnerhet när kommunikationen sker utanför ett skyddat fysiskt utrymme och i icke-betrodda nätverk. Med nätverk som saknar förtroende avses internet, kontorsnät eller andra nät där informationssäkerheten inte har bedömts och säkerställt i omfattande utsträckning.

Tillämpningen av kraven på överföring av information till identifieringssystemets underleverantör fastställs i bestämmelse 5.

De algoritmer, värden och metoder som listas i föreskriften är obligatoriska för föreskriftens användningssyfte inom *”kryptering, nyckelutbyte och underskrifter som anknyter till kryptering...”.* Därmed har man exempelvis inte hittat sådana angrepp mot vissa användningar av SHA-1-algoritmen, som i sig konstaterats vara svag, som skulle förhindra användning av den i dessa fall. Användning av algoritmen rekommenderas inte bland annat eftersom användaren kan ha svårt att bedöma vilka typer av användning som är säkra. I identifieringstjänster har den använts exempelvis för att skapa slumpmässighet, men det skulle vara bra att sluta använda den om det inte enligt en noggrann bedömning är säkert och nödvändigt.

Alternativa regleringssätt, 7.1 kryptering av datakommunikation. Ämbetsverket har vid beredningen av avsnitt 7.1 bedömt det alternativ som föreslagits i responsen från branschen om att förteckningen i föreskriften helt kunde ersättas med en hänvisning till NCSA:s anvisning [37]. Ämbetsverket anser framför allt utifrån sin tillsynserfarenhet att minimikraven fortfarande måste fastslås entydigt. För det andra anser ämbetsverket att NCSA:s och SOGIS MRA:s [38] listor upprätthålls för ett annat syfte och att de till vissa delar kan vara onödigt strikta med tanke på identifiering med tillitsnivån väsentlig. I föreskriftens krav måste man beakta kravnivån för identifieringstjänsternas säkerhet, och kraven knyts inte till en nationell eller internationell kravnivå för säkerhetsklassad information.

4.7.1.2 Bestämmelse 7.1.1 Obligatoriska krypteringsmetoder

Styckena 1–4 i bestämmelse 7.1.1 och deras ordning baserar sig på den typiska planeringsordningen och de typiska kraven för kryptografi.

I den inledande meningen har man för tydlighetens skull lagt till ordet certifikat, eftersom certifikat i praktiken är en nödvändig del av krypteringen av datakommunikation.

I definitionen av säkra förfaranden, algoritmer och värden har man som huvudsaklig källa använt anvisningen *Kryptografiset vahvuusvaatimukset luottamuksellisuuden suojaamiseen - kansalliset suojaustasot (anvisning 28.11.2018, dnr 190/651/2015)*, som publicerats av Transport- och kommunikationsverkets NCSA:s godkännandemyndighet för krypteringsprodukter CAA, för bedömning av krypteringsproduktlösningars säkerhet i situationer där information överförs i nätverk som saknar förtroende. [39]

Målet är en styrka på 112 bitar för tillitsnivån väsentlig.

NCSA (National Communications Security Authority) ansvarar för säkerhetsfrågor som berör elektronisk dataöverföring och -behandling i fråga om säkerhetsklassat material. NCSA-funktionen tjänar som nationell myndighet för godkännande av krypteringsprodukter (*CAA, Crypto Approval Authority*). Till CAA-myndighetens uppgifter hör att utvärdera och godkänna krypteringsprodukter som är avsedda för att skydda säkerhetsklassad information. Uppgiften baserar sig på Europeiska unionens råds säkerhetsbestämmelser (2013/488/EU) och lagen om internationella förpliktelser som gäller informationssäkerhet (588/2004).

Förkortningar som används i föreskriften:

AES = Advanced Encryption Standard (krypteringsmetod)
DH = Diffie-Hellman (protokoll för nyckelutbyte)
DHE = Med DH ephemeral-nycklar
ECDH = Elliptic Curve Diffie-Hellman (protokoll för nyckelutbyte)
ECDHE = Med ECDH ephemeral-nycklar
ECDSA = Elliptic Curve Digital Signature Algorithm (signaturmetod)
EdDSA = Edwards-curve Digital Signature Algorithm (förfarande för underskrifter)
RSA = Rivest-Shamir-Adleman (asymmetrisk krypterings- och signaturmetod)
SHA = Secure Hash Algorithm (hashfunktion)
TLS = Transport Layer Security (krypteringsprotokoll)

Med nyckelutbyte enligt 7.1.1 stycke 1 avses metoder som i sig hör till exempelvis TLS-protokollet. I föreskriften anges närmare de krypteringsmetoder som används vid nyckelutbyte.

Kraven på nyckelutbyte kan uppfyllas genom att använda IANAs (Internet Assigned Numbers Authority) DH-grupper 14–21, 23, 24 och 26 enligt IKEv2-parametrar.

https://www.iana.org/assignments/ikev2-parameters/ikev2-parameters.xhtml
Transform Type 4 - Diffie-Hellman Group Transform IDs [40]

Grunden för 7.1.1 stycke 2) är att RSA är en standard som bedömts och rekommenderats av NCSA och att ECDSA och EdDSA erbjuder motsvarande tillitsnivå. Enligt ämbetsverkets bedömning finns i praktiken inga andra alternativ. EdDSA läggs till i avsnittet. Avsnittet kompletteras med anpassning till asymmetrisk kryptering, eftersom det är fråga om asymmetrisk kryptering när RSA används för kryptering av meddelanden enligt avsnitt 9 i föreskriften.

Krypteringsalgoritmen ChaCha20 har lagts till i 7.1.1 stycke 3). Krypteringsmodulen CCM har lagts till i stycket. Krypteringsmodulen CBC blir kvar i föreskriften. Enligt vissa bedömningsverktyg betraktas den som föråldrad, men ämbetsverket anser att den är tillräckligt säker om man använder korrekta specifikationer och uppdaterade bibliotek. Man bör notera att 3DES togs bort från rekommendationerna redan 2016. Krypteringsmodulen XTS tas bort från stycket, eftersom den inte lämpar sig för kryptering av datakommunikation utan endast för kryptering av skivor.

Autentiseringskoden Poly1305 läggs till i 7.1.1 4). Ämbetsverket bedömer att kombinationen ChaCha20+Poly1305 kan anses tillräckligt säker i samband med identifieringsverksamhet, även om NCSA-FI eller SOGIS MRA inte ännu har fastställt POLY1305 för de syften som referenserna i fråga används för. Tillåtandet av kombinationen möjliggör i större utsträckning än i nuläget användning av olika ICT-tjänster och de senaste lösningarna i dem för identifieringstjänster.

Med SHA-2-funktionen avses funktionerna SHA-224, SHA-256, SHA-384 och SHA-512. Med SHA-3-funktionen avses funktionerna SHA3-224, SHA3-256, SHA3-384 och SHA3-512. Denna precisering flyttas från föreskriften till motiveringarna.

4.7.1.3 Rekommendation om skärpning av avsnitt 7.1.1 i identifieringstjänster med tillitsnivån hög

Rekommendationen från motiveringarna till föreskriften år 2016 om tillämpning av 7 § 1 mom., dvs. avsnitt 7.1 i den ändrade föreskriften, uppdateras. Vissa förenklade förfaranden och värden som listas i föreskriften lämnas bort från rekommendationen. Rekommendationen motsvarar definitionen för säkerhetsklass IV i bedömningsanvisningarna från myndigheten för godkännande av krypteringsprodukter (CAA) [39].

Alternativa regleringssätt, 7.1 med tillitsnivån hög. I beredningen har man övervägt om rekommendationen ska bli kvar i motiveringarna eller om den ska göras till ett tvingande krav på tillitsnivån hög i föreskriften. Ämbetsverket bedömer att det inte skulle uppstå interoperabilitetsproblem om värdena i rekommendationen för tillitsnivån hög gjordes obligatoriska, eftersom det är tekniskt möjligt att välja algoritmer specifikt för en viss transaktion i identifieringsförmedling. Ämbetsverket anser dock att konsekvenserna för förlitande parter som använder identifiering med tillitsnivån hög är svårare att bedöma.

Rekommendation

Obs. Kraven för tillitsnivån hög markeras med **fet stil** i texten, och de krav för tillitsnivån väsentlig som inte räcker för tillitsnivån hög är ~~överstrukna~~.

För tillitsnivån hög i identifieringssystem rekommenderas det att man i stället för de värden som förutsätts för tillitsnivån väsentlig enligt avsnitt 7.1 i föreskriften tillämpar följande värden inom parentes, med vilka man uppnår en styrka på 128 bitar:

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~~ (**4 096** på tillitsnivån hög) bitar i DHE-metoden och minst ~~224~~ (**256** på tillitsnivån hög) bitar i ECDHE-metoden.*

   *DH-grupperna ~~14~~-21, ~~23, 24 och 26~~ (**16~~15~~-21** på tillitsnivån hög) enligt IANAs IKEv2-parametrar uppfyller kraven ovan.*

2) ***Underskrift eller asymmetrisk kryptering:*** *Vid användning av RSA för elektronisk underskrift eller kryptering ska nyckeln utgöra minst ~~2 048~~ (**3 072** på tillitsnivån hög) bitar. Vid användning av ECDSA- eller EdDSA-metoden för elliptisk kurva ska den ändliga kroppen nedan utgöra minst ~~224~~ (**256** på tillitsnivån hög) bitar.*

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

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

*Med SHA-2 avses funktionerna ~~SHA224~~, SHA256, SHA384 och SHA512 (på tillitsnivån hög **SHA-3-256, SHA-3-384, SHA-3-512**.*

5) Utöver de som nämns i avsnitt 1–4 kan man använda metoder och värden som har bedömts som säkra för sådan användning som avses i nämnda avsnitt i följande dokument eller nyare versioner av dessa:

a) Anvisningen Kryptografiset vahvuusvaatimukset luottamuksellisuuden suojaamiseen – kansalliset turvallisuusluokat (Dnr 190/651/2015) [39] 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*) [41].

4.7.1.4 Bestämmelse 7.1.2 Tillåtna krypteringsmetoder bedömda av NSCA och SOGIS MRA

Bestämmelse 7.1.2 är ny.

Enligt den kan man utöva de algoritmer och metoder som listas i 7.1.1 avsnitt 1–4 använda de algoritmer och värden som bedömts som säkra av NCSA eller SOGIS MRA, vilka framgår i de källor som föreskriften hänvisar till. Man ska använda det aktuella och nyaste dokumentet av källorna.

Ämbetsverket betraktar NCSA:s lista som en lämplig källa, och den har även i övrigt använts som grund och referensobjekt när föreskriften har givits. Ämbetsverket betraktar också den lista som upprätthålls av SOGIS MRA som en aktuell och relevant källa.

Syftet med tillägget är att möjliggöra användning av tillförlitliga metoder i situationer där ändringar inte hinner göras i föreskriften tillräckligt snabbt.

4.7.1.5 Bestämmelse 7.13 Tvingande av inställningar

Kravet på tekniskt tvingande avseende krypteringsinställningar i bestämmelse 7.1.3 innebär att sämre standardvärden inte är tillåtna vid konfigurering av system eller att systemet inte får kringgå kraven. Kravet ändras inte.

Standardfunktioner i program och utrustning baserar sig ofta på att operabiliteten stöds flexibelt genom så många alternativa specifikationer som möjligt, men vid kryptering av identifieringssystem ska en svagare inställning förhindras.

4.7.2 Bestämmelse 7.2. Krypteringsprotokoll för datakommunikationen (TLS)

I bestämmelse 7.2 definieras krypteringsprotokoll för datakommunikationen. I avsnittet preciseras kravet endast för TLS-protokollet, eftersom det i praktiken dominerar.

Miniminivån för TLS höjs till TLS 1.2.

Det undantag för TLS 1.1 som tilläts enligt föreskriften från 2016 tillåts inte längre. TLS 1.1 är från 2006 och man känner till sårbarheter i den.

Versionen av TLS-protokollet för datakommunikationsförbindelserna påverkar hur gamla terminaler eller webbläsare användarna kan använda. Ämbetsverket bedömer bland annat utifrån respons från aktörerna att användarnas terminaler i mycket hög utsträckning stöder åtminstone TLS version 1.2. Version TLS 1.3 är också redan i bruk.

Utifrån respons från berörda parter bedömer ämbetsverket att ingen övergångstid för kravet behövs. Uppdatering av TLS-versionen hör till den normala tekniska utvecklingen. Med tanke på utbudet av identifieringstjänster och jämlik konkurrens är det enligt erfarenheterna från den förra regeländringen, det vill säga förbudet mot TLS 1.0, bra att alla är skyldiga att införa ändringen samtidigt.

Om identifieringstjänsten använder något annat protokoll än TLS för att säkerställa datakommunikationens integritet och sekretess (exempelvis IPSec eller SSH), ska genomförandet ge en motsvarande kryptografisk nivå. Ämbetsverket bedömer att det fortfarande inte finns behov av andra gemensamma rutiner än fastställande av TLS i föreskriften.

4.7.3 TLS 1.2 och TLS 1.3 krypteringsprofiler

I detta avsnitt ges råd om vilka chiffersviter som uppfyller kraven i avsnitt 7.1.

Inte alla algoritmer, metoder och värden som nämns i avsnitt 7.1 kan användas i TLS, men man kan plocka kombinationer ur förteckningen till TLS 1.2- och TLS 1.3-profiler. För att krypteringskraven ska uppfyllas i systemet i praktiken ska man, förutom att specificera chiffersviter, också säkerställa att DH-parametrarna och de asymmetriska nycklarna och certifikaten i TLS -konfigurationen är tillräckligt starka.

Chiffersviter som NCSA använder för att bedöma krypteringsprodukter (på nivån TL IV)

- DHE-RSA-AES-128-CBC-SHA256
- DHE-RSA-AES-256-CBC-SHA256
- DHE-RSA-AES-128-GCM-SHA256
- DHE-RSA-AES-256-GCM-SHA384
- ECDHE-RSA-AES-128-CBC-SHA256
- ECDHE-RSA-AES-256-CBC-SHA384
- ECDHE-RSA-AES-128-GCM-SHA256
- ECDHE-RSA-AES-256-GCM-SHA384
- ECDHE-ECDSA-AES-128-CBC-SHA256
- ECDHE-ECDSA-AES-256-CBC-SHA384
- ECDHE-ECDSA-AES-128-GCM-SHA256
- ECDHE-ECDSA-AES-256-GCM-SHA384

Listade i RFC 7905[42]
https://tools.ietf.org/html/rfc7905

- ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256
- ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256
- DHE-RSA-WITH-CHACHA20-POLY1305-SHA256

TLS 1.3 chiffersviter listade i RFC 8446 [43]
https://datatracker.ietf.org/doc/html/rfc8446

- AES-256-GCM-SHA384
- CHACHA20-POLY1305-SHA256
- AES-128-GCM-SHA256
- AES_128_CCM_SHA256

4.7.4 Källor för nationellt eller internationellt rekommenderade krypteringslösningar

- Transport- och kommunikationsverkets NCSA-funktions (National Communications Security Authority, NCSA-FI) kryptografiska krav på styrka för skydd av sekretess – nationella skyddsnivåer (anvisning 28.11.2018 dnr 190/651/2015, på finska) [39]
    - https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/ohje-kryptografiset-vahvuusvaatimukset-kansalliset-suojaustasot.pdf
    - Krypteringslösningar som godkänts av NCSA-funktionen (1.7.2020 dnr 1240/651/2017) [44] https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/NCSA_salausratkaisut.pdf
    - Allmän information om NCSA-FI https://www.kyberturvallisuuskeskus.fi/sv/var-verksamhet/ncsa
- SOGIS-MRA SOGIS Agreed Cryptographic Mechanisms (version 1.2 January 2020) [41]
    - https://www.sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.2.pdf
    - Är för närvarande nyare än NCSA-FI:s lista och innehåller ett flertal algoritmer som inte ännu har godkänts/listats i Finland. Uppdateras vartannat år.
    - Allmän information om SOGIS MRA https://www.sogis.eu/uk/supporting_doc_en.html#:~:text=The%20document%20%C2%AB%20SOG%2DIS%20Crypto,by%20all%20SOG%2DIS%20participants
- IANA (Internet Assigned Numbers Authority)
    - IKEv2-föreskrifterna [40]: http://www.iana.org/assignments/ikev2-parameters/ikev2-parameters.xhtml
    - IANA:s chiffersviter [40]: http://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml#tls-parameters-4
- RFC 7905 ChaCha20-Poly1305 Cipher Suites for Transport Layer Security (TLS) [42]
    - https://tools.ietf.org/html/rfc7905
- RFC 8446 The Transport Layer Security (TLS) Protocol Version 1.3 [43]
    - https://datatracker.ietf.org/doc/html/rfc8446
- eIDAS samarbetsnätverks (Cooperation Network) [45] tekniska specifikation eIDAS Cryptographic Requirements for the Interoperability Framework, TLS and SAML, Version 1.2, 31 August 2019 [46]
    - https://ec.europa.eu/cefdigital/wiki/download/attachments/82773108/eIDAS%20Cryptographic%20Requirement%20v.1.2%20Final.pdf?version=2&modificationDate=1571068651805&api=v2

- Allmän information om eIDAS Cooperation Network: Cooperation Network Resources - eID User Community - CEF Digital (europa.eu)

- ETSI:s standarder och specifikationer
  - Feb 2019 - ETSI TS 119 312 V1.3.1 (2019-02) "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites" [47]
  - https://ec.europa.eu/cefdigital/wiki/display/EIDTECHSUB/Security+Profile+v+1.3

- NIST SP 800-52 Rev. 2, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations [48]
  - https://csrc.nist.gov/publications/detail/sp/800-52/rev-2/final

4.8 Bestämmelse 8 Verifiering av parterna i datakommunikationen

4.8.1 Allmänt

Bestämmelse 8 preciserar och skärper kravet på identifiering av parterna i datakommunikation jämfört med 8.2 § i föreskriften från 2016, utvidgar kravet till kontakter mellan en identifieringstjänst och en förlitande part samt preciserar de grundläggande kraven för nyckelutbyte och uppdatering.

I bestämmelse 8.1 fastställs hur man vid upprättandet av en datakommunikationsförbindelse ska säkerställa att den andra parten är rätt aktör.

I bestämmelse 8.2 föreskrivs det om upprätthållandet av en förtroenderelation i en datakommunikationsförbindelse.

Kraven är desamma mellan aktörerna i förtroendenätet och mellan identifieringstjänsten och den förlitande parten, det vill säga ärendehanteringstjänsten. Autentisering av den förlitande parten är ett centralt sätt att skydda användaren av ett identifieringsverktyg från att bekräfta bedrägliga identifieringsbegäranden.

En förtroenderelation kan tekniskt basera sig på TLS-certifikat som levererats på ett tillförlitligt sätt eller på nycklar som är avsedda för att skydda meddelanden.

Gällande övergångstider se bestämmelse 24.

Övriga metoder för styrning

Anvisning. Hittills har det saknats en myndighetsanvisning för rutinerna för verifiering av parterna och utbyte av nycklar.

Rekommendation. Krav kan läggas till i rekommendationerna för gränssnitten. I enkäten fick man kommentarer om att rekommendationerna inte tillämpas enhetligt. Därför anser ämbetsverket att en anvisning eller rekommendation inte är ett tillräckligt effektivt sätt att säkerställa tillförlitliga rutiner i verifiering av ärendehanteringstjänster.

Samreglering. Man har strävat efter att sammanställa gemensamma rutiner för nyckelbyte i samarbetsgruppen för förtroendenätet. Ämbetsverkets bedömning är att man inte har hittat gemensamma rutiner som alla skulle kunna förbinda sig till.

Identifieringstjänsterna önskar att myndigheten ska slå fast vilka förfaranden som är godtagbara.

Styrning genom information. Har inte granskats.

4.8.2 Bestämmelse 8.1 Identifiering av parterna i en datakommunikationsförbindelse

I bestämmelse 8.1 fastställs hur man vid upprättandet av en datakommunikationsförbindelse ska säkerställa att den andra parten är rätt aktör. Verifieringen av parterna i datakommunikation är en grundläggande del av en tillförlitlig elektronisk identifieringstjänst. Vid elektronisk identifiering måste man se till att datakommunikationen och budskapen är riktiga och förblir konfidentiella.

Ett direkt bilateralt förfarande enligt föreskriften innebär att partens certifikat och krypteringsnycklar måste levereras så att innehavaren uttryckligen kan säkerställas. Föreskriften tar inte uttömmande ställning till detaljerna i förfarandet och vad som är ett tillräckligt sätt att identifiera den andra parten. Exempelvis är användning av stark autentisering en bra praxis. Mellan aktörerna ingås alltid ett avtal, så de praktiska åtgärderna kan kombineras med avtalsprocessen.

Kravet på ett bilateralt förfarande innebär att det befintliga kravet skärps. I verifieringen av parter kan man alltså inte stödja sig endast på de grundläggande rutiner som fastställs i protokollet, utan det krävs särskilda metoder för att säkerställa att ett certifikat för datakommunikation eller nycklar tillhör parten i datakommunikationen.

Bilateralt innebär att identifieringen inte kan basera sig endast på den andra partens certifikat, oberoende av kvaliteten på certifikatet i fråga.

Ämbetsverket anser att ett certifikat i övrigt inte i sig visar att det nyckelpar som det verifierar handhas av rätt innehavare. Certifikatinnehavarens rutiner för nyckelhantering ingår inte i kraven för beviljande av certifikat.

Ämbetsverket bedömer också att även om den CA som beviljar certifikatet och själva certifikatet skulle vara mycket tillförlitliga, kan det i konfigureringen av datakommunikationsförbindelsen i praktiken lätt bli så att det inte säkerställs att endast certifikatet i fråga godkänns, eftersom detta inte är en typisk grundläggande funktion.

Ett TLS-certifikat och en relaterad nyckel eller en nyckel för skydd av meddelanden kan dock levereras undertecknad med en godkänd elektronisk underskrift eller stämplad med en godkänd elektronisk stämpel enligt eIDAS-förordningen. En godkänd elektronisk underskrift och stämpel förutsätter användning av en certifierad anordning för skapande (QSCD, Qualified Signature/Seal Creation Device), och detta säkerställer att de nycklar som används för skapandet av underskriften eller stämpeln innehas av rätt person.

Se eIDAS-förordningen [3]

> Art. 35.2: *2. Till en godkänd elektronisk stämpel kopplas ett antagande om uppgifternas integritet och korrektheten i ursprunget hos de uppgifter som den godkända elektroniska stämpeln är kopplade till.*
>
> Art. 25.2: *2. En kvalificerad elektronisk underskrift ska ha motsvarande rättsliga verkan som en handskriven underskrift.*

För jämförelsens skull konstaterar ämbetsverket att förtroenderelationen under TUPAS-praxisens tid baserades på nyckelutbyte i den verkliga världen. Om praxisen nu i detta avseende ändras så att man litar på certifikat enligt normal datatrafikpraxis, skulle säkerheten inte längre vara på samma tillräckliga nivå. I detta avseende skiljer sig föreskriftens krav från exempelvis PSD2-reglernas krav i verifieringen av betalningsuppdragstjänster och kontoinformationstjänster (s.k. TPP-aktörer, *Third Party Providers*), där man förlitar sig på ett godkänt certifikat för verifiering av webbplatser eller ett godkänt certifikat för elektroniska stämplar enligt eIDAS-förordningen. Ett tilläggskrav i PSD2-reglerna är dock att TPP-aktörerna i fråga är underställda finanssektorns tillsynsmyndighets tillsyn och finns i myndighetens register.

Gällande den *tekniska tillämpningen* konstaterar ämbetsverket att en *jwks_uri*-adress inte i sig räcker för att verifiera en förlitande part vid användning av OpenID Connect-protokollet [49], utan att man också måste använda andra förfaranden. Verifiering av en *jwks_uri*-adress ger inte heller tillräcklig säkerhet om den andra parten, ens om den görs utifrån en fast IP-adress. Även vid användning av SAML-protokollet måste man autentisera signatär av metadata.

4.8.3 Bestämmelse 8.2 Förnyande av certifikat och nycklar

I bestämmelse 8.2 föreskrivs det om upprätthållandet av en förtroenderelation i en datakommunikationsförbindelse. De nycklar för säkerställande av sekretessen och integriteten som tagits i bruk i förfarandet för grundande kan inte gälla permanent, utan måste förnyas regelbundet.

Genom föreskriften preciseras kraven på upprätthållandet av nycklar. I föreskriften fastställs ramar för under vilka förutsättningar man kan använda automatiska förfaranden för förnyandet av nycklar.

Ämbetsverket anser att ett bra tidsspann enligt praxisen för informationssäkerhet är att förnya nycklarna minst vartannat år. Nycklarna måste naturligtvis förnyas oberoende av den regelbundna cykeln, om deras tillförlitlighet har äventyrats på grund av ett informationssäkerhetshot eller en avvikelse.

I bestämmelse 8.2 stycke a–c fastställs alternativa förfaranden genom vilka certifikaten och nycklarna kan förnyas på ett sätt som anses tillräckligt tillförlitligt. Genom dessa förfaranden skapar man alltså förtroendeankare som uppfyller kraven i bestämmelse 8.1. Tidigare nycklar och certifikat måste förstås stödas parallellt så länge som användningen/ibruktagandet av de nya nycklarna och certifikaten kräver det.

8.2 a) enligt det förfarande som beskrivs i punkt 8.1

I 8.2 stycke a) konstateras för tydlighetens skull det i sig självklara alternativet att förnya nycklarna i enlighet med förfarandet för grundande enligt avsnitt 8.1.

I förfarandena enligt avsnitt b och c stöder man sig på det förtroende som byggts upp i samband med grundandet.

8.2. 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

Förfarandet enligt 8.2 b) grundar sig på att man litar på det certifikat som levererats tidigare i det bilaterala förfarandet i grundandeförfarandet och med det verifierar den datakommunikationsförbindelse genom vilken de nya nycklarna levereras. Den tekniska termen för förfarandet är *secure channel,* och de möjliga metoderna för genomförande kan vara *certificate pinning eller key pinning och mutual TLS (mTLS)*. För OSI-modellens del förverkligas förfarandet på transportnivå.

Förfarandet är i sig vanligt och genomförbart i datakommunikation, men det är inte etablerat som standard i datakommunikationsförbindelser. Ämbetsverket lyfter fram att de tekniska konfigurationerna förutsätter omsorg, så att programvaror inte kan kringgå denna härdning.

Gällande den tekniska tillämpningen konstaterar ämbetsverket att certifikatets offentliga nyckel identifierar innehavaren och när en datakommunikationsförbindelse kopplas till denna offentliga nyckel, förverkligar kopplingen integritet och sekretess i datakommunikationsförbindelsen. Det räcker alltså inte att trafiken knyts till en CA, utan detta ska uttryckligen göras för ett visst certifikat eller en viss offentlig nyckel. Det är viktigt att omsorgsfullt skydda och förnya krypteringsmaterialet för certifikat som används för detta syfte.

Effekt. Enligt ämbetsverkets uppfattning används datatrafikförbindelser som verifierats enligt stycke b redan i viss mån inom förtroendenätet, och alternativet kan antas vara möjligt att förverkliga på ett ändamålsenligt sätt mellan identifieringstjänster. Detta alternativ möjliggör automatisering av förnyandet av nycklar som används för att skydda meddelanden.

I verifiering av förlitande parters datakommunikation kan *certificate pinning* vara oändamålsenligt. Däremot kan *key pinning* eller *mTLS* i dessa fall vara möjligt att använda och det kan uppfylla kraven.

I tillämpningar med certificate/key pinning kan ärendehanteringstjänster ofta använda exempelvis förmånliga DV-certifikat av typen Let's Encrypt, som kan bytas ut så ofta som var tredje månad. Även om en förtroenderelation skulle grundas omsorgsfullt enligt bestämmelse 8.1, måste man vid byte av certifikat kunna försäkra sig om att det nya certifikatet beviljas till samma nyckelpar och att den tidigare nyckeln förblir i bruk i den tekniska definitionen.

I tillämpningar med Mutual TLS (mTLS) verifieras parterna i datakommunikationen förutom med servercertifikat även genom identifiering med klientcertifikat (*client authentication*). mTLS är ett alternativt sätt att autentisera parterna i datakommunikation och trygga informationens sekretess och integritet.

De förfaranden för certificate/key pinning eller mTLS som möjliggjorts genom föreskriften möjliggör en automatiserad process för upprätthållandet av nycklar som används för att skydda meddelanden (JWK set).

Fästande (pinning) av TLS-förbindelser och mTLS skiljer sig från varandra i fråga om administrationen. I fästa förbindelser skaffar parterna normalt själva sina egna certifikat, men vid användning av mTLS är det typiskt att den ena parten levererar certifikatet (client certificate) till sin egen kund.

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

Förfarandet enligt 8.2 c) baserar sig på att man litar på den nyckel och det certifikat som levererats tidigare i grundandeförfarandet. Den nya nyckeln undertecknas med

den nyckel som levererats tidigare. För OSI-modellens del genomförs förfarandet på applikationsnivå.

Alternativet är i praktiken inte sannolikt, men ämbetsverket vill tillåta det i föreskriften, så att man inte utesluter genomföranden som kan stöda sig på detta.

Gällande den tekniska tillämpningen konstaterar ämbetsverket att kravet i bestämmelsen förutsätter att jwks-uri-nycklar vid användning av OpenID Connect-protokollet undertecknas med en underskriftsnyckel som levererats enligt bestämmelse 8.1.

Detta torde vara tekniskt möjligt, men standarden innehåller ingen färdig definition för detta förfarande. I beredningen av bestämmelse 8.2 stycke c) har ämbetsverket i synnerhet bedömt möjligheten att genomföra automatiserade uppdateringar. Detta förfarande skulle exempelvis vara undertecknande och kryptering av nya jwks-nycklar enligt 8.2 c) (vid användning av OpenID Connect-protokollet) med betrodda nycklar. Detta är inte ett krav på härdning av programmen, utan skulle kräva att en helt ny funktion byggs i de förlitande parternas system. Delar som anknyter till definitionen skulle i sig finnas, men ett kompatibelt förverkligande skulle kräva samordning och gemensam utveckling.

Enligt ämbetsverkets uppfattning kan förnyelsen alltså inte nödvändigtvis genomföras automatiskt så att verifieringen av en underskrift uttryckligen skulle knytas till en certifikat-/nyckelhelhet som levererats enligt bestämmelse 8.1. Om man ändå kan säkerställa att granskningen uttryckligen knyts till ett certifikat och en nyckel som levererats enligt 8.1, kan förfarandet uppfylla kravet enligt 8.2 c. Om man stöder sig på detta förfarande är det viktigt att detta beaktas i fastställandet och tillämpningen av identifieringsförmedlingstjänstens och den förlitande partens/ärendehanteringstjänstens förfaranden.

Det är osannolikt att de förlitande parterna skulle utföra ett sådant utvecklingsarbete för att fastställa ett förfarande som inte finns färdigt i standarden, där utvecklingsarbetet alltså skulle behöva göras i förtroendenätet. Om förfarandet inte var enhetligt för alla skulle kompatibilitet mellan identifieringstjänsterna och de förlitande parterna inte vara möjlig. Fel och bristande kompatibilitet skulle medföra behov av åtgärder och rådgivning.

Ämbetsverket bedömer att det inte är ändamålsenligt att utarbeta en egen definition av detta för förtroendenätet, eftersom förfarandet är förknippat med en uppenbar risk för interoperabilitetsproblem i praktiken.

Ämbetsverket har kontrollerat om SAML-standarden [50] innehåller en färdig definition för undertecknande av metadata med en nyckel som levererats manuellt.

4.8.4 Sammanfattning av den tekniska tillämpningen av bestämmelse 8.2.

Ämbetsverket bedömer att åtminstone följande alternativ enligt standarden är tillgängliga:

- Krypteringskravet på meddelandenivå och bytet av krypteringsnycklar enligt avsnitt 8.1, om man använder en TLS-skyddad förbindelse där man inte använder certificate eller key pinning.
- man har en TLS-förbindelse som är skyddad från start till slut, med certificate pinning enligt 8.1 (ett visst servercertifikat) eller key pinning eller mTLS, kryptering på meddelandenivå är då inte obligatorisk och bytet av krypteringsnyckel kan automatiseras (JWKS, och nyckelrotation)

- Ett krypteringskrav på meddelandenivå är alltid i kraft när identifieringsmeddelandena återvinns via användarens webbläsare eller terminal (t.ex. SAML front-channel)

Kryptering på meddelandenivå rekommenderas i alla sammanhang där det är möjligt.

4.8.5 Mål och konsekvensbedömning för bestämmelse 8

4.8.5.1 Mål

Syftet med kraven är att säkerställa att identifieringstransaktioner förmedlas inom förtroendenätet och från förtroendenätet endast till tillförlitligt verifierade organisationer. Autentisering av den förlitande parten är ett centralt sätt att skydda användaren av ett identifieringsverktyg från att bekräfta bedrägliga identifieringsbegäranden.

Ett ytterligare syfte är också att säkerställa integriteten och sekretessen i datakommunikation och meddelanden. Vid elektronisk identifiering måste man också se till att datakommunikationen och meddelanden är äkta och förblir konfidentiella.

Syftet är att förtydliga kraven och säkerställa enhetlig användning av säkra metoder oberoende av identifieringstjänst. Kraven har i praktiken varit otydliga och orsakat många tolkningsfrågor och säkerhetsmässigt varierande förfaranden i synnerhet i verifieringen av förlitande parter, det vill säga ärendehanteringstjänster.

Preciseringen av föreskriften förtydligar och förenhetligar i synnerhet förfarandena med förlitande parter. Ämbetsverket bedömer att kraven som helhet kan skärpa de förfaranden som används av vissa aktörer, men målet är att säkerställa kontinuerlig utveckling av säkerheten i identifiering och jämlik konkurrens.

4.8.5.2 Skärpning för grundläggande rutiner för standarder

Verifieringen av parterna i datakommunikation är en grundläggande del av en tillförlitlig elektronisk identifieringstjänst. Genom kravet uppnår man bättre säkerhet än i de grundläggande rutinerna för protokollen, i vilka man litar på vilka certifikat som helst som är allmänt betrodda på internet.

När det gäller den tekniska utvecklingen måste man komma ihåg att praxisen vid användning av TUPAS-protokollet tidigare var att ge den andra parten en gemensam delad nyckel genom något manuellt förfarande i den verkliga världen i samband med att avtalet ingicks. Genom denna praxis kunde man identifiera den andra parten i datakommunikationen på ett tillförlitligt sätt och säkerställa transaktionernas integritet.

Vid en övergång till användning av OIDC- eller SAML-protokollet skulle standarderna innehålla tekniskt standardiserade metoder för att inleda datakommunikation med en ny part. Därför finns det behov av att bedöma om dessa kunde användas för verifiering av parterna i datakommunikationsförbindelser med stark autentisering.

OIDC- och SAML-protokollens grundläggande förfaranden baserar sig på allmän praxis på internet. De möjliggör automatiskt grundande av en förtroenderelation, vilket främjar interoperabiliteten och användbarheten, men tryggar inte *tillräckligt tillförlitlig verifiering av en part* i förtroenderelationen eller integriteten och sekretessen.

Uppfyllande av kraven förutsätter fastställande av processerna för leverans av nycklar och certifikat samt fastställande av olika inställningar i serverprogramvaran såväl i identifieringstjänster som i ärendehanteringstjänster.

Bedömning av alternativet. Ett alternativ som övervägts vid beredningen är att man kunde fastställa certifikat som man kunde lita på utan krav på ett bilateralt leveransförfarande. Exempelvis skulle ett certifikat för verifiering av en webbplats (QWAC) som godkänts enligt eIDAS-förordningen eller certifikat för stämplar (eSeal) eller EV-certifikat ändå vara kostnadsfaktorer, och det är osannolikt att företag skulle skaffa dem. Ämbetsverket bedömer också att nyckelhanteringen ändå inte är garanterad.

Som ovan konstaterats anser ämbetsverket att ett certifikat i övrigt inte i sig visar att det nyckelpar som det verifierar handhas av rätt innehavare. Certifikatinnehavarens rutiner för nyckelhantering ingår inte i kraven för beviljande av certifikat.

Ämbetsverket bedömer också att även om den CA som beviljar certifikatet och själva certifikatet skulle vara mycket tillförlitliga, kan det i konfigureringen av datakommunikationsförbindelsen i praktiken lätt bli så att det inte säkerställs att endast certifikatet i fråga godkänns, eftersom detta inte är en typisk grundläggande funktion.

4.8.5.3 Skillnaden mellan förtroendenätet och förlitande parter

Antalet registrerade identifieringstjänster är begränsat, medan antalet ärendehanteringstjänster som använder identifiering är stort och förhoppningsvis ökar hela tiden. Därför fanns det särskilt behov av att överväga relationen mellan användbarhet och säkerhet och bedöma om det skulle finnas grunder för att använda andra förfaranden med ärendehanteringstjänster än inom ett förtroendenät.

Förmedling av identifieringen till rätt ärendehanteringstjänst är dock en central del av tillförlitligheten i stark autentisering. Transport- och kommunikationsverket har inte identifierat några grunder för att grundandet av en förtroenderelation för en datakommunikationsförbindelse mellan en identifieringsförmedlingstjänst och en ärendehanteringstjänst och förmedling av identifieringstransaktioner inte skulle kräva lika stark tillförlitlighet som datakommunikation inom förtroendenätet. Ämbetsverket har inte heller identifierat kompenserande säkerhetsåtgärder, genom vilka motsvarande effekt skulle kunna uppnås.

I fråga om teknisk beredskap kan identifieringstjänsterna och de ärendehanteringstjänster som använder dem skilja sig åt i betydande grad. I synnerhet hos andra än stora leverantörer av elektroniska ärendehanteringstjänster kan den egna tekniska beredskapen vara liten och de kan vara beroende av tekniska underleverantörer för förverkligandet av elektroniska tjänster. I de följande punkterna bedöms de tekniska krav som uppstår för ärendehanteringstjänster.

4.8.5.4 Grundande av en förtroenderelation och leverans av nycklar

Kravet på bilateralt förfarande enligt bestämmelse 8.1 orsakar behov av ändringar i grundandet av datakommunikationsförbindelser mellan identifieringsförmedlingstjänster och förlitande parter som tillhandahåller elektroniska tjänster som är deras kunder.

I ämbetsverkets gränssnittsrekommendationer 212 och 213 har det angetts som god praxis att undvika att härleda förtroende från en allmänt betrodd CA på internet eller i en webbläsare, men i beredningen av föreskriften har det framkommit att verifie-

ringen av förlitande parter i praktiken ofta görs utifrån ovan beskrivna *jwks-uri*. Kvaliteten på de certifikat som förlitande parter använder varierar mycket i fråga om huruvida fastställandet av certifikatets innehavare baserar sig på dennes egen anmälan eller huruvida beviljaren av certifikatet verifierar innehavaren på något sätt.

Se Transport- och kommunikationsverkets rekommendation 213/2021 S OpenID Connect Protocol Profile for the Finnish Trust Network [32], avsnitt 2.3

The use of extended validation (EV) certificates is RECOMMENDED.

Kravet påverkar framför allt genomförandet av processen för grundande av en förtroenderelation. Processer som är automatiserade eller sköts på distans skulle antagligen vara kostnadseffektivare. För identifieringstjänster ingås dock alltid ett avtal där man avtalar om sådant som gäller leveransen av tjänsten, och i denna process kan även certifikat och nycklar levereras på ett tillförlitligt sätt.

Om man gör ett besök i samband med att avtalet ingås kan man i detta sammanhang även utbyta de nycklar som behövs.

I de flesta fall torde avtal om identifieringstjänster med förlitande parter dock ingås elektroniskt, och då måste man fastställa ett tillräckligt **tillförlitligt elektroniskt sätt att leverera partens offentliga nyckel.** I föreskriften finns ett exempel på ett sätt som anses vara tillförlitligt enligt eIDAS-förordningen. Andra sätt måste övervägas utifrån helheten, så att man beaktar risken för att den levererade informationen är förfalskad eller kommer från fel aktör. Då behövs elektronisk identifiering av den andra parten som en del av processen, och stark autentisering ger bättre tillförlitlighet än andra sätt. Informationsförmedlingskanalens integritet är en annan faktor som ska bedömas. Det är uppenbart att e-post inte är tillräckligt säker, men olika lösningar för krypterad e-post kan trygga tillräcklig integritet och konfidentialitet, om de har förverkligats på ett högklassigt sätt så att avsändaren och mottagaren har identifierats och kommunikationen är krypterad. Även andra elektroniska lösningar för ärendehantering som parterna har tillgång till, såsom skyddade meddelandetjänster inom banktjänster, eller användning av flera kanaler som är oberoende av varandra, kan användas för att förmedla nycklar.

För *tjänster för identifieringsförmedling* bidrar kraven till att de i sina avtalsrelationer med förlitande parter måste sköta informationen om de tekniska kraven, eftersom det inte är sannolikt att dessa känner till dem. I ljuset av autentiseringslagen är det identifieringsförmedlingstjänsten som ansvarar för att den förmedlar identifieringstjänster till förlitande parter i enlighet med kraven. På samma sätt som man har bedömt i fråga om dataskyddsskyldigheterna (den förlitande partens rätt att behandla personuppgifter som överlåts eller bekräftas för den), gäller ansvaret att i avtalet ge akt på hanteringen av kraven och eventuella feltillstånd och medför inte exempelvis en skyldighet att auditera de förlitande parternas datasystem. En identifieringsförmedlingstjänst kan naturligtvis också, om den önskar, erbjuda tekniska tjänster för rådgivning, administration eller installation.

Till avtalsrelationen hör också uppföljning av giltigheten hos de förlitande parternas nycklar, säkerställande av att de förnyas regelbundet samt ibruktagande av nya nycklar i identifieringstjänstleverantörens system. Tekniska granskningar minst en gång vartannat år är enligt ämbetsverkets bedömning i sig på sin plats och en bra rutin.

4.8.5.5 Krav på härdande av den förlitande partens, det vill säga ärendehanteringstjänstens, system

De förlitande parternas eller deras tekniska underleverantörers kunnande kan också variera, och därför måste man även beakta de tekniska krav på kunnande som kravet medför.

Man måste beakta den tekniska genomförbarheten med allmänt tillgängliga tekniska lösningar och program, eventuella kostnader som avviker från normalt ICT-underhåll samt även möjligheten till misstag och mänskliga fel som anknyter till härdandet.

Man måste skilja mellan grundande av en ny förtroenderelation och förnyande av certifikat och nycklar under ett avtalsförhållande.

Grundandeskedet. Den förlitande parten måste kunna beakta att det certifikat eller den offentliga nyckel som den levererar är just den som kommer att användas i användningen av identifieringsförmedlingstjänsten antingen för TLS-kryptering av datakommunikationsförbindelsen eller för undertecknande av identifieringsbegäranden som skickas till identifieringsförmedlingstjänsten och för kryptering på meddelandenivå. Hanteringen av en privat nyckel som är kopplad till en offentlig nyckel i den förlitande partens system måste också vara så omsorgsfull att ingen kan få kännedom om den eller komma över den.

Till grundandeskedet hör även det krav på härdande av den förlitande partens datasystem, enligt vilket TLS-förbindelsens kryptering enligt bestämmelse 7 måste konfigureras så att man endast använder ett visst betrott nyckelpar. Detta förutsätter omsorgsfulla men relativt normala tekniska inställningar i programvarorna.

Om man vill basera säkerheten i uppdateringen av nycklar på verifiering av en TLS-förbindelse enligt 8.2 b), ska TLS-förbindelsens certificate pinning eller key pinning eller mTLS göras uttryckligen för nyckeln eller certifikatet, inte för CA. Detta är ett krav på härdande för den förlitande parten för specifikationer i en programvara, där man i allmänhet litar på någon CA på internet.

Enligt ämbetsverkets uppfattning är certificate eller key pinning eller mTLS i sig ett förfarande som är helt kompatibelt med standarderna. Det mest ändamålsenliga förfarandet för fästande av TLS-förbindelser skulle sannolikt vara key pinning, eftersom det skulle möjliggöra täta byten av certifikat, vilket är karakteristiskt exempelvis för Let's Encrypts certifikat.

Dessa konfigurationer i inledningsskedet är därmed väsentliga. Även om grundandeskedet skulle ha genomförts omsorgsfullt kan det utan härdande gå så att ett omsorgsfullt utbytt certifikat i samband med en automatisk uppdatering byts ut mot ett certifikat som inte granskats, eller att de granskningar som krävs inte görs när datakommunikationsförbindelsen skapas.

Teknisk kravnivå i kraven på härdande och kostnader för de förlitande parterna. De behov av härdande som nämns ovan i 8.1 och 8.2 b är enligt ämbetsverkets uppfattning i sig relativt enkla för den förlitande parten att genomföra, men de kräver att de processer som hör till frågan och underhållet/genomförandeansvaret beaktas i den förlitande partens tekniska underhåll, och de kräver förstås i viss mån ett djupare kunnande utöver grundläggande användning av program. Det är ofta en teknisk underleverantör som ansvarar för det tekniska genomförandet, och identifieringen anknyter till någon större ICT-helhet. Förändringarna orsakar också kostnader för

de förlitande parterna. Autentiseringen av parterna och hanteringen av krypteringsnycklar orsakar alltså vissa kostnader, men dessa torde kunna ses som grundläggande kostnader för ICT-lösningar i identifieringstjänsterna.

Ämbetsverkets bedömning är att ändringarna är tekniskt genomförbara och nödvändiga för den kontinuerliga utvecklingen av säkerheten i stark autentisering. Man måste dock reservera en övergångstid för kravet, särskilt i förhållande till ärendehanteringstjänster, och genomförandet av ändringarna förutsätter samarbete inom rådgivningen och informationen.

4.8.6 Bestämmelse 8.2, bedömning av alternativen för den tekniska tillämpningen

I beredningen av bestämmelse 8.2 har ämbetsverket också bedömt om användning av DNSSEC kunde trygga sekretessen i en datakommunikationsförbindelse och vid användning av OpenID Connect-protokollet JWKS-endpoint-faktorn enligt standarden lika tillförlitligt som om kommunikationen knyts till ett betrott certifikat. DNSSEC är en allmänt taget bra och absolut rekommenderad praxis vid datakommunikation. Om man stödde sig på detta skulle det möjliggöra automatiskt förnyande av nycklar vid användning av OpenID Connect.

Ämbetsverket bedömer dock att sådana exakta tekniska definitioner som säkerheten i genomförandet kräver inte kan säkerställas på ett tillräckligt tillförlitligt sätt, i synnerhet i de förlitande parternas system. Säkert förverkligande skulle förutsätta att man använder DANE och att applikationens (clientens) resolvernamnservrar förutsätts använda DNSSEC-teknik i ett hard fail -läge. För användning av DANE finns det inte nödvändigtvis programvarusupport i någon större utsträckning. Därför har detta förfarande INTE tagits med i alternativen för förfarandet enligt avsnitt 8.2 i föreskriften. (Med härdade specifikationer TLS with DNSSEC, JWT Encryption, Rotation of encryption keys (JWKS)).

Jfr Financial-grade API (FAPI) WG [51] https://openid.net/wg/fapi/

4.9 Bestämmelse 9 Identifieringsmeddelandenas integritet och sekretess

4.9.1 Bestämmelse 9.1 Kryptering av meddelanden mellan identifieringstjänster och en part som förlitar sig på tjänsten

I bestämmelse 9 inkluderas kraven på kryptering av identifieringsmeddelanden enligt 7–9 § i föreskriften från 2016. Kravet preciseras och ändras.

I bestämmelse 9.1 stycke a) fastställs ett alternativt skyddsförfarande vid sidan av kryptering och undertecknande av meddelanden. Det baserar sig på särskilt säkerställande av datakommunikationsförbindelsens sekretess och integritet och är möjligt om meddelandena inte förmedlas via användarens webbläsare eller terminal. Genom detta tillägg görs det kategoriska kravet på kryptering på meddelandenivå från föreskriften år 2016 mer flexibelt.

Enligt bestämmelse 9.1 stycke a) kan man förverkliga integritet och sekretess i identifieringsmeddelandena genom att säkerställa datakommunikationsförbindelsens integritet och sekretess genom att knyta parternas datakommunikation till certifikat som levererats enligt bestämmelse 8 i båda ändarna. På så sätt kan man säkerställa certifikatets tillförlitlighet från början till slut och i båda ändarna av datakommunikationsförbindelsen samt att kommunikationen inte öppnas någon annanstans än i system som anknyter till parternas produktion av identifieringstjänsten.

Förfarandet och kraven på certifikatets tillförlitlighet motsvarar det som anges i avsnitt 8 i föreskriften. En grundläggande förutsättning är naturligtvis att datakommunikationsförbindelsen (”TLS-röret”) är krypterad enligt kraven i avsnitt 7 i föreskriften. Om man använder en tillämpning med IPsec-VPN (virtual private network) i stället för TLS-kryptering för att skydda och kryptera en datakommunikationsförbindelse, måste man utföra motsvarande åtgärder för att skydda sekretessen i meddelandena.

Bedömning av alternativ. Ämbetsverket anser att exempelvis MPLS-förbindelser inte erbjuder tillräckliga säkerhetskontroller för detta syfte, eftersom de inte som regel erbjuder integritet och sekretess. Se Pitukri, [26] avsnitt SA-02: Internet samt MPLS-nät som tillhandahålls av operatörer och exempelvis så kallade svartfibrer (dark fiber) tolkas som offentliga nätverk.

Personuppgifter. Som personuppgifter betraktas med tanke på de allmänna dataskyddsreglerna alla uppgifter som direkt eller indirekt kan kopplas till en person, det vill säga även exempelvis pseudonymer eller transaktionskoder, som kan kopplas till en person när de sammanställts/kombinerats ur olika källor. Av de personuppgifter som används för identifiering berörs personbeteckningen av ett särskilt skydd enligt dataskyddsregelverket. Transport- och kommunikationsverket har dock inte någon objektiv grund för att begränsa skyddet för andra personuppgifter. **Därför fastställer föreskriften inte skyldighet att skydda identifieringsmeddelanden på grund av hurdana personuppgifter de förmedlar** (”*minderårig*" vs. "*121212+999Å, Alma Virtanen*"). Det skulle vara svårt att definiera objektiva och heltäckande grunder för en klassificering av personuppgifter, och det är enklast att göra de tekniska genomförandena på samma sätt för alla identifieringstransaktioner.

4.9.2 Bestämmelse 9.1, effekter och genomförbarhet

Syftet med kravet på skydd av identifieringsmeddelanden är att personuppgifter inte ska röjas utan tillstånd i webbläsaren i användarens terminal eller i servrar. Skyddsmetoderna ska förhindra att datakommunikationen öppnas upp ”på vägen” i en server eller sparas utan kryptering i användarens terminal, vilket kan medföra en risk för att identifieringsmeddelanden och personuppgifter röjs för personer som inte har rätt till dem eller missbrukas.

Krypteringen och undertecknandet av identifieringsmeddelanden i kombination med kraven enligt bestämmelse 8 bidrar också till att skydda identifieringstransaktionen från förfalskning och omspelning (tamper/replay). Vidare bidrar skyddsförfarandet till att säkerställa att bekräftelsen av autentiseringen och personuppgifterna vid autentiseringen endast skickas till rätt ärendehanteringstjänst. Det är därför inte motiverat att skilja mellan kraven inom förtroendenätet och mellan förtroendenätet och ärendehanteringstjänsterna. Kravet gäller både kontakter mellan identifieringstjänster och kontakter mellan identifieringstjänster och förlitande parter.

Föreskriftens krav är fortfarande tekniskt neutralt, men möjligheterna att förverkliga andra skyddsmetoder kan variera mellan olika protokoll (OIDC, SAML, ETSI MSS) och genomföranden. Syftet med ändringen är att bättre beakta egenskaperna hos olika protokoll och standarder. Ändringen ökar flexibiliteten i det tekniska genomförandet vid OIDC-genomföranden och möjliggör också den nuvarande mobilcertifikatlösningen som använder ETSI MSS-standarden [52], som inte bedömdes tillräckligt i beredningen av föreskriften 2016. Vid SAML-genomföranden används användarens webbläsare, så kryptering av meddelandena måste alltid ske där. SAML skulle också möjliggöra andra typer av förverkliganden, som dock inte vanligen torde användas.

4.9.3 Bestämmelse 9.1.2 Undertecknande av identifieringsmeddelanden

Bestämmelse 9.1.2 är ny.

Genom bestämmelse 9.1.2 lägger man till ett krav på att underteckna identifieringsmeddelanden, det vill säga identifieringsbegäranden som den förlitande parten gör till identifieringsförmedlingstjänsten och de svarsmeddelanden som identifieringsförmedlingstjänsten skickar till den förlitande parten.

Kravet gäller endast meddelanden mellan identifieringsförmedlingstjänster och förlitande parter i förtroendenät, det vill säga identifieringsbegäranden och svarsmeddelanden. Syftet är att verifiera att den förlitande partens identifieringsbegäran kommer från rätt system och att verifiera det Spname-attribut som uttrycker den förlitande partens namn, som leverantören av identifieringsförmedlingstjänsten måste verifiera enligt bestämmelse 12.1.

Kravet gäller alltså på applikationsnivå även situationer där man använder en säkerställd datakommunikationsförbindelse enligt 9.1 a) på transportnivå. Syftet är i synnerhet att verifiera de applikationer som begär identifiering från den förlitande partens datasystem.

Kravet definieras inte som obligatoriskt mellan identifieringstjänster i förtroendenätet, eftersom informationssäkerheten i deras system har bedömts som helhet, men det är en bra rutin även där.

Effekt/genomförbarhet. Undertecknandet av förlitande parters identifieringsbegäranden har tagits upp i beredningen av gränssnittsrekommendationer. Detta är enligt den respons som inkommit under beredningen ett förfarande för att öka säkerheten som allmänt efterlyses. Förfarandet är tekniskt sett sedvanligt.

Jfr eIDAS Cryptographic Requirements for the Interoperability Framework, version 1.2 [46]

I fastställandet av tekniska krav för gränsöverskridande identifiering mellan nationella noder används endast SAML-protokollet. I definitionerna har undertecknandet av meddelanden definierats som obligatoriskt medan undertecknande och kryptering av meddelandenas innehåll är valfritt.

3.1. GENERAL REQUIREMENTS

The following rules MUST apply to the SAML communication between eIDAS nodes:
- *SAML request and SAML response messages MUST be signed by the sending party.*
- *The signature of a SAML assertion is OPTIONAL.*
- *The (signed) SAML assertion within the SAML response message MUST be encrypted.*

Ephemeral keys or random numbers (for nonces or generation of ephemeral keys) SHALL be used only once. It is REQUIRED that random numbers to be used within SAML are generated with cryptographically secure random number generators that provide sufficient entropy (according to the security level of 120 bits).

3.2. XML ENCRYPTION WITH SAML

To protect the confidentiality of data, a hybrid crypto system is used. The content MUST be encrypted via symmetric cryptography (Content Encryption) and the corresponding symmetric key (Session Key) MUST be randomly generated for each transmission. A static public key of the receiver MUST be used to encrypt the session key (Key Encryption).

3.2.1 Content Encryption

For content encryption, algorithms of the following list MUST be supported:
- *http://www.w3.org/2009/xmlenc11#aes128-gcm*

• http://www.w3.org/2009/xmlenc11#aes256-gcm
Additionally, the following algorithms MAY be supported:
• http://www.w3.org/2009/xmlenc11#aes192-gcm
Other algorithms than listed above SHALL NOT be used or accepted for content encryption.

4.9.4 Bestämmelse 9.2 Kryptering av meddelanden i användargränssnittet

Syftet med bestämmelse 9.2 är att förtydliga att föreskriftens krav också inverkar på gränssnitt för användarens terminalenhet.

Om användarens webbläsare, en applikation eller terminalen i övrigt används vid förmedling av identifieringsmeddelandet mellan identifieringstjänsten och den förlitande parten, det vill säga ärendehanteringstjänsten, är kryptering av meddelandet fortfarande obligatorisk vid sidan av kryptering av TLS-förbindelsen enligt avsnitt 7.

Användarens webbläsare eller applikationen för tjänsten kan under den elektroniska ärendehanterings- och identifieringstransaktionen vara i kontakt med ärendehanteringstjänsten, identifieringsförmedlingen och den som beviljat identifieringsverktyget. Med tillförlitlig kryptering vill man skydda personuppgifterna i hela processen.

Man bör observera att föreskriften inte gäller gränssnittet mellan den förlitande parten, det vill säga ärendehanteringstjänsten, och användaren, men den förpliktar leverantören av identifieringsverktyget och leverantören av identifieringsförmedlingstjänsten att genomföra sin identifieringstjänst så att de sköter personuppgifternas tillförlitlighet i användarens gränssnitt för terminalenheten.

4.9.5 Bestämmelse 9.3 Krypteringsalgoritmer och metoder

Bestämmelse 9.3 hänvisar till bestämmelse 7.1, som listar säkra algoritmer och metoder. I krypteringen av meddelanden ska man använda de fastställda metoderna till de delar som de lämpar sig tekniskt. Bestämmelse 7.1 har ändrats så att den även gäller kryptering på meddelandenivå.

Gällande den tekniska tillämpningen konstaterar ämbetsverket att en bra rådande praxis är att använda RSAES-OAEP.

Här finns inga tillämpningsexempel för krypteringsmetoderna för meddelanden, men ämbetsverket konstaterar att RFC 7519 vid behov är en bra källa för fastställandet.

RFC 7519 JSON Web Token (JWT) [53] https://tools.ietf.org/html/rfc7519

> *Support for encrypted JWTs is OPTIONAL. If an implementation provides encryption capabilities, of the encryption algorithms specified in [JWA https://tools.ietf.org/html/rfc7519#ref-JWA], only RSAES-PKCS1-v1_5 with 2048-bit keys ("RSA1_5"), AES Key Wrap with 128- and 256-bit keys ("A128KW" and "A256KW"), and the composite authenticated encryption algorithm using AES-CBC and HMAC SHA-2 ("A128CBC-HS256" and "A256CBC-HS512") MUST be implemented by conforming implementations. It is RECOMMENDED that implementations also support using Elliptic Curve Diffie-Hellman Ephemeral Static (ECDH-ES) to agree upon a key used to wrap the Content Encryption Key ("ECDH-ES+A128KW" and "ECDH-ES+A256KW") and AES in Galois/Counter Mode (GCM) with 128- and 256-bit keys ("A128GCM" and "A256GCM"). Support for other algorithms and key sizes is OPTIONAL.*

I ämbetsverkets OIDC-gränssnittsrekommendation 213 [32] finns sedan tidigare följande anvisningar för kryptering på meddelandenivå. Motsvarande finns i rekommendationen för 212 SAML.

Header	Usage	Value	Algorithm	Status in FTN
alg	**JWS**	**RS256**	**RSASSA-PKCS1-v1_5 using SHA-256**	**REQUIRED**
alg	JWS	PS256	RSASSA-PSS using SHA-256 and MGF1 with SHA-256	OPTIONAL
alg	JWS	ES256	ECDSA using P-256 and SHA-256	OPTIONAL
alg	**JWE**	**RSA-OAEP**	**RSAES OAEP using default parameters**	**REQUIRED**
alg	JWE	RSA-OAEP-256	RSAES OAEP using SHA-256 and MGF1 with SHA-256	OPTIONAL
alg	JWE	ECDH-ES	Elliptic Curve Diffie-Hellman Ephemeral Static key agreement using Concat KDF	OPTIONAL
enc	**JWE**	**A128GCM**	**AES GCM using 128-bit key**	**REQUIRED**

4.10 Bestämmelse 10 Krav på informationssäkerhet i gränssnitt för en nationell nod

Med en nationell nod avses ett nationellt gränssnitt som ingår i EU:s interoperabilitetsramverk för elektronisk identifiering. Den nationella noden ska enligt autentiseringslagen upprätthållas av Myndigheten för digitalisering och befolkningsdata. Sådan gränsöverskridande identifiering med anmälda identifieringsverktyg som avses i eIDAS-förordningen ska genomföras via nationella noder.

Bestämmelse 10 föreskriver om att samma krypteringskrav ska iakttas mellan förtroendenätet och den nationella noden som i förtroendenätets övriga interna och externa gränssnitt.

Kraven för gränssnitt mellan nationella noder fastställs i dokumentet *eIDAS - Cryptographic requirements for the Interoperability Framework, TLS and SAML, Version 1.2, 31 August 2019* [46]

https://ec.europa.eu/cefdigital/wiki/download/attachments/82773108/eIDAS%20Cryptographic%20Requirement%20v.1.2%20Final.pdf?version=2&modificationDate=1571068651805&api=v2

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

4.11.1 Bestämmelse 11.1 Betydande hot eller störningar (anmälningströskel)

Genom bestämmelse 11 preciseras kravet enligt 16 § i autentiseringslagen att utan ogrundat dröjsmål anmäla betydande hot eller störningar som berör tjänstens funktion, informationssäkerheten eller användningen av elektronisk identitet till Transport- och kommunikationsverket.

Ämbetsverket har enligt 42 § i autentiseringslagen behörighet att avgöra *när en störning som avses i 16 § är betydande samt anmälans innehåll och form och inlämnandet av den.*

Syftet med anmälan är att stödja ämbetsverkets lägesbild i fråga om tillförlitligheten hos identifieringstjänster samt hot mot och störningar i dem. På basis av uppgifterna bedömer ämbetsverket om man har iakttagit kraven och om det finns behov att informera om läget mer än vad tjänsteleverantören har gjort. Transport- och kommunikationsverket kan också erbjuda information för återhämtning, om sådan information finns att tillgå.

Bestämmelse 11.1 motsvarar i huvudsak 11 § 2 momentet i den tidigare föreskriften. Förtydliganden med anknytning till rutinerna för tillsyn och tillämpning har gjorts i bestämmelsen. Man avser inte att ändra anmälningströskeln eller de uppgifter som ska anmälas, utan endast att förtydliga bestämmelsen.

Avsnitt 11.1 i föreskriften innehåller allmänna bestämmelser om de faktorer som är relevanta med tanke på hur betydande en störning eller ett hot är, det vill säga anmälningströskeln. Sådana betydande störningar är bland annat
– när ett identifieringsverktyg beviljas till fel person
– sådana störningar i spärrfunktions funktion där en uppdaterad spärrlista inte är tillgänglig
- intrång i en tjänsteleverantörs system
– avslöjande av signeringsnycklar för certifikat hos en leverantör av identifieringsverktyg
– allvarliga fall av missbruk av identifieringsverktyg, till exempel fall i anslutning till sammankoppling av identifieringskoder
– allvarliga fall av internt missbruk.

Tröskeln för när fel i eller missbruk av en elektronisk identitet anses vara betydande är mycket låg, och detsamma gäller exempelvis sårbarheter och fel som äventyrar riktigheten i identifieringsuppgiften. Däremot är tröskeln för att anmäla problem i tillgängligheten eller kvaliteten i princip högre och sådana problem är än mer betydande främst på grund av att problemet påverkar andra aktörer i förtroendenätet. Den här typen av problem är sådana långvariga störningssituationer i ett identifieringsverktyg eller en identifieringsförmedlingstjänst som förhindrar förmedling av identifieringstjänster till ärendehanteringstjänster. Även en störning som under en längre tid förhindrar sammankoppling av inledande identifieringar är betydande.

Allmänt taget bedömer ämbetsverket att antalet störningsanmälningar har ökat jämfört med 2016. Ämbetsverket konstaterar att det i detta avseende fortfarande finns stora skillnader i aktörernas förfaranden. Ämbetsverket konstaterar att störningsanmälningar gärna även får göras frivilligt.

Uppgifter som lämnas i en anmälan till Transport- och kommunikationsverket behandlas i enlighet med lagen om offentlighet i myndigheternas verksamhet

(621/1999) och lämnas endast ut till utomstående eller medlemmarna i förtroendenätet på de villkor som fastställs i lagen.

I 16 § i autentiseringslagen finns också bestämmelser om skyldigheten och rätten att göra anmälningar mellan aktörer. Det kan vara nödvändigt att ge information endast till en del av medlemmarna i förtroendenätet. I lagen finns också bestämmelser om Transport- och kommunikationsverkets möjlighet att tekniskt förmedla anmälningar mellan aktörer. Ämbetsverket saknar ett system där det, utan att tekniken i systemet behöver utvecklas, är möjligt att förmedla krypterade data automatiskt mellan aktörer och så att sådana data från fall till fall endast förmedlas till en del medlemmar i förtroendenätet. Transport- och kommunikationsverket upprätthåller en e-postlista genom vilken identifieringstjänster kan informera varandra om frågor som rör störningar, som inte kräver en kanal med bättre informationssäkerhet.

För användningen av meddelanden om störningar och hot som förmedlas inom förtroendenätet har det i 12 a § i autentiseringslagen angetts särskilda begränsningar vars syfte är att sänka informationströskeln mellan leverantörerna av identifieringstjänster.

4.11.2 Bestämmelse 11.2 Uppgifter som ska anmälas

Bestämmelsen motsvarar 11 § 1 mom. i den tidigare föreskriften.

I bestämmelse 11.2 anges de uppgifter som leverantören av identifieringsverktyget eller identifieringsförmedlingstjänsten måste uppge i anmälan till Transport- och kommunikationsverket. I anmälan krävs utöver en beskrivning av störningen eller hotet även information om hur olika aktörer påverkas.

I anmälan bör man uppge tidpunkterna när störningen eller hotet inträffade och upptäcktes samt den uppskattade eller förverkligade längden, om dessa uppgifter är kända.

I den tekniska beskrivningen av händelsen bör framgå vilken del av identifieringssystemet som påverkats av störningen eller hotet, observationer av hur händelsen framskridit, en beskrivning av eventuella andra tjänsteleverantörers delaktighet i händelserna samt information om orsaken till händelsen.

Av anmälan bör det framgå den yttersta orsaken till störningen, dvs. om orsaken till störningen är ett mänskligt fel, fel i system eller program, trasig anläggning, överlastningsangrepp eller annat angrepp eller ett annat externt hot eller naturfenomen.

Om det är fråga om ett hot mot informationssäkerheten ska det i anmälan framgå om det exempelvis är fråga om ett skadligt program, en sårbarhet i programvaran, ett dataintrång eller olovlig användning, ändring eller förfalskning av certifikat eller nyckeltrafik eller något annat motsvarande.

Av beskrivningen av störningen eller hotet och dess verkningar ska det framgå bl.a. om störningen eller hotet har påverkat uppgifternas tillförlitlighet, integritet eller tillgänglighet och om den har äventyrat personuppgifterna.

I anmälan bör man också uppge antalet användare och ärendehanteringstjänster som störningen eller hotet har påverkat. Det lönar sig också att berätta om man vet att störningen eller hotet har påverkat en tjänst eller en funktion som är viktig eller kritisk för samhället.

Vidare ska det av anmälan framgå kort- och långsiktiga åtgärder för avhjälpande som man har vidtagit eller kommer att vidta för att undanröja och lindra störningens eller hotets verkningar och för att förebygga motsvarande situationer.

Av anmälan ska det framgå hur ärendehanteringstjänster, användare och andra leverantörer av identifieringsverktyg och identifieringstjänster i förtroendenätet har informerats om störningen eller hotet. Informationströskeln samt innehållet i och tidpunkten för information till olika parter kan naturligtvis variera. I informationen ska man beakta den informerades möjlighet och behov att skydda sig mot störningens eller hotets verkningar och minimera dess verkningar.

4.11.3 Bestämmelse 11.3 Anmälningsförfarande

Bestämmelsen är ny. Genom den vill man förtydliga det etablerade förfarandet i föreskriften.

Enligt 16 § i autentiseringslagen ska anmälan göras *utan ogrundat dröjsmål*. I föreskriften definieras ingen särskild tidsfrist, men Transport- och kommunikationsverket rekommenderar att hot och störningar som överskrider anmälningströskeln enligt bestämmelse 11.1 anmäls till ämbetsverket senast 1–2 dygn efter att de inträffat eller upptäckts. Ju allvarligare störningen är, desto snabbare bör den anmälas till ämbetsverket.

Eftersom det inte alltid finns fullständiga uppgifter om störningen när störningen upptäcks och man börjar avhjälpa den, kan man först anmäla de omständigheter man har kännedom om och komplettera anmälan senare.

På Transport- och kommunikationsverkets webbplats finns en blankett för anmälning av störningar. Med webblanketten kan man även skicka in sekretessbelagd information, men exakta uppgifter om säkerhet i nätverket bör skickas på annat sätt, exempelvis med krypterad e-post. Anmälan kan också skickas per e-post till eidas@traficom.fi.

I särskilt allvarliga och brådskande störningssituationer kan man anmäla en störning till ämbetsverket per telefon på nummer 0295 390 80. Som allvarliga och brådskande räknas hot eller störningar som innebär att man snabbt måste förebygga skadeverkningar i samhället genom Cybersäkerhetscentrets samordning och information.

4.11.4 Bestämmelse 11, övervägda alternativ och andra metoder för styrning

I svaren på ämbetsverkets enkät om behoven av ändringar i föreskriften framkom en oro över att alla inte anmäler störningar till ämbetsverket med tillräckligt låg tröskel och att alla identifieringstjänster inte informerar varandra om störningar.

Ämbetsverket bedömer att dessa observationer måste påverkas främst genom tillsyn och genom att ytterligare effektivisera den inbördes informationen inom förtroendenätet. Det sistnämnda hör inte till behörigheten att utfärda bestämmelser.

Ämbetsverket anser utifrån responsen inte heller att det är ändamålsenligt eller nödvändigt att införa nya exakta anmälningströsklar för funktionsstörningar i föreskriften, genom vilka man skulle definiera en anmälningströskel för betydande störningar som baserar sig på tid och beräkning av användarantal. Bedömningen ändras inte jämfört med bedömningen från 2016. Det bör också noteras att autentiseringslagen inte innehåller uttryckliga krav på identifieringstjänsternas driftssäkerhet, säkerställande eller beredskap, och att befogenheterna därför inte fastställs enligt dessa.

Anvisning, rekommendation. Inga anmärkningar.

Samreglering. I samarbetsgruppen för förtroendenätet har man utarbetat en praxis för informationsutbyte om störningar och hot mellan aktörerna.

Styrning genom information. Inga anmärkningar.

Kapitel 3 i föreskrifen Identifieringstjänsternas interoperabilitet

4.12 Bestämmelse 12 Minimiuppsättning uppgifter som ska förmedlas i förtroendenätet

4.12.1 Bestämmelse 12.1 Obligatoriska uppgifter (attribut)

4.12.2 Allmänt

I bestämmelsen anges de uppgifter, m.a.o. attribut, som måste förmedlas i en identifieringstransaktion mellan en leverantör av identifieringsverktyg och identifieringsförmedlingstjänst eller där det måste finnas en färdighet för förmedling. Attributen motsvarar de uppgifter som fastställs i EU-kommissionens interoperabilitetsförordning (EU) 2015/1501 [5].

I avsnitt 1–3 i bestämmelse 12.1 i föreskriften anges de identifieringsuppgifter som en leverantör av identifieringsverktyg ska förmedla i identifieringstransaktionen till identifieringsförmedlingstjänsten. Föreskriften har förtydligats genom ett omnämnande i dessa avsnitt om att avsnitt 1 och 2 gäller uppgifter som säkerställts av leverantören av identifieringsverktyget.

Syftet med bestämmelsen är att säkerställa interoperabilitet, det vill säga att leverantörer av identifieringsverktyg och identifieringsförmedlingstjänster smidigt kan komma överens om förmedlingen av identifieringstransaktioner utan att behöva specificera attributen separat för varje avtalsförhållande. Syftet är också att säkerställa att det är möjligt att använda inhemska identifieringsverktyg i gränsöverskridande ärendehantering, om identifieringsverktyg anmäls till EU.

I identifieringstransaktionen för fysiska personer ska det förmedlas en identifikator som identifierar en person och som är antingen en personbeteckning eller en elektronisk kommunikationskod, om bestämmelserna tillåter det. Parterna kommer sinsemellan överens om vilken identifikator som ska användas. I identifieringsuppgifterna ingår också personens för- och efternamn och födelsetid. Enligt 7 § i autentiseringslagen ska leverantörer av identifieringsverktyg hämta och uppdatera de uppgifter som de behöver för tillhandahållandet av identifieringstjänster för fysiska personer med användning av befolkningsdatasystemet. Enligt lagens 6 § ska leverantörer av identifieringstjänster kontrollera sökandens personbeteckning när de kontrollerar sökandens identitet.

Vid identifiering av en juridisk person ska åtminstone följande uppgifter förmedlas: den identifieringsuppgift som identifierar den fysiska personen som företräder den juridiska personen, personens efternamn och förnamn och identifieringsuppgiften om organisationen. Enligt 7 a § i autentiseringslagen ska leverantörer av identifieringsverktyg hämta och uppdatera de uppgifter som de behöver för tillhandahållandet av identifieringstjänster för juridiska personer med användning av företags- och organisationsregistren.

Tillitsnivån för identifieringsverktyg som används i det nationella förtroendenätet kan vara väsentlig eller hög enligt eIDAS-förordningen. Uppgiften om tillitsnivån ska förmedlas via gränssnittet mellan leverantören av identifieringsverktyget och leverantören av tjänsten för identifieringsförmedling.

4.12.3 Nytt attribut: den förlitande partens namn

I bestämmelse 12.1 stycke 4) kompletteras de obligatoriska uppgifterna med information som säkerställts av tjänsten för identifieringsförmedling om parten som förlitar sig på tjänsten, det vill säga ärendehanteringstjänstens namn. I gränssnittsrekommendationerna anges detta attribut med förkortningen SPname, dvs. service provider name.

Syftet är att lägga till ett nytt sätt att säkerställa säkerheten i elektronisk identifiering. Syftet med attributet är att möjliggöra att användaren informeras om den förlitande parten, till vilken bekräftelsen och personuppgifterna ska skickas. I bestämmelse 6.2.2 anges en skyldighet att visa informationen för användaren av identifieringsverktyget.

Informationen om ärendehanteringstjänstens namn fastställs i relationen mellan identifieringsförmedlingstjänsten och den förlitande parten. Med tanke på tillförlitligheten ska ansvaret för attributet ligga hos identifieringsförmedlingstjänsten, eftersom användning av information som tillhandahålls av ärendehanteringstjänsten urvattnar syftet.

I fråga om den tekniska tillämpningen konstaterar ämbetsverket att attributet sedan tidigare har varit definierat i gränssnittsrekommendationerna och att förverkligandet tekniskt sett är problemfritt enligt den information man fått i beredningen. I fastställandet av namn rekommenderas med tanke på användningsbehovet att man använder ett namn utifrån vilket användaren sannolikt kan identifiera tjänsten. Man måste alltså inte nödvändigtvis använda det företagsnamn som finns antecknat i handelsregistret, om företaget använder ett namn för tjänsten som är mer känt.

Namnen måste definieras statiskt i förväg. Säkerställande av korrektheten hos namn som definieras dynamiskt för varje identifieringstransaktion skulle kräva arbetsamma processer och öka risken för fel exempelvis på grund av skrivfel.

Leverantör av identifieringsverktyg. Initiativet till att göra attributet obligatoriskt kom från leverantörerna av identifieringsverktyg i beredningen av föreskriften. Attributet har sedan tidigare varit definierat i gränssnittsrekommendationerna, så en del leverantörer av identifieringsverktyg kan redan ha beredskapen definierad i gränssnitten. För leverantörer av identifieringsverktyg kräver det att ett fält läggs till i de gränssnittsdefinitioner som är i bruk och för användaren att den information som ska ges läggs till i identifieringsbegäran.

I 12 a § 5 mom. i autentiseringslagen finns bestämmelser om användningsbegränsningar för information som fåtts i förtroendenätet och om skadeståndsansvar. Utifrån detta bedömer Transport- och kommunikationsverket att en leverantör av ett identifieringsverktyg inte kan använda den information den fått om identifieringsförmedlingstjänstens ärendehanteringstjänstkund exempelvis för att marknadsföra en egen konkurrerande identifieringsförmedling.

De obligatoriska attributen omfattas enligt 12 b § i autentiseringslagen av reglerna för maximipris för identifieringstransaktioner, men prisregleringen gäller den information som produceras av leverantören av identifieringsverktyget, så den har ingen betydelse i detta fall.

Identifieringsförmedlingstjänst. Identifieringsförmedlingstjänsten producerar SPname-attributet (den förlitande tjänst till vilken identifieringen förmedlas). Avtal måste i vilket fall som helst ingås med ärendehanteringstjänsterna, så fastställandet av tjänstens namn i avtalsförhållandet torde inte orsaka några väsentliga tilläggskostnader. Utöver den innehållsmässiga definitionen förutsätter förändringen att ett

fält läggs till i de gränssnittsdefinitioner som används. Attributet har varit definierat i gränssnittsrekommendationerna, så en del leverantörer av identifieringsförmedlingstjänst kan redan ha beredskapen definierad i gränssnitten.

Ärendehanteringstjänst/förlitande part. Ärendehanteringstjänsten ska tillsammans med identifieringsförmedlingstjänsten fastställa ett namn på sin tjänst som användaren ska informeras om. Detta har inga väsentliga ekonomiska effekter.

Övriga metoder för styrning

Anvisning. Utifrån observationer i tillsynen och respons från enkäten bedömer ämbetsverket att ibruktagande av attribut i alla identifieringstjänster inte nödvändigtvis skulle förverkligas endast genom en anvisning, utan skulle kräva en bindande föreskrift.

Rekommendation. Attributet finns redan i ämbetsverkets rekommendationer för gränssnitt [31, 32]. Dess status blev obligatorisk i en uppdatering av rekommendationerna 2021.

Samreglering. I förtroendenätet kan man vid behov utbyta information om observationer gällande fastställandet av ärendehanteringstjänstens namn och om presentationen av informationen för användaren.

Styrning genom information. Inga anmärkningar.

4.12.4 Bestämmelse12.2 Valfria uppgifter

I bestämmelse 12.2 fastsälls valfria uppgifter. Attributen motsvarar de valfria uppgifter som fastställs i EU-kommissionens interoperabilitetsförordning (EU) 2015/1501 [5].

Gränsöverskridande identifiering skulle behövas redan nu och efterfrågan ökar också inom den privata sektorn. Syftet med icke-obligatoriska attribut är att stöda identifiering och ärendehantering i de situationer där obligatoriska attribut inte är tillräckliga, exempelvis när man kontrollerar om personen sedan tidigare är registrerad i ärendehanteringstjänsten (*identity matching, identity linking*).

I föreskriftens 25 § 4 mom. fastställdes i föreskriftsändringen 2018 en övergångsperiod för beredskap att förmedla icke-obligatoriska attribut som avses i 2 mom. i det gränssnitt som används för förtroendenätet. *Beredskap att förmedla uppgifter enligt föreskriftens 12 § 2 mom. ska vara tekniskt planerad i identifieringssystemet senast den 1 oktober 2018.* Samtidigt kontrollerades då i motiveringarna vad som avses med beredskap i föreskriften.

Bestämmelse 12.2 har kompletterats med en precisering från övergångsbestämmelsen enligt vilken beredskapen ska vara *tekniskt planerad*.

Beredskap att förmedla icke-obligatoriska attribut betyder att behandlingen av icke-obligatoriska attribut måste planeras i gränssnittet och identifieringssystemet så att leverantören av identifieringstjänster har en uppfattning om de tekniska åtgärder som är nödvändiga vid införandet. Den tekniska planeringen förutsätter dokumentation av planen.

Icke-obligatoriska attribut behöver inte genomföras tekniskt i systemen. Vid teknisk konfigurering ska man dock beakta att icke-obligatoriska attribut i identifieringsmeddelanden inte ska störa identifieringstransaktioner även om man inte kommit överens om användningen av dem.

Transport- och kommunikationsverket anser att det är ändamålsenligt att öka beredskapen steg för steg och med beaktande av företagens tidtabeller för utvecklingen av systemen. I det första skedet räcker det att attributen beaktas vid planeringen av identifieringssystemet. Ämbetsverket anser att planeringen vid behov påskyndar användningen. Här kan aktörerna använda ämbetsverkets SAML- och OIDC-specifikationer. Det är inte nödvändigt att föra attributen in i systemen innan det uppstår användningsbehov.

4.12.5 Bestämmelse 12.3. Pseudonymisering av identifiering

Bestämmelsen är ny. Dess syfte är att klargöra attributkraven i gränssnitt mellan tillhandahållarna av identifieringsverktyg och identifieringsförmedling i fall där den förlitande parten, det vill säga ärendehanteringstjänsten, endast får en pseudonymiserad bekräftelse av autentiseringen av användaren.

I autentiseringslagens 8 § 2 mom. sägs att *Bestämmelserna i 1 mom. hindrar inte att specifika tjänster tillhandahålls så att leverantören av identifieringstjänster meddelar den tjänsteleverantör som använder en identifieringstjänst den pseudonym som innehavaren av identifieringsverktyget använder eller endast ett begränsat antal personuppgifter.*

Varken i lagen eller denna föreskrift regleras vilka personuppgifter som ska skickas till den förlitande parten eller verifieras genom stark autentisering. I föreskriften fastställs attribut som behandlas inom förtroendenätet vid autentisering. Till den förlitande parten förmedlas vanligen exempelvis namn och personbeteckning, men på det sätt som beskrivs i lagen kan även exempelvis en pseudonym eller en begränsad mängs personuppgifter förmedlas till den förlitande parten. Även i detta fall ska användaren autentiseras genom stark autentisering och identifieringstransaktionens uppgifter ska sparas enligt lagens 24 §.

I föreskriften används termen pseudonym, eftersom det i fråga om regleringen av personuppgifter enligt ämbetsverkets bedömning är fråga om pseudonymiserade personuppgifter. Även om informationen skulle vara anonym ur den förlitande partens perspektiv på så sätt att den förlitande parten inte nödvändigtvis kan koppla den till en viss person, kan informationen kopplas till personen utifrån de uppgifter som identifieringstjänsterna sparat.

Pseudonymen kan vara av engångsnatur eller mer permanent berodende på hur identifieringstjänsten är utformad. Den förlitande parten kan också få exempelvis en bekräftelse på att användaren är myndig. Vidare kan den förlitande parten få användarens adress eller någon annan enskild personuppgift eller grupp av personuppgifter utan information om personbeteckningen eller bekräftelse av personbeteckningen, som ger möjlighet att identifiera användaren som person.

Transport- och kommunikationsverket bedömer att erbjudande av identifieringstjänster som pseudonymiserats på detta sätt kunde öka antalet situationer där stark autentisering används och säker användning av tjänster även i situationer där den förlitande parten inte har rätt till eller behov av användarens identitet utan endast tillförlitlig autentisering av någon annan information. Enligt den information som fåtts vid beredningen av föreskriften skulle pseudonymisering tekniskt sett vara en ganska trivial sak, men det verkar åtminstone inte hittills finnas någon särskild efterfrågan på en sådan tjänst. För att främja interoperabiliteten är det eventuellt nödvändigt att definiera gemensamma profiler mellan identifieringsverktyg och förmedlingstjänster i förtroendenätet.

Ämbetsverket känner inte till att sådana tjänster skulle finnas, men för jämförelsens skull kan sägas att det enda som såvitt man vet autentiseras säkert exempelvis vid betalning med betalkort mellan betalarens och betalningsmottagaren betaltjänster är att betalaren är innehavare av det betalkort som uppges till betalningsmottagaren, och inga personuppgifter förmedlas mellan betalningstjänsterna.

Användaren måste informeras om behandlingen av personuppgifterna i förtroendenätet och om de uppgifter som ges till den förlitande parten i enlighet med allmänna dataskyddsregler.

Övriga metoder för styrning

Anvisning. Inga anmärkningar.

Rekommendation. Det skulle vid behov vara möjligt att skriva in gemensamma rutiner i Transport- och kommunikationsverkets gränssnittsrekommendationer.

Samreglering. Inom förtroendenätet kan man vid behov utbyta information om förverkligandet av pseudonymisering av information och utarbeta gemensamma modeller.

Styrning genom information. Inga anmärkningar.

4.12.6 Bestämmelse 12, övervägda alternativ

4.12.6.1 Nya valfria attribut

Vid beredningen av föreskriften har man granskat om man borde lägga till nationalitet, födelseland, födelseort, boendeland, telefonnummer och/eller e-postadress i de naturliga valbara attributen. Vidare har man granskat om det finns ett behov av att lägga till telefonnummer och/eller e-postadress i de valfria attributen för juridiska personer.

Nämnda attribut diskuteras i den tekniska eIDAS-arbetsgruppen för gränsöverskridande identifiering. Attributen skulle främja interoperabiliteten i gränsöverskridande identifiering och möjligheten att koppla ihop en person med eventuella tidigare personuppgifter om personen i den ärendehanteringstjänst som tar emot identifieringen.

Attributens källor och möjligheterna till tillförlitlig verifiering av dem varierar. Attributen skulle kunna ha olika tillförlitlighetsnivåer.

Tilläggsuppgifter kan skaffas, verifieras och erbjudas av leverantören av identifieringsverktyget eller av identifieringsförmedlingstjänsten.

I autentiseringslagens 12 b § hänvisas till kommissionens genomförandeförordning (EU) 2015/1501 [5] i fråga om identifierande uppgifter för stark autentisering. Behandlingsgrunderna för andra än dessa personuppgifter och skyldigheterna i fråga om dataskydd ska bedömas och skötas i enlighet med den allmänna dataskyddsförordningen.

Attribut som inte ingår i kommissionens genomförandeförordning omfattas inte av prisregleringen enligt autentiseringslagens 12 c §.

Enligt branschens bedömning är utökande av attributen att vänta i och med utvecklingen av Self Sovereign Identity (SSI)-modeller, och det är viktigt att utvecklingen

inte förhindras. I den nuvarande verksamhetsmodellen ser man dock inget akut behov. I en marknadskartläggning år 2020 framgick det inte heller att ärendehanteringstjänsterna skulle ha några tydligt identifierbara behov av nya attribut.[3]

Riktlinjer. Ämbetsverket gör inga tillägg, eftersom man inte kan se ett sådant behov av nya valbara attribut att fastställandet av dem nu skulle behöva främjas genom föreskriften.

Övriga metoder för styrning

Anvisning. Inga anmärkningar.

Rekommendation. För att möjliggöra interoperabilitet kan valfria attribut och sätten att visa dem listas i gränssnittsrekommendationerna.

Samreglering. Inom förtroendenätet kan man vid behov utbyta information om ärendehanteringstjänsternas attributbehov.

Styrning genom information. Interoperabilitet förutsätter enhetliga gränssnittsspecifikationer. Endast information om attribut som används i olika identifieringstjänster är inte ett fungerande sätt att fastställa en attributlista och ett visningssätt som uppfyller interoperabilitet i en miljö med många aktörer.

4.12.6.2 Attribut för inledande identifiering

I föreskriftsberedningen år 2016 framfördes önskemål gällande utvecklingen på längre sikt om att man ska kunna förmedla uppgifter om inledande identifiering via gränssnittet (t.ex. vad personlig inledande identifiering har grundat sig på: pass, ID-kort, elektronisk identifiering).

I föreskriftsberedningen har man nu bedömt på nytt om uppgifter från ett betrott identifieringsverktyg som förmedlas i sammankoppling av en inledande identifiering behöver läggas till i föreskriften.

Till följd av en ändring av 17 § i autentiseringslagen har leverantörer av identifieringsverktyg i obegränsad omfattning kunnat sammankoppla identifiering, det vill säga skapa nya elektroniska identifieringsverktyg genom att lita på de elektroniska identifikatorer som andra leverantörer tillhandahåller.

I Transport- och kommunikationsverkets gränssnittsrekommendationer har man definierat attributet *FTN chain level* för transaktioner för inledande identifiering. Detta visas i den identifieringsbegäran som en leverantör av ett identifieringsverktyg gör till en annan leverantör av ett identifieringsverktyg. Reglerna förhindrar inte heller att begäran och identifieringen för beviljande av ett nytt identifieringsverktyg förmedlas via en identifieringsförmedlingstjänst.

Ämbetsverket föreslog i beredningen av föreskriften att vissa uppgifter som anknyter till ett betrott identifieringsverktyg skulle definieras som obligatoriska i föreskriften. Enligt ämbetsverkets förhandsbedömning skulle förmedling av uppgifter medföra fördelar med tanke på informationssäkerheten och den allmänna tillförlitligheten i

[3] Se Traficoms undersökningar och utredningar 2/2021 Sähköisen tunnistamisen markkinat, Sähköinen tunnistaminen turvallisen asioinnin mahdollistajana, avsnitt 5.2 Yritysten tarpeet, Sähköisten asiointipalvelujen näkemyksiä tulevaisuuden tarpeista, s. 53 Nästan alla, dvs. 98 procent av de respondenter som gav sin synpunkt, anser att de uppgifter som fås i samband med stark autentisering är tillräckliga.

elektronisk identifiering. På grund av prisregleringen kan användningen av sammankoppling av inledande identifiering antas öka.

Vid utredning av kränkningar av informationssäkerheten är det viktigt att uppgiften om sammankoppling på ett eller annat sätt kan utredas snabbt och effektivt. Om en leverantör av identifieringsverktyg beviljar till exempel identifikatorer utifrån stulna eller falska identitetbevis, ska man kunna utreda om nya identifieringsverktyg har ansökts på elektronisk väg med sådana elektroniska identifieringsverktyg som fel person förfogar över.

De nödvändiga uppgifterna kunde exempelvis vara information om tidpunkten för beviljande av identifieringsverktyget och information om huruvida det betrodda identifieringsverktyget har beviljats utifrån ett dokument som bevisar den sökandes identitet (pass, identitetskort eller före år 2019 körkort) eller utifrån stark autentisering. I fråga om sammankoppling av inledande identifiering framförde ämbetsverket frågan om en eventuell tidigare identifieringskedja behövs och kan förmedlas.

Enligt ämbetsverkets förhandsbedömning skulle de nödvändiga uppgifterna ur teknisk synvinkel finnas färdiga i identifieringssystemet, eftersom uppgifter om den inledande identifieringen måste sparas enligt autentiseringslagens 24 §. Uppfyllande av kraven skulle därmed utöver föreskriften kräva utarbetande av gränssnittsdefinitioner i gränssnittsrekommendationerna och ändringar enligt detta i identifieringstjänstleverantörernas gränssnitt och användning av databaser.

Uppgifter om inledande identifiering och parter som är med i sammankopplingen stöder enligt ämbetsverkets uppfattning riskbedömningen och -hanteringen. Den som litar på en annan leverantörs identifieringsverktyg och beviljar verktyget har utifrån 17 § 4 mom. i autentiseringslagen skadeståndsansvar. Sammankoppling förutsätter därför att den som beviljar verktyget och utnyttjar sammankopplingen bedömer vilken risk som eventuellt är förknippad med den betrodda identifikatorn. Faktorer som påverkar denna risk är (det följande är ett citat från bedömningen år 2016) hur lång tid det har gått efter den ursprungliga personliga identifieringen och vilket identitetsbevis som har använts vid identifieringen, om sammankopplingen omfattar flera parter som beviljar identifieringsverktyg, om någon av dessa parter har upphört med sin verksamhet och om parterna har drabbats av sådana kränkningar av informationssäkerheten som kan ha påverkat uppgifternas integritet.

Leverantörerna av identifieringstjänster har i beredningen av föreskriften framfört sin enhälliga åsikt att det skulle ta lång tid att täcka kostnaderna för specifikation av nya attribut med det fastställda maximipriset på 3 cent för inledande identifiering, att felutredningssituationerna är få och att kostnaderna för specifikationen skulle överskrida nyttan med utredning av fel, samt att utvecklingsarbete skulle krävas för att inhämta, spara och förmedla uppgifterna. Det skulle vara arbetsamt att enhetligt definiera begriplig information. År 2016 och mu på nytt föreslog identifieringstjänsterna att en databas över sammankoppling av inledande identifieringar (dvs. identifieringsverktyg som beviljats till användarna) som upprätthålls av en myndighet, exempelvis Myndigheten för digitalisering och befolkningsdata, skulle uppfylla säkerhetsmålen och möjliggöra stängning av alla sammankopplade identifieringsverktyg.

Riktlinjer. Bestäms inte. Transport- och kommunikationsverket har beaktat aktörernas motiveringar och att störningar i sammankoppling av inledande identifieringar enligt de störningsanmälningar som gjorts till ämbetsverket är mycket ovanliga. Äm-

betsverket ser det också som ändamålsenligt att följa hur statens pågående utvecklingsprojekt för digital identitet eventuellt påverkar inledande elektroniska identifieringar.

Övriga metoder för styrning

Anvisning. Inga anmärkningar.

Rekommendation. Transport- och kommunikationsverket följer upp eventuella störningssituationer och bedömer vid behov om de uppgifter som förmedlas i sammankoppling av inledande identifieringar borde fastslås som frivilliga i gränssnittsrekommendationerna. Enligt den respons som fåtts i beredningen av föreskriften är det dock osannolikt att identifieringstjänsterna skulle förmedla attribut frivilligt.

Samreglering. I störningsgruppen i förtroendenätet kan man vid behov utbyta information och precisera rutinerna i fråga om utredning av störningssituationer.

Styrning genom information. Inga anmärkningar.

4.13 Bestämmelse 13 Uppgifter som förutsätts vid gränsöverskridande identifiering

4.13.1 Identifiering inom den offentliga sektorn

eIDAS-förordningens mål är att identifieringsverktyg som Finland har anmält i framtiden ska kunna användas vid identifiering i utländska offentliga tjänster för ärendehantering och utländska anmälda identifieringsverktyg kan i sin tur i framtiden användas vid identifiering i finländska offentliga tjänster för ärendehantering.

Bestämmelse 13 gäller situationer där en finländsk identifieringstjänst har anmälts till kommissionen i enlighet med eIDAS-förordningen och användaren av identifieringsverktyget identifierar sig med sitt verktyg i en elektronisk tjänst inom en annan medlemsstats offentliga sektor. Identifieringen med ett finländskt verktyg skulle ske från tillhandahållaren av identifieringsverktyget via identifieringsförmedlingstjänsten och den nationella nod som upprätthålls av Myndigheten för digitalisering och befolkningsdata.

I bestämmelse 13 fastställs att de uppgifter som definieras i bestämmelse 12 då ska förmedlas från förtroendenätet till noden. Gränsöverskridande identifiering i offentliga tjänster för ärendehantering ska enligt eIDAS-förordningen vara avgiftsfri mellan medlemsstater. Utifrån eIDAS-förordningen och genomförandebestämmelserna är det dock vid identifiering i privata ärendehanteringstjänster möjligt att ta ut en ersättning för användning av identifieringsverktyg. Därför ska det vara möjligt att också via gränssnittet överföra en uppgift om huruvida identifieringstransaktionen gäller en offentlig eller en privat tjänst för ärendehantering.

Gränssnittet mellan tillhandahållaren av förmedlingstjänsten och noden omfattas enligt bestämmelse 10 av samma allmänna krav som gäller gränssnitt mellan leverantörer av identifieringsverktyg och leverantörer av tjänster för identifieringsförmedling. I övrigt kan leverantören av förmedlingstjänsten och den som skapar noden sinsemellan avtala om gränssnittets egenskaper i enlighet med bestämmelse 14. Visserligen är det ändamålsenligt att som protokoll välja ett protokoll som används i förtroendenätet.

Identifiering med utländska anmälda identifieringsverktyg i en tjänst för en *finländsk offentlig sektor* görs via den nationella noden och via suomi.fi-identifikation. Detta behandlas inte i föreskriften.

4.13.2 Identifiering inom den privata sektorn

13 § 2 mom. i den tidigare föreskriften gällde hanteringen av attribut i situationer där någon med ett utländskt identifieringsverktyg som anmälts i enlighet med eIDAS-förordningen identifierar sig via en nod och ett förtroendenät i en ärendehanteringstjänst inom den privata sektorn i Finland. Denna bestämmelse tas bort från föreskriften.

För användning av en nationell nod för identifiering i *privata ärendehanteringstjänster* finns dock inga enhetliga definitioner på EU-nivå och inte heller några nationella stipulationer i Finland. I den nationella noden förverkligas gränsöverskridande identifiering för ärendehanteringstjänster inom den offentliga förvaltningen, men Myndigheten för digitalisering och befolkningsdata har inte förverkligat eller planerat förmedling av utländsk identifiering till privata ärendehanteringstjänster. Bestämmelsen i föreskriften är därmed överflödig. Ärendet ses över vid behov, om kommande ändringar i eIDAS-förordningen kräver det.

Kunder som använder utländska identifieringsverktyg kan identifieras i finländska tjänster för ärendehantering utifrån avtal på samma sätt som identifiering med finländska identifieringsverktyg i en tjänst för en utländsk privat sektor. Tillförlitligheten i utländska identifieringstjänster kunde konstateras indirekt på basis av anmälningar, eventuell reglering i identifieringstjänstens hemstat eller avtal.

Om en identifieringsförmedlingstjänst som hör till förtroendenätet förmedlar stark autentisering även utomlands, gäller samma krav för gränssnittet och avtalsförhållandet mellan identifieringsförmedlingstjänsten och den utländska ärendehanteringstjänsten som när man vänder sig till inhemska ärendehanteringstjänster. Regleringen och Transport- och kommunikationsverkets tillsyn täcker då kraven i autentiseringslagen och föreskriften för identifieringsförmedlingen. eIDAS-förordningens krav på interoperabilitet och säkerhet vid gränsöverskridande identifiering i kommissionens förordning (EU) 2015/1501 gäller endast den nationella noden.

4.14 Bestämmelse 14 Protokoll som används vid dataöverföring samt övriga krav

4.14.1 Bestämmelse 14.1 Protokoll som används vid dataöverföring

Bestämmelsen har preciserats genom att nämna OpenID Connect och SAML som standarder varav åtminstone någon måste tillämpas på det gränssnitt som identifieringstjänsten ska erbjuda mellan leverantörer av identifieringsverktyg, det vill säga för sammankoppling av inledande identifiering, samt mellan identifieringsverktyget och identifieringsförmedlingstjänsten.

Syftet med bestämmelsen är att precisera kraven gällande interoperabilitet och gränssnittens egenskaper i autentiseringslagens 12 a §, 17 § och statsrådets förordning om förtroendenätet samt begränsa antalet standarder som identifieringstjänsten måste ha beredskap att upprätthålla gränssnitt som motsvarar för att kunna förmedla eller ta emot identifieringsuppgifter vid inledande identifiering eller identifieringsförmedling mellan förlitande parter.

Möjliggörande innebär i bestämmelsen att kravet tolkas med tanke på rätten, som autentiseringslagen och statens förordning är tänkt att trygga för leverantör av identifieringsverktyg eller identifieringsförmedlingstjänst. En identifieringstjänst kan uppfylla sina skyldigheter i förtroendenätet även genom att erbjuda en funktion via ett annat förtroendenäts identifieringstjänst, så länge de angivna och fastställda kraven fortfarande uppfylls.

Enligt de svar som Transport- och kommunikationsverket fick på sin enkät om behov av ändringar i föreskriften år 2020 finns inga stora ändringsbehov i fråga om den tekniska styrningen av gränssnittsprotokoll. De svar man fick på enkäten stödde ämbetsverkets förhandsbedömning att den informativa bestämmelsen i 14 § gärna kan behållas. Det är mest ändamålsenligt att fortsätta förverkliga den detaljerade styrningen av gränssnitt genom rekommendationer. Man fick dock kritiska kommentarer gällande rekommendationernas effektivitet, eller snarare ineffektivitet, i främjandet av interoperabilitet.

Transport- och kommunikationsverket rekommenderar att man använder SAML 2.0- eller OpenID Connect-protokollens nationella profiler, som ämbetsverket publicerade som separata rekommendationer 2018 och uppdaterade 2021 [31, 32]. De särskilda krav som angivits och/eller fastställts nationellt gällande förverkligandet av gränssnitt preciseras i rekommendationerna, och i övrigt bör man tillämpa allmänna goda praxis i efterlevnaden av standarder.

Avtalsfriheten påverkas av regleringen i autentiseringslagen och i statsrådets förordning om förtroendenätet. I autentiseringslagens 12 a § 3 mom. anges att *[l]everantörer av identifieringstjänster ska samarbeta för att säkerställa att de tekniska gränssnitten mellan medlemmarna i förtroendenätet är kompatibla och att de gör det möjligt att tillhandahålla gränssnitt som följer allmänt kända standarder för de förlitande parterna.*

Enligt 1 § 1 mom. i statsrådets förordning 169/2016 (ändrad 1212/2018) [2] *är de tekniska gränssnitt som avses i 12 a § 2 mom. i autentiseringslagen (hänvisningen har inte uppdaterats, men om detta föreskrivs efter ändringen av lagen 12 a § i 12 a § 3 mom.)*
1) gränssnittet mellan leverantörer av identifieringsverktyg,
2) gränssnittet mellan en leverantör av identifieringsverktyg och en leverantör av tjänster för förmedling av identifiering,
3) gränssnittet mellan en leverantör av tjänster för förmedling av identifiering och en part som förlitar sig på identifieringstjänsterna.

Enligt 1 § 3 mom. förordningen ska en leverantör av identifieringstjänster som hör till förtroendenätet i vartdera av de gränssnitt som avses i 1 mom. 1–2 punkten tillhandahålla minst ett tekniskt gränssnitt som baserar sig på en allmänt tillämpad standard.

I föreskriftsberedningen 2016 bedömdes följande frågor: *Med vilken noggrannhet ska kraven på gränssnitt fastställas i föreskriften i förhållande till enskilda protokoll, som SAML och Open ID Connect? Ska med andra ord användning av andra protokoll också möjliggöras? Hur beaktas det rent nationella Tupas-protokollet som inte till alla delar uppfyller kraven och vars utvecklingsplaner eller möjligheter man inte har haft säker kännedom om vid beredningen av föreskriften?*

I föreskriftsberedningen 2016 fastställdes att *vilka protokoll som ska användas fastställs inte, utan aktörerna får avtala om detta själva. Däremot fastställs det resultat som ska uppnås med protokollet, det vill säga den minimiuppsättning uppgifter som ska kunna överföras med hjälp av protokollet, och kraven på informationssäkerhet i gränssnitt.*

Efter 2016 har Tupas-protokollet tagits ur bruk åtminstone för stark autentisering och mobiloperatörerna har i en del gränssnitt övergått till att använda OpenID Connect i stället för det gamla ETSI-gränssnittet för mobilcertifikat. OpenID Connect är även i övrigt det dominerande protokollet, men även SAML används i viss mån.

4.14.2 Bestämmelse 14.2 Gränssnittets övriga egenskaper

Bestämmelsen motsvarar 14 § i den tidigare föreskriften.

Bestämmelsens syfte är att förtydliga att förtroendenätets parter och de förlitande parterna sinsemellan ska avtala om protokollet och de egenskaper hos gränssnittet som inte regleras. Inom förtroendenät har avtalsfriheten begränsats genom reglering för attributens och protokollens del. Avtalsfriheten med de förlitande parterna har begränsats i fråga om gränssnittets säkerhetskrav.

4.14.3 Införande av nya protokollstandarder i förtroendenätet

Ämbetsverket bedömer utifrån information som det fått i beredningen av föreskriften och uppföljning av sektorn att man i den tekniska styrningen för närvarande inte kan se ett behov av att närmare behandla vissa nya protokoll. Inom förtroendenät verkar OpenID Connect och SAML i tillräcklig grad möjliggöra utveckling av identifieringstjänsterna. ETSI används i viss mån i gränssnitt mellan tillhandahållare av mobilcertifikat.

Om det uppstår ett behov av att ta i bruk nya protokoll i form av ett *tekniskt gränssnitt som baserar sig på en allmänt tillämpad standard* som avses i statsrådets förordning om förtroendenätet, utbyter man i beredningen information i en sådan samarbetsgrupp för förtroendenätet som avses i förordningen och ämbetsverket bedömer den tekniska utvecklingens mognad utifrån nationellt och internationellt tillgänglig objektiv information.

De gränssnitts- eller arkitekturbehov för möjliggörande av en autonom identitet (Self Sovereign Identity) som gruppen Findy lyfte fram under beredningen av föreskriften är inte ännu internationellt sett så tydliga eller etablerade (enligt statsrådets förordning om förtroendenätet ”som baserar sig på en allmänt tillämpad standard”) att det skulle vara möjligt eller ändamålsenligt att beakta dem i föreskriften eller den tekniska styrningen. Saken bedöms vid behov på nytt, om ändringar i regleringen på EU-nivå eller nationell nivå eller den tekniska utvecklingen kräver det.

4.14.4 Bestämmelse 14, övervägda alternativ

4.14.4.1 Interoperabilitetskrav som påverkar de förlitande parterna

Transport- och kommunikationsverket har i beredningen av föreskriften utrett om de tekniska specifikationerna för förtroendenätet är förknippade med faktorer som kan påverka möjligheterna att förmedla identifiering till förlitande parter.

I autentiseringslagens 12 a § anges att *man genom samarbete i förtroendenätet ska säkerställa att de tekniska gränssnitten möjliggör tillhandahållande av gränssnitt som följer de allmänt kända standarderna för de förlitande parterna.*

Transport- och kommunikationsverket har i detta sammanhang uppmärksammat åtminstone användningsbegränsningarna för identifieringsverktyg enligt 18 § i autentiseringslagen och de granskningsmöjligheter som leverantören av ett identifieringsverktyg måste ordna för den förlitande parten.

I den enkät som ordnades 2020 om behoven av ändringar i föreskriften och i beredningen av föreskriften framkom dock inga behov som anknöt till de förlitande parterna, förutom tillgången till enkel inloggning.

Transport- och kommunikationsverket har inga observationer av funktioner vars möjliggörande skulle behöva eller kunna främjas genom föreskriften för att främja

interoperabilitet för de förlitande parterna. Villkoren för enkel inloggning som påverkar tjänsterna för förlitande parter och informationssäkert förverkligande behandlas i bestämmelse 6.2.3, och pseudonymisering av identifieringen behandlas i bestämmelse 12.3.

Kapitel 4 i föreskriften Kriterier för bedömning av en identifieringstjänst

4.15 Bestämmelse 15 Bedömningskriterier för överensstämmelse

4.15.1 Bestämmelse 15.1 Funktioner som ska bedömas i identifieringssystemet och identifieringsmedlet

Bestämmelsen motsvarar 15.1 § i den tidigare föreskriften. Genom bestämmelsen preciseras de bedömningsgrunder för identifieringstjänsters överensstämmelse om vilka det finns bestämmelser i autentiseringslagens 29 §.

Alla krav som ställs i lagen och i denna föreskrift. I bestämmelsen förtydligas att bedömningen måste omfatta alla krav som ställs på de funktioner som bedöms enligt autentiseringslagen och föreskriften. Med autentiseringslagen avses också de avsnitt i EU-kommissionens förordning om tillitsnivåer för elektronisk identifiering som lagen hänvisar till. Kraven gällande informationssäkerhet och interoperabilitet preciseras i synnerhet i kapitel 2 och 3 i denna föreskrift.

I bestämmelsen uppräknas de funktioner i genomförandet och tillhandahållandet av identifieringstjänster, där uppfyllandet av de lägstadgade kraven ska visas antingen genom en extern eller genom en intern kvalitetsrevision. Grupperingen av funktioner eller delområden baserar sig på grupperingen av kraven enligt EU-kommissionens förordning om tillitsnivåer. En bedömning av interoperabiliteten enligt den nationella regleringen av förtroendenätet läggs till i föreskriften.

En detaljerad bedömning av och anvisning för vilka angivna och föreskrivna krav bedömningskravet gäller ges i bedömningsanvisningen för elektroniska identifieringstjänster 211/2019. I avsnitt 3 i anvisningen listas relevanta bestämmelser per delområde och i bilaga B om allmänna bedömningskriterier för identifieringstjänster presenteras kraven per område.

Delområdena i bestämmelse 15.1 stycke 1) täcker följande.

Med *ledningen avseende informationssäkerhet* avses kraven i bestämmelse 4 i föreskriften, som preciserar kraven i autentiseringslagens 8 § 1 mom. 5 punkt samt inledningen till avsnitt 2.4 och avsnitten 2.4.3 och 2.4.7 i bilagan till förordningen om tillitsnivåer.

I föreskriften och anvisningen har *förvaring* och övrig *behandling av uppgifter* slagits ihop till en helhet.

Med *anläggningar och personal* avses säkerheten i lokalerna samt personalens kompetens och tillräcklighet enligt autentiseringslagens 8 § 1 mom. 5 punkt och 13 § samt avsnitt 2.4.5 i bilagan till förordningen om tillitsnivåer.

Teknska kontroller (engl. *controls*) omfattar ett brett spektrum av informationssäkerhetsåtgärder genom vilka identifieringssystemets och identifieringsmedlets integritet och sekretess tryggas. Till helheten hör förutom datasystem-, datakommunikations- och användningssäkerhet även krypteringstekniska lösningar samt upptäckande och hantering av avvikelser och information om dem. Informationssäkerheten i identifieringssystem regleras i autentiseringslagens 8 § 1 mom. 4 punkt samt

i avsnitten 2.2.1, 2.3.1 och 2.4.6 i bilagan till förordningen om tillitsnivåer. Anmälningen av störningar regleras i lagens 16 §. I föreskriften gäller de tekniska kontrollerna kapitel 2.

Interoperabilitet i förtroendenätet omfattar förmedling av attribut och gränssnitt. I föreskriften gäller interoperabiliteten kapitel 3.

Relation till ledningssystemet för informationssäkerhet. I bedömningen av överensstämmelse måste man observera att hantering av informationssäkerhet och risker enligt bestämmelse 4 inte räcker för att uppfylla identifieringssystemets materiella krav, utan att identifieringssystemet till alla delar måste uppfylla de angivna och fastställda tekniska kraven. I fråga om bedömning av överensstämmelse innebär detta att endast bedömning av ledningen av informationssäkerhet inte räcker för att visa att de fastställda kraven uppfylls, utan att man uttryckligen måste bedöma om systemet uppfyller exempelvis krypteringskraven för datakommunikation.

Exempelvis standarden ISO 27001 har ett helt annat perspektiv än bedömningsgrunderna enligt autentiseringslagen och denna föreskrift. Ett system för hantering av informationssäkerhet som certifierats enligt ISO-standarderna eller fastställts på annat sätt skapar en administrativ nivå och snarare ramarna för hanteringen av information och administrationen av tjänster, och certifieringen i sig visar inte att nivån på datasäkerheten eller dataskyddet i en enskild tjänst eller alla tjänster inom organisationen är tillräcklig eller att det finns tekniska informationssäkerhetsåtgärder.

Jfr tillämpningsanvisningen för förordningen om tillitsnivåer, LOA guidance, avsnitt 2.4 [22]

> *En allmän princip för riskhanteringen är att organisationen själv måste välja vilken risknivå den anser godtagbar. Genom kravet i avsnitt 2.4 ändras denna allmänna princip, eftersom det föreskriver att organisationens säkerhetsåtgärder ska ställas i relation till riskerna på respektive nivå.*

Delområdena i bestämmelse 15.1 stycke 2) täcker följande. Man bör notera att kraven här beskrivs på en allmän nivå och att olika specialsituationer måste bedömas i ljuset av lagen och dess motiveringar. Gränsdragningen mellan olika åtgärder är inte entydig exempelvis när man endast förnyar en enskild autentiseringsfaktor.

Ansökan om och registrering av ett identifieringsmedel avser ett ansökningsförfarande för identifieringsverktyg samt insamling och granskning av de personuppgifter som behövs för identifieringen i enlighet med 6 § och 7 § i autentiseringslagen.

Autentisering och verifiering av den sökandes identitet innebär en första identifiering av den som ansöker om ett identifieringsverktyg enligt autentiseringslagens 17 §, inklusive bland annat granskning av autenticitet hos tillförlitliga identitetsbevis och säkerställande av deras giltighet enligt lagens 7 b §.

Med *identifieringsmedlets egenskaper och utformning* avses val av de autentiseringsfaktorer som ska användas i identifieringsmedlet samt de egenskaper av autentiseringsfaktorer och autentiseringsmekanism som tryggar medlets tillförlitlighet som helhet enligt autentiseringslagens 8 a § och 8 § 1 mom. 4 punkt samt avsnitt 2.2.1 och 2.3.1 enligt bilagan till förordningen om tillitsnivåer.

Med *utfärdandet, leverans och aktivering* av ett identifieringsmedel avses förfaranden och åtgärder enligt autentiseringslagens 20 § och 21 § samt avsnitt 2.2.2 i bilagan till förordningen om tillitsnivåer, genom vilka identifieringsverktyget kopplas till innehavaren samt förmedlas till innehavaren och tas i bruk.

Med avbrytande av giltigheten, återkallande och återaktivering avses stängningstjänster och -åtgärder enligt autentiseringslagens 25 § och 26 § på innehavarens eller identifieringstjänstens initiativ.

Med *förnyelse och ersättning* avses att ett identifieringsverktyg levereras i stället för ett tidigare i enlighet med autentiseringslagens 22 § och avsnitt 2.2.4 i bilagan till förordningen om tillitsnivåer. Leveransen kan också anknyta till tillämpning av lagens 26 §.

Med *autentiseringsmekanism* avses identifieringsverktygets innehavares autentiseringsförfarande enligt autentiseringslagens 8 a § och genom dynamisk autentisering enligt avsnitt 2.3.1 i bilagan till förordningen om tillitsnivåer. Kraven på autentiseringsmekanismen gäller också identifieringsförmedlingstjänsten, när den deltar i förmedlandet av meddelanden vid autentisering.

4.15.2 Bestämmelse 15.2 Bedömningskriterier

Bestämmelsen förtydligas för att bättre beskriva syftet och den etablerade tillsynspraxisen.

I autentiseringslagens 29 § sägs det att *Som bedömningsgrund kan Transport- och kommunikationsverket utöver de författningar och rättsakter som avses i 1 och 2 mom. fastställa bestämmelser eller riktlinjer som antagits av Europeiska unionen eller något annat internationellt organ, publicerade och generellt eller regionalt tillämpade anvisningar för informationssäkerhet samt datasäkerhetsstandarder eller förfaranden som används allmänt.*

Ämbetsverket fastställer inte specifika källor som grunder, utan föreskriften definierar ramar för de kriterier som ska användas i bedömningen av överensstämmelse. Bestämmelsen kompletteras med en hänvisning till Transport- och kommunikationsverkets bedömningsanvisning. Vid tidpunkten för beredningen av föreskriften är den aktuella versionen 211/2019 [21]. Anvisningen uppdaterades grundligt år 2019 för att beakta alla fastställda krav, och den har kompletterats med specialkriterier för mobilapplikationer. Man bör använda den senaste versionen av anvisningen, så att alla krav beaktas.

Andra källor kan också beaktas vid kvalitetsrevisioner. Exempel på dessa är informationssäkerhetsstandarder som preciserar god sed inom informationssäkerhet och ger konkreta detaljer som är beaktansvärda vid kvalitetsrevisionen. Exempel på dessa listas nedan.

Leverantörerna av identifieringstjänster kan uppfylla de krav på kvalitetsrevision som fastställs i bestämmelsen genom en eller flera kvalitetsrevisioner som leverantören har valt. Bedömningsorganen kan också vara flera. Kraven på bedömningsorganens oberoende och kompetens föreskrivs i 33 § i autentiseringslagen och preciseras i bestämmelse 18 och 19 i denna föreskrift.

En leverantör av identifieringstjänster som skaffar en kvalitetsrevision ska se till att de krav som uttryckligen gäller identifieringssystem och identifieringsmedel också beaktas vid kvalitetsrevisionen, även om produktions- och administrationsmiljön för tjänsten ofta endast är en del av den övriga produktions- och administrationsmiljön och den övergripande kvalitetsrevisionen riktas till denna mer omfattande helhet.

Målet är att aktörerna flexibelt ska kunna använda de bedömningskriterier som de redan använder. Å andra sidan ska aktörerna bedöma och försäkra sig om att alla de på olika standarder baserade kriterier som aktörerna använder verkligen omfattar alla de krävda delområdena av bedömningen av identifieringssystem och deras krav.

4.15.3 Exempel på källor för bedömningar

Standarder eller källor som även kan lämpa sig för bedömning av ett identifieringssystem som en del av en revision.

- ISO/IEC 27001 [11]
- Katakri [12]
- PiTuKri [26]
- PCI DSS, PCI/QSA [20]
- Webtrust Trust Services Principles and Criteria for Certification Authorities och Webtrust for Certification Authorities - SSL Baseline Requirements Audit Criteria [54]
- Information Security Forum (ISF) Standard of Good Practice [55]
- ISF:s IRAM-kriterier (Information Risk Analysis Methodology) [55]
- ISRS 4400 [56] och ISAE 3000 [57]
- Vahti-anvisningarna [58]
- Informationshanteringsnämndens rekommendationer [59]
- Europeiska centralbankens anvisningar
- FIVA:s föreskrifter eller anvisningar [60]
- Finansinspektionens föreskrift och anvisning 2.4 ”Kundkännedom – åtgärder mot penningtvätt och finansiering av terrorism” [61]
- Europeiska centralbankens SREP cyber risk questionnaire [62]
- BIS, Bank for International Settlements, anvisningarna External audits of banks och supplemental note to External audits of banks - audit of expected credit loss [63]
- Svenska Finansinspektionens (FFFS) och finska Finansinspektionens föreskrifter och anvisningar gällande organisering av och verksamhet med intern granskning
- IIA, The Institute of Internal Auditors [64] den internationella paraplyorganisationens anvisningar, regler och granskningsprinciper.
- ETSI:s standarder [66, sammanställda länkar för betrodda tjänster]

4.15.4 Alternativa styrmetoder till föreskriften och ämbetsverkets bedömningsanvisning

Rekommendation/anvisning. Transport- och kommunikationsverkets bedömningsanvisning för elektroniska identifieringstjänster 211/2019 uppdaterades grundligt år 2019 för att beakta alla fastställda krav, och den har kompletterats med specialkriterier för mobilapplikationer. Det är tänkt att anvisningen ska upprätthållas så att användning av dess aktuella version täcker alla föreskrivna krav.

Samreglering. Med tanke på tröskeln för att komma in i branschen och eventuella konkurrensrättsliga frågor är det också bättre att myndigheten ansvarar för att ställa minimikraven. Utbyte av information om användning av olika kriterier och om tolkningsfrågor omfattas av samreglering.

Informationsstyrning. Inga anmärkningar.

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

4.16.1 Utredningar gällande identifieringstjänstens anmälningsskyldighet

I bestämmelsen har man för tydlighetens skull sammanställt de delområden som berör tillförlitligheten hos leverantören av identifieringstjänsten och de uppgifter som den enligt lagen ska offentliggöra, för vilka det inte krävs en oberoende och behörig bedömning av överensstämmelse enligt bestämmelse 15.

Bestämmelsen gäller identifieringstjänstens skyldighet att göra anmälningar till Transport- och kommunikationsverket enligt 10 § i autentiseringslagen. Ämbetsverket har enligt 42 § i autentiseringslagen behörighet att fastställa *innehållet i de uppgifter som ska anmälas i inlednings- eller ändringsanmälan och inlämnandet av dem till Transport- och kommunikationsverket*.

Leverantören av identifieringstjänsten ska alltså ge information och utredningar till Transport- och kommunikationsverket i samband med inlednings- eller ändringsanmälan eller om ämbetsverket annars begär dem i tillsynen av identifieringstjänsterna.

Bestämmelsen är inte uttömmande i fråga om uppgifter som ska anmälas och utredningarnas form. I bestämmelsen fastställs på en allmän nivå att uppfyllandet av dessa krav kan bevisas genom företagets egen utredning eller någon annan lämplig utredning eller bedömning.

Vägledning och råd för anmälan och utredningarna ges på anmälningsblanketten och i anmälningsanvisningarna samt vid behov genom aktörspecifik rådgivning.

4.16.2 Uppgifter som ska utredas

Ordalydelserna i bestämmelsen kommer delvis från förordningen om tillitsnivåer i elektronisk identifiering avsnitt 2.4 Hantering och organisation och i synnerhet 2.4.1 Allmänna bestämmelser och 2.4.2 Offentliggjorda meddelanden och användaruppgifter. Motsvarande krav finns i autentiseringslagen. Bestämmelsens rubrik och ordalydelse har förtydligats, avsnittens inbördes ordning har ändrats och vissa preciseringar har gjorts i innehållet med tanke på identifieringstjänstleverantörens anmälningsskyldigheter.

1) *en etablerad juridisk person som ansvarar för identifieringstjänsten samt de ansvarigas handlingsbehörighet och tillförlitlighet* Kraven i detta avsnitt anknyter till kraven i 9 § i autentiseringslagen. En juridisk persons identitet kan exempelvis bevisas genom ett registerutdrag och de ansvariga personernas tillförlitlighet utreds exempelvis genom en skriftlig försäkran från personerna eller utifrån lämpliga källor.

2) *offentliggjorda meddelanden och användaruppgifter, såsom identifieringsprinciper, dataskyddsprinciper, användningsbegränsningar, avtalsvillkor och prislistor.* Kraven i avsnittet anknyter till kraven i 12 b, 14, 15 och 18 § i autentiseringslagen. De offentliggjorda uppgifternas tillförlitlighet utreds genom att man presenterar platserna för offentliggörandet och de offentliggjorda uppgifterna.

3) *tillräckliga ekonomiska resurser och beredskap att ta en risk för skadeståndsansvar.* Kraven i detta avsnitt anknyter till kraven i 13 § i autentiseringslagen. De ekonomiska resurserna och förmågan att bära skaderisker utreds utifrån bokslutet, balansräkningen och revisionsberättelsen samt eventuell utredning om en ansvarsförsäkring.

Kravet i avsnitt 4) anknyter till kravet i 13 § i autentiseringslagen. *Ansvaret för underleverantörerna* framgår också i bedömningen av överensstämmelse enligt avsnitt 15, men utgör även en del av överensstämmelsen i identifieringstjänstens förvaltning. De centrala underleverantörerna ska också nämnas i identifieringsprinciperna enligt lagens 14 §.

Avsnitt 5) anknyter till kravet i 13 § i autentiseringslagen. Planens syfte och innehåll beskrivs i avsnitt 2.4.1 5 i förordningen om tillitsnivåer för elektronisk identifiering: *System för elektronisk identifiering som inte inrättats enligt nationell rätt ska ha en fullt användbar plan för verksamhetens upphörande. En sådan plan ska innefatta en*

metodisk nedläggning av driften eller fortsättning genom en annan tillhandahållare av tjänster, sättet på vilket behöriga myndigheter och slutanvändare informeras samt ingående uppgifter om hur register ska skyddas, bevaras och destrueras i enlighet med systemets policy.

4.16.3 Ämbetsverkets anmälningsanvisning

I Kommunikationsverkets anvisning 214/2016 O om anmälningar om identifieringstjänster och betrodda tjänster [65] behandlas till vissa delar uppgifter eller bilagor som ska lämnas till Transport- och kommunikationsverket. Det har dock inte utfärdats några detaljerade tillämpningsanvisningar om uppgifterna utan det innehåll som behövs bedöms bl.a. med hjälp av motiveringen till autentiseringslagen.

4.17 Bestämmelse 17 Grunder för bedömning av den nationella noden

Bestämmelsen är främst informativ. I kommissionens genomförandeförordning (EU) 2015/1501 [5] nämns som antagande ledning av informationssäkerhet, som bygger på ISO/IEC 27001 [11]. I föreskriften bekräftas detta antagande, eftersom det är en lösning som också lämpar sig för verksamheten inom Myndigheten för digitalisering och befolkningsdata i praktiken. Kommissionens genomförandeförordning innehåller några krav på verksamheten i noden.

Kapitel 5 i föreskriften Kompetensen hos bedömningsorgan för identifieringstjänster

4.18 Bestämmelse 18 Krav på utomstående bedömningsorgan för identifieringstjänster

I en anmälan om att inleda verksamhet och ändringsanmälan och dess bilagor som enligt 10 § i autentiseringslagen ska lämnas in till Transport- och kommunikationsverket lämnas tillsynsmyndigheten uppgifter om oberoende bedömning. Det ska också lämnas en utredning som gör det möjligt att bedöma att den som gjort bedömningen uppfyller de krav som ställs på bedömningsorgans oberoende och kompetens i 33 § i autentiseringslagen.

Enligt 29 § i autentiseringslagen kan ett bedömningsorgan som gör en kvalitetsrevision vara ett internt kontrollorgan, ett annat utomstående bedömningsorgan eller ett ackrediterat bedömningsorgan för överensstämmelse.

Syftet med bestämmelsen är att klargöra specificering av grunderna för ett bedömningsorgans oberoende och kompetens förutsebart. Syftet har också varit att klargöra att bedömningsorganets oberoende och kompetens inte kan basera sig på aktörens egen bedömning eller egna verksamhetssätt utan de ska vara objektivt motiverade.

I bestämmelse 18.1 finns exempel på sådana internationella standarder, regelverk eller ramar för självreglering som bedömningsorgans oberoende och kompetens kan bygga på. Förteckningen är inte fullständig och i avsnitt 5 fastslås de allmänna förutsättningarna för att visa bedömningsorgans oberoende och kompetens. Avsikten är att aktörerna så smidigt som möjligt ska kunna använda de bedömningar som de också i övrigt redan använder.

Exempel på eventuella bedömningsorgan är kontrollorgan som är ackrediterade enligt ISO 27001, andra utomstående ISO 27001-kvalitetsrevisorer eller motsvarande bedömningsorgan som bygger på andra relevanta standarder.

Av bestämmelse 18.2 framgår att olika standarder eller regelverk kan användas vid oberoende och kompetenta bedömningar av identifieringssystem, förutsatt att bedömningen verkligen riktas till kraven på identifieringssystem. Det är leverantören av identifieringstjänsten som ansvarar för att detta förverkligas och bedömningen omfattar alla de delområden som anges i denna föreskrift.
Av inspektionsberättelsen ska det på ett tydligt sätt framgå att revisionen de facto riktas till kraven på identifieringssystem.

4.19 Bestämmelse 19 Krav på interna kontrollorgan för identifieringstjänster

Bestämmelsens motiveringar är desamma som motiveringarna till bestämmelse 18. Oberoende och kompetens hos ett internt kontrollorgan kan inte heller basera sig på aktörens egen bedömning eller egna verksamhetssätt utan de ska vara objektivt motiverade och av grundad anledning lämpa sig för bedömningar av kraven i identifieringssystem.

Kapitel 6 i föreskriften Kvalificerade betrodda tjänster

4.20 Bestämmelse 20 Kriterier för bedömning av kvalificerade tillhandahållare av betrodda tjänster

4.20.1 Allmänt om regleringen av och standarderna för betrodda tjänster

Det allmänna målet för regleringen av betrodda tjänster är utveckling av informationssamhället och ökat förtroende för elektronisk ärendehantering. Reglerna för betrodda tjänster hjälper leverantörerna och användarna av elektroniska tjänster att känna igen de tjänster där det är möjligt att implementera olika funktioner för elektroniska ärendehanteringstjänster med högsta möjliga informationssäkerhet.

I eIDAS-förordningen [3] anges de krav som en kvalificerad tillhandahållare av betrodda tjänster och de betrodda tjänsterna ska uppfylla. För precisering av innehållet i kraven har Europeiska institutet för telestandarder ETSI enligt kommissionens mandat utfärdat standarder för tillhandahållare av betrodda tjänster [66]. Standarderna omfattar detaljerade konkreta krav som säkerställer att tillhandahållaren av betrodda tjänster överensstämmer med eIDAS-förordningen när den uppfyller kraven i standarder.

Målet med föreskriften är att förtydliga de krav som ställs på kvalificerade betrodda tjänster i eIDAS-förordningen genom hänvisningar till de internationella standarder som har tagits upp i EU:s beredningsarbete och som åtminstone hittills inte har hänvisats till genom kommissionens genomförandeakter, trots att kommissionen har befogenheter för det enligt eIDAS-förordningen.

Hänvisningarna till standarderna stöder också de faktorer som åtminstone ska beaktas som kompetenskrav på eventuella bedömningsorgan för överensstämmelse, när organen ackrediteras.

Standarderna är inte obligatoriska, utan funktionerna också kan genomföras på något annat sätt. Standarderna anger dock vilken tillitsnivå som eIDAS-förordningen förutsätter. Om någon annan standard med motsvarande krav används, ska den som utformar tjänsten särskilt visa att tjänsten uppfyller kraven i eIDAS-förordningen. Föreskriften innehåller hänvisningar till de standarder som är färdiga när föreskriften utfärdas.

Föreskriften kompletteras med hänvisningar till standarder som blivit klara efter att den föregående föreskriften gavs.

ETSIs standarder har satts i kraft som sådana i Finland och de finns också som SFS-standarder. Då märks standarden ut t.ex. SFS-EN 319 401.

Enisa har gjort en bedömning av eIDAS-standarderna: Enisa Assessment of Standards related to eIDAS (December 14, 2018)[67] https://www.enisa.europa.eu/publications/assessment-of-standards-related-to-eidas

4.20.2 Allmänna och tjänstespecifika krav på kvalificerade tillhandahållare av betrodda tjänster

4.20.2.1 Bestämmelse 20.1.1 Allmänna krav på kvalificerade tillhandahållare av betrodda tjänster

ETSI EN 319 401 V2.2.1 (2018-04) Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers [66]

Standarden innehåller allmänna serviceoberoende krav för tillhandahållare av betrodda tjänster. Den innehåller krav på bl.a. riskbedömning, informationssäkerhetspolicy och -praxis samt ledning av verksamheten.

4.20.2.2 Bestämmelse 20.1.2 Tilläggskrav på tillhandahållare av kvalifirerad certifikat

Standardhänvisningarna till kvalificerade tillhandahållare av betrodda tjänster som beviljar certifikat har slagits ihop i samma bestämmelse som gäller beviljandet av kvalificerade certifikat.

ETSI EN 319 411-1 V1.2.2 (2018-04) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements [66]

Följande version ETSI EN 319 411-1 V1.3.0 (2021-02) genomgår ett godkännandeförfarande.

Standarden innehåller allmänna krav för tillhandahållare av betrodda tjänster som tillhandahåller certifikat. Standarden kompletterar och preciserar kraven i standard EN 319 401. Standarden innehåller detaljerade krav bl.a. för certifikatpolicy och certifieringsstandard. Till standarden hänför sig en informativ bilaga C (Conformity Assessment Check list) med en checklista för att kontrollera kraven i standarden. Checklistan kan användas till exempel vid kvalitetsrevision av tillhandahållare av betrodda tjänster.

ETSI EN 319 411-2 V2.2.2 (2018-04) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates [66]

Följande version ETSI EN 319 411-2 V2.3.0 (2021-02) har gått ut på remiss för godkännande.

Standarden innehåller krav på tillhandahållaren av betrodda tjänster som tillhandahåller kvalificerade certifikat enligt eIDAS-förordningen. Den kompletterar kraven i standard EN 319 411-1 för att motsvara de speciella kraven i eIDAS. De ytterligare kraven gäller bl.a. certifikatpolicy och certifieringsstandard.

Till standarden hänför sig en informativ bilaga B (Conformity Assessment Check list) med en checklista för att kontrollera kraven i standarden. Checklistan kan användas till exempel vid kvalitetsrevision av tillhandahållare av betrodda tjänster.

4.20.2.3 Bestämmelse 20.1.3 Tilläggskrav på tillhandahållare av kvalificerad tidsstämpling

ETSI EN 319 421 V1.1.1 (2016-03) Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Electronic Time-Stamps [66]

Standarden innehåller kraven på informationssäkerhetspolicy och kraven på informationssäkerhet för tillhandahållaren av betrodda tjänster som tillhandahåller elektronisk tidsstämpling. Standarden hänvisar främst till kraven i standarden EN 319 401, men preciserar dem till en viss del. Standarden omfattar detaljerade krav på administration av enheten TSU (Time-Stamping Unit) som innehåller en tidsstämpling till en elektronisk underskrift. Till standarden hänför sig en informativ bilaga H (Conformity Assessment Check list) med en checklista för att kontrollera kraven i standarden. Checklistan kan användas till exempel vid kvalitetsrevision av tillhandahållare av betrodda tjänster.

4.21 Bestämmelse 21 Kriterier för bedömning av kvalificerade betrodda tjänster

4.21.1 Kvalificerade typer av betrodda tjänster

Kvalificerade (qualified) betrodda tjänster enligt eIDAS-förordningen (EU) 910/2014 [3] kan vara av följande typer:

1) Kvalificerat certifikat för elektronisk underskrift (artikel 28) (Qualified certificate for electronic signature)

2) Kvalificerad valideringstjänst för kvalificerade elektroniska underskrifter (artikel 33) (Qualified validation Service for qualified electronic signature)

3) Kvalificerad tjänst för bevarande av kvalificerad elektronisk underskrift (artikel 34) (Qualified preservation Service for qualified electronic signature)

4) Kvalificerat certifikat för elektronisk stämpel (artikel 38) (Qualified certificate for electronic seal)

5) Kvalificerad valideringstjänst för kvalificerad elektronisk stämpel (artikel 40) (Qualified preservation Service for qualified electronic signature)

6) Kvalificerad bevarandetjänst för kvalificerad elektronisk stämpel (artikel 40) (Qualified preservation Service for qualified electronic seal)

7) Kvalificerad elektronisk tidsstämpling (artikel 42) (Qualified time stamp)

8) Kvalificerad elektronisk tjänst för rekommenderade leverans (artikel 44) (Qualified electronic registrered delivery Service, "eDelivery"/QERDS)

9) Kvalificerat certifikat för autentisering av webbplatser (artikel 45) (Qualified certificate for website authentication, QWAC)

Kvalificering skaffas enligt artikel 20 och 21 i eIDAS-förordningen.

4.21.2 Standarder

I bestämmelsen preciseras bedömningskriterierna för kvalificerade betrodda tjänster.

I bilagorna I, III och IV i eIDAS-förordningen anges kraven som gäller kvalificerade certifikat för elektroniska underskrifter, elektroniska stämplar och autentisering av webbplatser.

För precisering av innehållet i kraven har Europeiska institutet för telestandarder ETSI enligt kommissionens mandat utfärdat de standarder som uppräknas i föreskriftstexten. Standarderna omfattar detaljerade konkreta krav som säkerställer att den betrodda tjänsten överensstämmer med eIDAS-förordningen när den uppfyller kraven i standarder.

Standarderna är inte obligatoriska, utan tjänsterna också kan genomföras på något annat sätt. Standarderna anger dock vilken tillitsnivå som eIDAS-förordningen förutsätter i tjänster. Om en tjänst genomförs enligt en hänvisad standard, blir kraven i eIDAS beaktade. Om någon annan standard med motsvarande krav används, ska den som utformar tjänsten särskilt visa att tjänsten uppfyller kraven i eIDAS-förordningen.

I de certifikatprofiler som uppräknas i föreskriften ingår en standard som innehåller allmänna krav (EN 319 412-1), standarder enligt den avsedda tillämpningen av certifikatet (EN 319 412 del 2–4) samt en standard som specificerar innehållet i de kvalificerade certifikaten (statements) (EN 319 412-5).

Till den del standarderna har delar som gäller uppfyllande av kraven i EU-lagstiftningen och delar som gäller övriga krav, anses kraven i EU-lagstiftningen vara lämpliga med tanke på denna föreskrift.

I följande tabell sammanställs standarderna för kvalificerade tillhandahållare av betrodda tjänster och olika betrodda tjänster. De tekniska specifikationerna (ETSI TS) har inte ännu bekräftats, så föreskriften hänvisar inte till dem.

Tabell: Standarder för kvalificerade tillhandahållare av betrodda tjänster och betrodda tjänster

Standardreferenser finns i referensförteckningen, de färdiga standarderna [66] och de tekniska specifikationerna [68]

Tjänst, eIDAS-artikel	**färdig standard**	**teknisk specifikation**
kvalificerade tillhandahållare av betrodda tjänster (alla typer av betrodda tjänster)	ETSI EN 319 401	se ETSI TS 119 312 V1.3.1 (2019-02)[47]
Tillhandahållare av betrodda tjänster som erbjuder certifikat (alla kvalificerade certifikat)	ETSI EN 319 411-1 ETSI EN 319 411-2	
Signaturcertifikat artikel 28	ETSI EN 319 412-1 ETSI EN 319 412-2 ETSI EN 319 412-5	
Stämpelcertifikat	ETSI EN 319 412-1	

artikel 38	ETSI EN 319 412-3 ETSI EN 319 412-5	
webbplatscertifikat (QWAC) artikel 45	ETSI EN 319 412-1 ETSI EN 319 412-4 ETSI EN 319 412-5	
Tidsstämpling artikel 42	ETSI EN 319 421 ETSI EN 319 422	
validering av elektronisk underskrift artikel 33	ETSI EN 319 102-1	ETSI TS 119 441 ETSI TS 119 442 ETSI TS 119 102-2 ETSI TS 119 172-4
validering av elektronisk stämpel artikel 40, hänvisning till artikel 33	ETSI EN 319 102-1	ETSI TS 119 441 ETSI TS 119 442 ETSI TS 119 102-2 ETSI TS 119 172-4
bevarande av elektronisk underskrift artikel 34		ETSI TS 119 511 ETSI TS 119 512
bevarande av elektronisk stämpel Artikel 40, hänvisning till artikel 34		ETSI TS 119 511 ETSI TS 119 512
elektronisk tjänst för rekommenderade leverans (eDelivery) artikel 44	ETSI EN 319 521 ETSI EN 319 522 1-4	ETSI TS 119 524

Kapitel 7 i föreskriften Bedömningsorgan för överensstämmelse hos betrodda tjänster

4.22 Bestämmelse 22 Bedömning av bedömningsorgans kompetens

4.22.1 Ackreditering och godkännande

En förutsättning för att få statusen bedömningsorgan för överensstämmelse är att man genom ackreditering som ansöks om hos FINAS [69] visar att kraven på oberoende och kompetens enligt 33 § i autentiseringslagen uppfylls.

Genom bestämmelsen preciseras behörighetskraven enligt 33 § i autentiseringslagen på bedömningsorgan för överensstämmelse.

När FINAS fattar ett sådant beslut om kriterier för ackreditering av ett bedömningsorgan som avses i lagen om konstaterande av tillförlitligheten hos tjänster för bedömning av överensstämmelse med kraven (920/2005), kan FINAS också beakta andra krav för bedömning av oberoende och kompetens än de standarder som denna föreskrift hänvisar till.

Därutöver ska bedömningsorganet ansöka om godkännande hos Transport- och kommunikationsverket. För godkännandet krävs FINAS ackreditering och en redogörelse för de anvisningar och den uppföljning av anvisningarna som krävs i 33 § 1 mom. 4 punkten i autentiseringslagen.

I bilden nedan beskrivs förhållandena mellan de allmänna ackrediteringsreglerna och tillsynen per sektor enligt eIDAS vid bedömning av överensstämmelse hos betrodda elektroniska tjänster. På bilden ingår inte bedömningsorganets (*conformity assessement body, CAB*) godkännande- och tillsynsroll, som nationellt fastställts som Transport- och kommunikationsverkets uppgift i autentiseringslagen. Preciseringarna av föreskriften anknyter i schemat till ackrediteringskraven (*Accreditation Scheme*), som ackrediteringsorganet beslutar om (National Accreditation Body, i Finland FINAS).

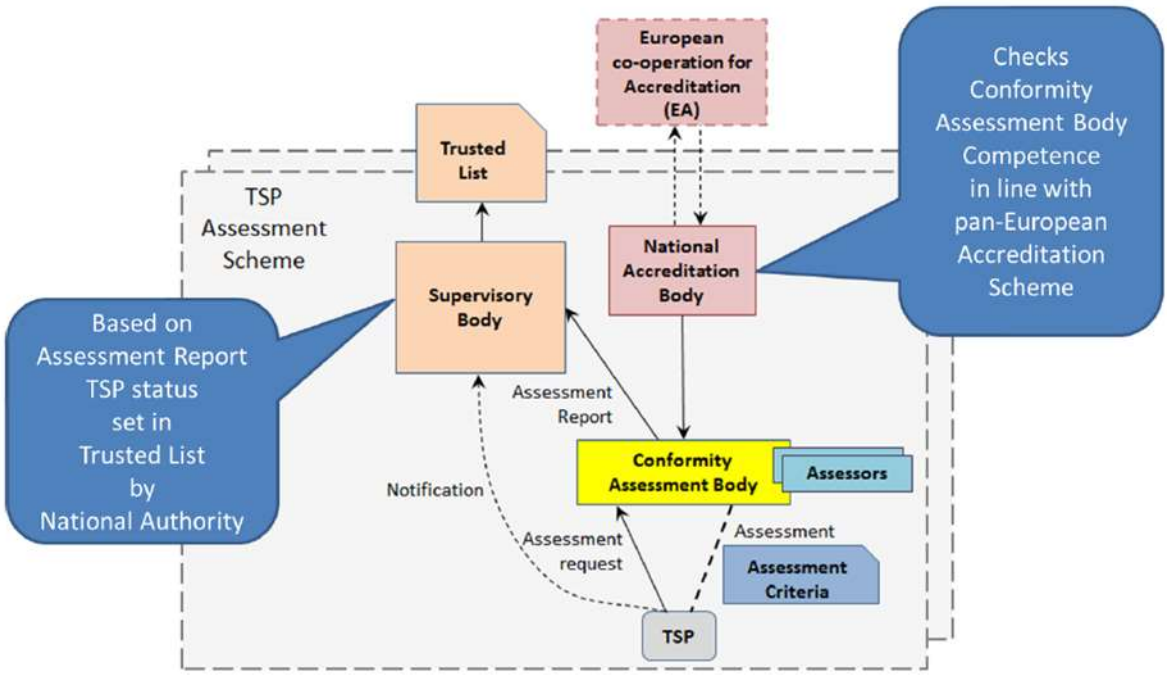

Bild: Schema för bedömning av tillhandahållaren av betrodda tjänster

(Källa: Europeiska byråns för nät- och informationssäkerhet ENISAs dokument Auditing Framework for TSPs, Guidelines for Trust Service Providers, Version 1.0 - December 2014 [70])

4.22.2 Standard

Kommissionen har inte fattat något genomförandeakt utifrån vilket de standarder som gäller bedömningsorgan för överensstämmelse skulle preciseras med stöd av artikel 20.4 i eIDAS.

Eftersom kommissionen inte har gett någon genomförandeakt om detta, utgör de standarder som listas i EA:s dokument som beskrivs i nästa stycke grunden för ackreditering och godkännande av bedömningsorgan för överensstämmelse. En del medlemsstater har ställt upp egna krav.

De europeiska ackrediteringsorganisationernas samarbetsorgan EA (European Cooperation for Accreditation) har år 2015 utarbetat dokumentet *EA Certification Committee Reference Paper; ETSI / EA Recommendations regarding; Preparation for Audit under EU Regulation (EU) No 910/2014 Article 20.1*. [71] Dokumentet fastställer på vilket sätt man vid ackreditering av bedömningsorgan för överensstämmelse hos betrodda tjänster (Conformity Assessment Bodies – CAB) ska övergå från tidigare praxis till praxis enligt eIDAS, vilka ackrediteringskrav bedömningsorganen ska uppfylla och vilka frågor organen ska ha kompetens för. Grunden utgörs av ETSIs standarder.

Kraven på bedömningsorgan för överensstämmelse definieras i standarden *ETSI EN 319 403-**1** V2.3.1 (2020-06) Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers* [72].

Standarden bygger på ISO/IEC 17065, som fastställer de allmänna kraven för bedömningsorgan. Standarden EN 319 403 kompletterar kraven i ISO/IEC särskilt med krav på tillhandahållare av betrodda tjänster och deras tjänster.

Standarden har kompletterats med en del 2, som berör bedömning av utfärdare av certifikat. Delen har inte ännu fastställts, endast den tekniska specifikationen (TS). Standarden anges därför inte som referens, men den kan tillämpas.

*ETSI TS 119 403-**2** V1.2.1 (2019-04) Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 2: Additional requirements for Conformity Assessment Bodies auditing Trust Service Providers that issue Publicly-Trusted Certificates* [73]

I enlighet med autentiseringslagen ska ett bedömningsorgan ha kompetens för att bedöma en tjänsteleverantör och de tjänster som den tillhandahåller. Bestämmelserna 20 och 21 i föreskriften preciserar bedömningskraven på tillhandahållare av betrodda tjänster och på betrodda tjänster, vilket betyder att bedömningsorganet ska vara kompetent för bedömning enligt de standarder som nämns i paragraferna.

4.22.3 Bedömningsberättelse

ETSI-standarden 119 403 har också fått en del 3, som standardiserar bedömningsberättelsen. Delen har inte ännu fastställts, endast den tekniska specifikationen (TS).

*ETSI TS 119 403-**3** V1.1.1 (2019-03) Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 3: Additional requirements for conformity assessment bodies assessing EU qualified trust service providers* [74]

Transport- och kommunikationsverkets behörighet att utfärda bestämmelser enligt autentiseringslagens 42 § gäller inte bedömningsberättelsen för betrodda tjänsters överensstämmelse, utan endast bedömningskriterierna. Standarden anges därför inte som referens, men bedömningsorganet kan tillämpa den.

Transport- och kommunikationsverket har utfärdat en anvisning 215/2019 *om bedömningsberättelser för betrodda eIDAS-tjänster* [75]. Anvisningens innehåll om bedömning av betrodda tjänster är detsamma som i anvisningen 215/2016.

Kapitel 8 i föreskriften Certifiering av kvalificerade anordningar för skapande av elektroniska underskrifter och stämplar

4.23 Bestämmelse 23 Certifieringsorgan för anordningar för skapande av elektronisk underskrift eller stämpel

4.23.1 Kompetenskrav

Bestämmelserna 23 och 24 i den tidigare föreskriften har slagits ihop.

Om en finländsk certifieringsinstans vill ansöka om att bli ett uttsett certifieringsorgan, kan instansen ansöka om godkännande hos Transport- och kommunikationsverket i enlighet med 36 § i autentiseringslagen och under de förutsättningar som föreskrivs i den paragrafen.

I bestämmelse 23 definieras hur den behörighet som förutsätts i lagen kan påvisas. Möjliga metoder är åtminstone ackreditering, som innebär FINAS kompetensbedömning, och anslutning till ett förfarande för kompetensbedömning som bygger på referentgranskning enligt SOGIS-MRA-avtalet.

SOGIS-MRA (Senior Officers Group for Information Systems, Mutual Recognition Agreement)[38] är ett europeiskt system för ömsesidigt erkännande av certifieringar. Avtalet omfattar åtta länder som har egna certifieringsinstanser (*qualified/authorising participant*) och två länder (*consuming participant*) som saknar egna certifieringsinstanser (bl.a. Finland).

Kompetens som certifieringsorgan förutsätter att aktören kan verifiera kraven på anordningen för skapande, som ställs upp genom kommissionens genomförandebeslut (EU) 2016/650 [8].

Certifieringar för de certifieringsorgan som EU-medlemsstater eller medlemsstater inom EES-området har anmält till kommissionen och som har godkänts i medlemsstaterna är som sådana giltiga även i Finland. För tillfället omfattar SOGIS-MRA-avtalet även en stor del av de till kommissionen anmälda certifieringsorganen.

4.23.2 Standarder

Kraven grundar sig på kommissionens genomförandebeslut (EU) 2016/650 [8].

Beslutet (EU) 2016/650 innehåller hänvisningar till standarder för anordningar för skapande som baserar sig på innehav. CEN:s standarder för verktyg för skapande på distans har godkänts i standardiseringsförfarandet, men tillägget av dem till kommissionens genomförandebeslut har vid tidpunkten för färdigställandet av denna motiveringspromemoria ännu bara gjorts anhängigt.

Av de standarder som fastställs i bilagan till kommissionens genomförandebeslut är den allmänna standarden för bedömning av IT-säkerhet ISO/IEC 15408 Information technology -- Security techniques -- Evaluation criteria for IT security-standardisarja [23] känd som Common Criteria-kraven.

Kapitel 9 i föreskriften Övergångsbestämmelser och underskrifter

4.24 Bestämmelse 24 Föreskriftens ikraftträdande och övergångsbestämmelser

Föreskriften avses träda i kraft i april 2022.

Föreskriften träder i kraft dd.mm.2022

4.24.1 Övergångstid för bestämmelse 6.2 och 12.1

Övergångstiden för avsnitt 6.2.1 i bestämmelsen, det vill säga visningen av information om transaktionen, innebär att informationen ska visas för användaren av identifieringsverktyg vid identifieringstransaktioner senast den X oktober 2022.

Kravet hör till identifieringstjänstleverantörens uppgifter och kräver inga åtgärder av de förlitande parterna. I många identifieringstjänster används denna funktion sedan tidigare. Förverkligandet förutsätter att leverantören av identifieringsverktyget tar

fram tekniska definitioner enligt vilka man i bakgrundssystemet skapar en teckensträng, QR-kod eller annat meddelande, som visas i webbläsarsessionen eller applikationen och i den bekräftelsebegäran som visas i identifieringsverktyget. Ämbetsverket bedömer att de tekniska definitioner som krävs är relativt ringa, men en övergångstid behövs för att de nödvändiga definitionerna ska kunna planeras och genomföras.

Avsnitt 6.2.2 och 12.1 4), det vill säga övergångstiden för visningen av den förlitande partens namn, innebär att den förlitande partens namn ska visas för användaren vid identifieringstransaktioner senast den X oktober 2022.

Uppfyllandet av kravet kräver åtgärder av identifieringstjänsterna och i viss mån av de förlitande parterna.

Identifieringsförmedlingstjänsten och den förlitande parten ska komma överens om vilka namn som ska visas. Detta behandlas i avsnitt 4.12.3 i motiveringspromemorian.

Till visningen av den förlitande partens namn anknyter också bestämmelse 9.1.2, där det förutsätts att den förlitande parten undertecknar identifieringsbegäran. Om den nyckel som ska användas vid undertecknandet och övergångstiden för 9.1.2 föreskrivs i bestämmelse 24.4.

Uppfyllandet av kravet förutsätter tekniska specifikationer för identifieringsförmedlingstjänstens och identifieringsverktygsleverantörens gränssnitt för att förmedla informationen. Attributet har definierats i gränssnittsrekommendationerna sedan tidigare, och i uppdateringen av rekommendationerna år 2021 har det gjorts obligatoriskt. Rekommendationen har beretts i nära samarbete med aktörerna. Beredskapen för interoperabilitet är därmed god.

Uppfyllandet av kravet förutsätter tekniska specifikationer för den bekräftelsebegäran som visas i identifieringsverktyget. Detta gäller i första hand leverantören av identifieringsverktyget, men om identifieringsförmedlingstjänsten visar information för användaren av identifieringsverktyget i identifieringstransaktionens mellanskede, kräver visningen av informationen åtgärder även av identifieringsförmedlingstjänsten.

Ämbetsverket bedömer att de tekniska specifikationer som krävs är relativt ringa. En del identifieringstjänster har förverkligat denna funktion sedan tidigare. Ämbetsverket bedömer att en övergångstid är nödvändig för att förverkliga de tekniska specifikationerna och för att identifieringsförmedlingstjänsterna ska ha möjlighet att komma överens med de förlitande parterna om vilka namn som ska visas, om detta inte har gjorts tidigare.

4.24.2 Övergångstider för bestämmelse 8

Övergångstiden enligt bestämmelse 24.3 stycke a) innebär att datakommunikationsförbindelser mellan identifieringstjänster i förtroendenätet senast den x oktober 2022 måste ha ett certifikat som levererats enligt bestämmelse 8.1.

Övergångstiden enligt bestämmelse 24.3 stycke b) innebär att identifieringsförmedlingstjänsten senast den X oktober ska använda ett förfarande enligt 8.1 när den lägger till nya ärendetjänstkunder i sitt identifieringssystem.

Övergångstiden enligt bestämmelse 24.2 stycke c) innebär att identifieringsförmedlingstjänsten senast den X april 2023 måste identifiera de ärendetjänstkunder som

identifieringsförmedlingstjänsten har anslutit till sitt identifieringssystem utan identifiering enligt 8.1. Certifikatet eller nyckeln måste bytas ut i enlighet med 8.1. Övergångstiden innebär att det gamla avtalsbeståndet måste göras förenligt med de nya kraven senast den x april 2023 oberoende av när ett avtal ursprungligen ingåtts.

Bestämmelsens krav på att kravet i 8.2 ska tas i bruk senast den x april 2023 innebär att uppdateringen av certifikat och nycklar från och med denna tidpunkt alltid måste ske i enlighet med föreskriftens krav.

Uppfyllande av kraven förutsätter fastställande av förfaranden och processer för identifiering och leverans av nycklar och certifikat samt fastställande av processer för uppföljning av bytescykler. Tekniskt förutsätter förverkligande av kraven fastställande av olika inställningar i serverprogramvaran såväl i identifieringstjänster som i ärendehanteringstjänster.

Antalet identifieringstjänster i förtroendenätet är begränsat och de har teknisk förmåga att uppfylla kraven. Planeringen tar dock en viss tid, och man måste också reservera tid för informationsutbyte om förfaranden så att man om man vill kan förenhetliga dem inom förtroendenätet.

I fråga om tjänster för identifieringsförmedling innebär kraven att tjänsterna i sina avtalsrelationer med förlitande parter måste sköta informationen om de tekniska kraven, eftersom det inte är sannolikt att de förlitande parterna känner till dem.

De tekniska kraven på ärendehanteringstjänster enligt bestämmelse 8.1 och 8.2 bedöms i avsnitt 4.8.5.5. De behov av härdande i ärendehanteringstjänsternas system som förfarandena förutsätter kräver också att de relaterade processerna samt ansvaren för underhåll och genomförande sköts i det tekniska underhållet av ärendehanteringstjänsten och i eventuellt underleverantörsarbete inom detta. För nya kunder kan förfarandena enligt ämbetsverkets bedömning tas i bruk genast när identifieringsförmedlingstjänsten tar dem i bruk och ärendehanteringstjänsten skaffar identifieringstjänsten. Gamla avtalskunder har däremot redan ett användningssätt för identifieringstjänsten, som de måste göra ändringar i. Med tanke på att identifieringsförmedlingstjänsten först måste planera sina processer och informera ärendehanteringstjänsterna om den kommande förändringen måste man reservera en längre övergångstid för detta. ICT-projekt planeras och skaffas enligt ämbetsverkets uppfattning ofta i cykler, och projekt kombineras.

Ämbetsverket bedömer att eftersom det inte är fråga om en tekniskt krävande sak utan den kritiska faktorn är kommunikation och medvetenhet om ändringarna och deras innehåll, kan ändringsbehoven planeras och genomföras i ärendehanteringstjänsterna inom ett år. Detta förutsätter naturligtvis att identifieringstjänsterna och myndigheten aktivt kommunicerar om de kommande förändringarna och deras innehåll.

4.24.3 Övergångstider för bestämmelse 9

Övergångsbestämmelsen för det nya förfarandet enligt bestämmelse 9.1.1 stycke a) innebär att ett alternativt förfarande för kryptering på meddelandenivå kan tas i bruk först när man i det kan använda ett certifikat eller en nyckel som uppfyller kraven i bestämmelse 8.1.

Bestämmelsens övergångstid för undertecknande av meddelanden innebär att krypteringen och undertecknandet måste göras med nycklar enligt stycke 8 senast när de måste vara i bruk enligt övergångstiderna enligt bestämmelse 8. Under övergångstiden kan man i kryptering på meddelandenivå fortfarande använda de nycklar

som varit i bruk innan föreskriften trädde i kraft. Även undertecknandet av meddelanden kan göras med dessa nycklar, tills man har bytt till nya nycklar. Undertecknande av meddelanden är dock inte obligatoriskt innan övergångstiden har löpt ut.

5 Bilagor och hänvisningar

5.1 Referenslista

Författningar som hänför sig till föreskriften finns i författningssamlingarna Finlex eller Eur-Lex och är markerade med en asterisk* i listan.

Transport- och kommunikationsverkets anvisningar och rekommendationer finns på ämbetsverkets webbplats och är försedda med två asterisker** i referenslistan. På webbsidorna finns också hänvisningar till författningar.

Allmänna länkar
Elektronisk identifiering | Cybersäkerhetscentret
Elektronisk underskrift och övriga eIDAS-tjänster | Cybersäkerhetscentret

ETSI standarder finns på ETSIs webbsidor och de försedda med tre asterisker*** i referenslistan

- Allmän länk med sökningen Elecetronic Signatures: https://portal.etsi.org/TBSiteMap/ESI/ESIActivities.aspx

[1] * Lag om stark autentisering och betrodda elektroniska tjänster (617/2009 jämte ändringar, **autentiseringslag**) 617/2009 - Författningsändringsregister - FINLEX ®

[2] * Statsrådets förordning om förtroendenätet för leverantörer av tjänster för stark autentisering 169/2016, ändrad 1212/2018 (**statsrådets förordning om förtroendenätet**) 169/2016 - Författningsändringsregister - FINLEX ®

[3] * Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG (**eIDAS-förordningen**) EUR-Lex - 32014R0910 - SV - EUR-Lex (europa.eu)

[4] * KOMMISSIONENS GENOMFÖRANDEFÖRORDNING(EU) 2015/1502 (**förordning om tillitsnivåer**) om fastställande av tekniska minimispecifikationer och förfaranden för tillitsnivåer för medel för elektronisk identifiering i enlighet med artikel 8.3 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden EUR-Lex - 32015R1502 - SV - EUR-Lex (europa.eu)

[5] * KOMMISSIONENS GENOMFÖRANDEFÖRORDNING (EU) 2015/1501 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 EUR-Lex - 32015R1501 - SV - EUR-Lex (europa.eu)

[6] KOMMISSIONENS GENOMFÖRANDEBESLUT (EU) 2015/1984 (EU:s beslut om anmälningsförfarande) om förutsättningar, format och förfaranden för anmälan enligt artikel 9.5 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om

elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden

[7] * KOMMISSIONENS GENOMFÖRANDEBESLUT (EU) 2015/296 (**EU:s beslut om samarbetsnätverk**) om inrättande av förfaranden för samarbete mellan medlemsstaterna om elektronisk identifiering i enlighet med artikel 12.7 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden

[8] * 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 (Obs! Gäller s.k. QSCD-certifiering) EUR-Lex - 32016D0650 - SV - EUR-Lex (europa.eu)

[9] * EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (**allmän dataskyddsförordning**)

[10] * Dataskyddslag (1050/2018)

[11] ISO/IEC 27001 Information security management

[12] KATAKRI, Katakri – verktyg för informationssäkerhetsauditering för myndigheter, Traficoms publikationsserie 232/2020 https://um.fi/katakri-verktyg-for-informationssakerhetsauditering-for-myndigheter och Katakri 2020 (um.fi)

[13] SFS-ISO 31000:2018 Riskhantering Anvisningar. ISO 31000 Riskienhallinta | SFS

- På engelska ISO 31000:2018(en), Risk management — Guidelines

[14] ISO/TR 31004, Risk management – Guidance for the implementation of ISO 31000, and International Standard/ISO/TR 31004:fi [14]

- På engelska ISO - ISO/TR 31004:2013 - Risk management — Guidance for the implementation of ISO 31000

[15] ISO/IEC 31010, Risk management – Risk assessment techniques ISO - IEC 31010:2019 - Risk management — Risk assessment techniques

- SFS-ISO/IEC 31010 Produkt (sfs.fi)

[16] SFS-ISO/IEC 27005:2018, Information technology — Security techniques — Information security risk management Produkt (sfs.fi)

- På engelska ISO - ISO/IEC 27005:2018 - Information technology — Security techniques — Information security risk management

[17] VAHTI Riskhanteringsanvisning, Finansministeriets publikationer 22/2017, https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/80013/VM_22_2017.pdf?sequence=1&isAllowed=y

[18] NIST Risk Management Framework (RMF) https://csrc.nist.gov/projects/risk-management/about-rmf

- NIST, (National Institute of Standards and Technology) www.nist.gov

[19] FIPS 140-3 Security Requirements for Cryptographic Modules, https://csrc.nist.gov/publications/detail/fips/140/3/final

- FIPS, FIPS-standarderna (Federal Information Processing Standards) www.nist.gov

[20] PCI Security Standards, ml. PA-DSS (Payment Application Data Security Standards) Official PCI Security Standards Council Site - Verify PCI Compliance, Download Data Security and Credit Card Security Standards

[21] ** Transport- och kommunikationsverket 211/2019 O Anvisning om bedömning av elektroniska identifieringstjänster https://www.traficom.fi/sites/default/files/media/regulation/O211_Anvisning_om_bed%C3%B6mning_av_elektroniska_identifieringstj%C3%A4nster_211_2019_O_SV.pdf

[22] Tillämpningsanvisning för EU:s förordning om tillitsnivåer (EU) 2015/1502 (LOA Guidance 2021) https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/LoA%20guidance%20%282021%29.pdf

- Översättning av versionen från 2016 https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/LOA_Guidance_Final_suomeksi.pdf [översättningen från 2021 läggs till när den är klar]
- På engelska LOA Guidance 2021 https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/LOA_Guidance.pdf
- Samarbetsnätverket (cooperation network) https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Cooperation+Network+Resources

[23] ISO/IEC 15408 Information technology – Security techniques – Evaluation criteria for IT security (s.k. Common Criteria)

- *www.commoncriteriaportal.org/cc CCPART1-3 motsvarar standarden ISO/IEC 15408*

[24] ISO/IEC 18045 Information technology – Security techniques – Methodology for IT security evaluation

- *www.commoncriteriaportal.org/cc CEM motsvarar standarden ISO/IEC 18045*

[25] ISO/IEC 29115 Information technology — Security techniques — Entity authentication assurance framework ISO - ISO/IEC 29115:2013 - Information technology — Security techniques — Entity authentication assurance framework

[26] ** PiTuKri, Säkerhetkriterier för molntjänster, Traficoms publikation 21/2021 https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Traficom_PiTuKri_2020_SE_210506_WEB.pdf

[27] ITU-R TF.1876 (03/2010) Trusted time source for time stamp authority https://www.itu.int/dms_pubrec/itu-r/rec/tf/R-REC-TF.1876-0-201004-I!!PDF-E.pdf

[28] NIST 800-63B, Digital Identity Guidelines, Authentication and Lifecycle Management https://pages.nist.gov/800-63-3/sp800-63b.html

[29] NIST, Face Recognition Vendor Test (FRVT) https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt21]

[30] * Lag om tillhandahållande av digitala tjänster (306/2019) 306/2019 - Författningsändringsregister - FINLEX ®

[31] ** Transport- och kommunikationsverkets rekommendation 212/2021 S, Finnish Trust Network SAML 2.0 Protocol Profile, Dnro Traficom/6194/09.02.00/2020 7.7.2021 [Länk läggs till]

[32] ** Transport- och kommunikationsverkets rekommendation 213/2021 S, OpenID Connect Protocol Profile for the Finnish Trust Network, Traficom/6194/09.02.00/2020, 7.7.2021 [Länk läggs till]

[33] * EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV (EU) 2015/2366 om betaltjänster på den inre marknaden, om ändring av direktiven 2002/65/EG, 2009/110/EG och 2013/36/EU samt förordning (EU) nr 1093/2010 och om upphävande av direktiv 2007/64/EG (**PSD2**, Andra betaltjänstdirektivet – Payment Services Directive) EUR-Lex - 32015L2366 - SV - EUR-Lex (europa.eu)

[34] * KOMMISSIONENS DELEGERADE FÖRORDNING (EU) 2018/389 om komplettering av Europaparlamentets och rådets direktiv (EU) 2015/2366 vad gäller tekniska tillsynsstandarder för stränga kundautentisering och gemensamma och säkra öppna kommunikationsstandarder (**RTS SCA & CSC**) EUR-Lex - 32018R0389 - SV - EUR-Lex (europa.eu)

[35] * Betaltjänstlag 290/2010 290/2010 - Författningsändringsregister - FINLEX ®

[36] Bedömningsmaterial

- Presentation från 2018 om eIDAS och PSD2/RTS-granskning https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kalvot%2010102018%20PSD2-seurantaryhm%C3%A4%20eIDAS-%20ja%20PSD2-RTS-vaatimusten%20vertailu.pdf
- Utlåtandeversion 10102018 med jämförelse av Kommunikationsverkets och Finansinspektionens eIDAS-PSD2-RTS-krav (bestämmelse-excel) https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Lausuntoversio%2010102018%20Vivin%20ja%20Fivan%20eIDAS-PSD2-RTS-vertailu.XLSX

[37] NCSA, Transport- och kommunikationsverkets nationella informationssäkerhetsmyndighet (National Communications Security Authority, NCSA-FI)

- Allmän information om NCSA-FI https://www.kyberturvallisuuskeskus.fi/sv/var-verksamhet/ncsa

[38] SOGIS-MRA (Senior Officers Group for Information Systems, Mutual Re-cognition Agreement), http://www.sogisportal.eu/

- Allmän information om SOGIS MRA https://www.sogis.eu/uk/supporting_doc_en.html#:~:text=The%20document%20%C2%AB%20SOG%2DIS%20Crypto,by%20all%20SOG%2DIS%20participants

[39] ** Kryptografiset vahvuusvaatimukset luottamuksellisuuden suojaamiseen - kansalliset suojaustasot (anvisning 28.11.2018, dnr 190/651/2015) https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/ohje-kryptografiset-vahvuusvaatimukset-kansalliset-suojaustasot.pdf

[40] IANAn (Internet Assigned Numbers Authority)

- IKEv2-föreskrifterna http://www.iana.org/assignments/ikev2-parameters/ikev2-parameters.xhtml
- chiffersviter: http://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml#tls-parameters-4

[41] SOG-IS Crypto Evaluation Shceme Agreed Cryptographic Mechanisms, (version 1.2 January 2020) https://www.sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.2.pdf

[42] RFC 7905 ChaCha20-Poly1305 Cipher Suites for Transport Layer Security (TLS) https://tools.ietf.org/html/rfc7905

[43] RFC 8446 The Transport Layer Security (TLS) Protocol Version 1.3 https://datatracker.ietf.org/doc/html/rfc8446

[44] Krypteringslösningar som godkänns av NSCA-FI-funktionen (1.7.2020 dnr 1240/651/2017, på finska) https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/NCSA_salausratkaisut.pdf

[45] eIDAS samarbetsnätverk, Cooperation Network

- Allmän information om eIDAS Cooperation Network: Cooperation Network Resources - eID User Community - CEF Digital (europa.eu)

[46] eIDAS - Cryptographic requirements for the Interoperability Framework, TLS and SAML, Version 1.2, 31 August 2019 https://ec.europa.eu/cefdigital/wiki/download/attachments/82773108/eIDAS%20Cryptographic%20Requirement%20v.1.2%20final.pdf?version=2&modificationDate=1571068651805&api=v2

[47] *** ETSI TS 119 312 V1.3.1 (2019-02) Electronic Signatures and Infrastructures (ESI); Cryptographic Suites https://ec.europa.eu/cefdigital/wiki/display/EIDTECHSUB/Security+Profile+v+1.3

[48] NIST SP 800-52 Rev. 2, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations https://csrc.nist.gov/publications/detail/sp/800-52/rev-2/final

[49] OpenID Connect [kompletteras]

[50] SAML [kompletteras]

[51] Financial-grade API (FAPI) WG Financial-grade API (FAPI) WG | OpenID

[52] ETSI MSS, ETSI TS 102 204 V1.1.4 (2003-08) Mobile Commerce (M-COMM); Mobile Signature Service; Web Service Interface

[53] RFC 7519 JSON Web Token (JWT) https://tools.ietf.org/html/rfc7519

[54] Webtrust, CA/Browser Forum https://cabforum.org/webtrust-for-cas/

- Webtrust Trust Services Principles and Criteria for Certification Authorities och Webtrust for Certification Authorities - SSL Baseline Requirements Audit Criteria

[55] Information Security Forum (ISF)

- Standard of Good Practice https://www.securityforum.org/solutions-and-insights/standard-of-good-practice-for-information-security-2020/
- INFORMATION RISK ASSESSMENT METHODOLOGY 2 (IRAM2) https://www.securityforum.org/solutions-and-insights/information-risk-assessment-methodology-iram2/

[56] ISRS 4400, International Standard on Related Services (ISRS) 4400, https://www.iaasb.org/publications/isrs-4400-uudistettu-toimeksiannot-erikseen-sovittujen-toimenpiteiden-suorittamisesta

[57] ISAE 3000, International Standard on Assurance Engagements (ISAE) 3000 Revised, Assurance Engagements Other than Audits or Reviews of Historical Financial Information https://www.iaasb.org/publications/basis-conclusions-international-standard-assurance-engagements-isae-3000-revised-assurance

[58] Vahti-anvisningarna https://www.suomidigi.fi/sv/ohjeet-ja-tuki/vahti-anvisningar

[59] Informationshanteringsnämndens rekommendationer https://vm.fi/sv/rekommendationer

[60] Finansinspektionens föreskrifts- och anvisningssamling Föreskriftssamling - Regelverk - www.finanssivalvonta.fi

[61] Finansinspektionen, Standard 2.4, Kundkännedom – åtgärder mot penningtvätt och finansiering av terrorism https://www.finanssivalvonta.fi/sv/regelverk/foreskriftssamling/organisation-av-verksamheten-i-foretag-under-tillsyn/2.4/

[62] Europeiska centralbankens SREP cyber risk questionnaire https://www.eba.europa.eu/regulation-and-policy/supervisory-review-and-evaluation-srep-and-pillar-2/guidelines-on-ict-risk-assessment-under-the-srep

[63] BIS, Bank for International Settlements

- External audits of banks External audits of banks (bis.org)
- Supplemental note to External audits of banks - audit of expected credit loss Supplemental note to External audits of banks - audit of expected credit loss (bis.org)
- The internal audit function in banks http://www.bis.org/publ/bcbs223.htm

[64] IIA, The Institute of Internal Auditors www.theiia.fi

[65] ** [Transport- och] Kommunikationsverkets anvisning 214/2016 O om anmälning av identifieringstjänster och betrodda tjänster https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/Ohje_214_2016_O_tunnistus_ja_luottamuspalveluiden_ilmoitukset_SV.pdf

[66] ETSIs standarder för betrodda tjänster

- För aktuella versioner se (med sökningen Digital Signatures och/eller ESI - Electronic Signatures and Infrastructures) Download ETSI ICT Standards for free

*** Tillhandahållare av betrodda tjänster

- ETSI EN 319 401 ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); **General Policy Requirements** for Trust Service Providers
- ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers **issuing certificates**; Part 1: General requirements
- ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers **issuing EU qualified certificates**
- ETSI EN 319 421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers **issuing Electronic Time-Stamps**
- ETSI EN 319 521 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for **Electronic Registered Delivery Service Providers**

*** Betrodda tjänster

- EN 319 412-1 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: **Overview and common data structures**
- EN 319 412-2 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to **natural persons**
- EN 319 412-3 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to **legal persons**
- EN 319 412-4 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for **web site certificates**
- EN 319 412-5 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements

- ETSI EN 319 422 Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and **time-stamp token profiles**

- ETSI EN 319 102-1 Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and **Validation**

- ETSI EN 319 522 Electronic Signatures and Infrastructures (ESI); **Electronic Registered Delivery Services**
  - ETSI EN 319 522-1 Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services; Part 1: **Framework and architecture**
  - ETSI EN 319 522-2 Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 2: **Semantic contents**
  - ETSI EN 319 522-3 Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 3: **Formats**
  - ETSI EN 319 522-4-1 Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 4: Bindings; Sub-part 1: **Message delivery bindings**

- ETSI EN 319 522-4-2 Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 4: Bindings; Sub-part 2: **Evidence and identification bindings**
- ETSI EN 319 522-4-3 Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 4: Bindings; Sub-part 3: **Capability/requirements bindings**

[67] Enisa Assessment of Standards related to eIDAS (December 14, 2018) https://www.enisa.europa.eu/publications/assessment-of-standards-related-to-eidas

- Allmänt om ENISA, The European Union Agency for Network and Information Security, www.enisa.europa.eu

[68] *** ETSIs tekniska specifikationer

- ETSI TS 119 441 Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing **signature validation** services
- ETSI TS 119 442 Electronic Signatures and Infrastructures (ESI); Protocol profiles for trust service providers providing AdES digital **signature validation** services
- ETSI TS 119 102-1 Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and **Validation**
- ETSI TS 119 102-2 Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 2: Signature **Validation Report**

- ETSI TS 119 172-4 Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 4: Signature applicability rules (validation policy) for European qualified electronic signatures/seals **using trusted lists**

- ETSI TS 119 511 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing **long-term preservation of digital signatures** or general data using digital signature techniques
- ETSI TS 119 512 Electronic Signatures and Infrastructures (ESI); Protocols for trust service providers providing **long-term data preservation services**

- ETSI TS 119 524 Electronic Signatures and Infrastructures (ESI); Testing Conformance and **Interoperability of Electronic Registered Delivery Services**

[69] FINAS (Finnish Accreditation Service) Säkerhets- och kemikalieverket (Tukes) ackrediteringsenhet https://www.finas.fi/sites/sv/Sidor/default.aspx

[70] Auditing Framework for TSPs, Guidelines for Trust Service Providers, Version 1.0 - December 2014 Auditing Framework for TSPs — ENISA (europa.eu)

[71] De europeiska ackrediteringsorganisationernas samarbetsorgan EA (European Co-operation for Accreditation): EA Certification Committee Reference Paper; ETSI / EA Recommendations regarding; Preparation for Audit under EU Regulation (EU) No 910/2014 Article 20.1. (har inte publicerats på internet)

- Allmänt European co-operation for Accreditation - European Accreditation (european-accreditation.org)

[72] ***ETSI EN 319 403-1 Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for **conformity assessment bodies** assessing Trust Service Providers

[73] ***ETSI TS 119 403-2 V1.2.1 (2019-04) Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 2: Additional requirements for **Conformity Assessment Bodies** auditing Trust Service Providers that issue Publicly-Trusted Certificates https://www.etsi.org/deliver/etsi_ts/119400_119499/11940302/01.02.01_60/ts_11940302v010201p.pdf

[74] ***ETSI TS 119 403-3 V1.1.1 (2019-03) Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 3: Additional requirements for **conformity assessment bodies** assessing EU qualified trust service providers

[75] ** Transport- och kommunikationsverkets anvisning 215/2019 O om bedömningsberättelser för betrodda e-IDAS-tjänster https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/O215_Hyv%C3%A4ksytyn_eIDAS-luottamuspalvelun_arviointikertomus_%289_10_2019%29.pdf

5.2 Sammandrag av utlåtanden