Motivering till och tillämpning av domännamnsföreskriften

Innehåll

Föreskriftens bakgrund och rättsgrund

Bakgrunden till en förnyad föreskrift är behovet att uppdatera den nuvarande föreskriften så att den motsvarar den förändrade lagstiftningen och verksamhetsmiljön. Domännamnssystemet har identifierats som kritisk infrastruktur vars upprätthållande och förvaring som tillförlitligt, störningstolerant och säkert är centralt med tanke på att förvara integritet och speciellt viktigt för en kontinuerlig och stabil funktion av internet. Nya krav för domännamnsverksamheten uppställs speciellt i Europaparlamentets och rådets direktiv 2022/2555 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet), vilket har medfört krav på att även den nationella lagstiftningen och därigenom domännamnsföreskriften ska ändras.

Genom NIS 2-direktivet har lagen om tjänster inom elektronisk kommunikation (917/2014) ändrats genom författningen (x/xxxx). Lagen om tjänster inom elektronisk kommunikation har dessutom ändrats genom författningen 661/2024, som trätt i kraft den 30 november 2024, och genom vilken namnskyddade produkter har fogats till definitionen av skyddat namn och märke. Dessa författningars konsekvenser har beaktats vid beredningen av domännamnsföreskriften. Motiveringspromemorian till domännamnsföreskriften innehåller dessutom hänvisningar till kommissionens genomförandeförordning 2024/2690[1] som utfärdats med stöd av NIS 2-direktivet samt till lagen om hantering av cybersäkerhetsrisker (x/xxxx) (nedan "cybersäkerhetslagen") som inte gäller alla registrarer utan bland annat DNS-tjänsteleverantörer som är centrala aktörer inom digital infrastruktur.

Den gällande domännamnsföreskriften är från år 2016. Innehållet i den är delvis gammalt. Utöver de ändringar som beror på den förändrade lagstiftningen är avsikten med den uppdaterade föreskriften att höja mognadsnivån för registrarernas informationssäkerhet och förbättra kvaliteten på domännamnsverksamheten med beaktande av den respons som Transport- och kommunikationsverket har fått av kunderna.

Denna domännamnsföreskrift är den andra versionen av föreskrift M 68. Den första versionen av domännamnsföreskriften M 68 av den 15 juni 2016 (nedan "gammal föreskrift") upphävs genom en ny version av föreskriften. Den nya versionen innehåller dock reglering som funnits i den gamla föreskriften. I den nya versionen har föreskriftens uppbyggnad uppdaterats. För sakinnehållet har föreskriften uppdaterats enligt följande:

[1] Kommissionens genomförandeförordning (EU) 2024/2690 av den 17 oktober 2024, om fastställande av regler för tillämpningen av direktiv (EU) 2022/2555 vad gäller tekniska och metodologiska specifikationer för riskhanteringsåtgärder för cybersäkerhet och närmare angivelse av i vilka fall en incident ska anses vara betydande med avseende på leverantörer av DNS-tjänster, registreringsenheter för toppdomäner, leverantörer av molntjänster, leverantörer av datacentraltjänster, leverantörer av nätverk för leverans av innehåll, leverantörer av utlokaliserade driftstjänster, leverantörer av utlokaliserade säkerhetstjänster, leverantörer av marknadsplatser online, leverantörer av sökmotorer, leverantörer av plattformar för sociala nätverkstjänster och tillhandahållare av betrodda tjänster.

Föreskrift 68 version 1	Föreskrift 68 version 2	Ändring
1 § Föreskriftens syfte	-	Strukits som onödigt
2 § Tillämpningsområde	Punkt 1 Tillämpningsområde	Formuleringen har preciserats
3 § Definitioner	Punkt 2 Definitioner	Definitioner har fogats med anledning av NIS 2-direktivet.
4 § Uppgifter som lämnas i anmälan om bedrivande av registrarverksamhet 5 § Anmälans form och inlämnande av den till den myndighet som förvaltar domännamnsregistret	Punkt 3.1 Form och inlämnande av anmälan om registrarens bedrivande av verksamhet till den myndighet som förvaltar domännamnsregistret	Uppgifter som krävs av registrarer har uppdaterats och paragraferna i den gamla föreskriften har integrerats i en punkt
7 § Registrarens rådgivningsskyldighet gentemot användare	Punkt 3.3 Registrarens rådgivningsskyldighet gentemot användare	Underpunkt om produkter med skyddad beteckning har fogats
8 § Anteckning av uppgifter om användare i domännamnsregistret	Punkt 3.4 Anteckning av uppgifter om användare i domännamnsregistret	Uppgifter som ska antecknas i domännamnsregistret har uppdaterats och skyldigheter som försäkrar att uppgifterna är korrekta har fogats
-	Punkt 3.5 Anteckning av uppgifter om återförsäljare i domännamnsregistret	Ny skyldighet för registrarer som anlitar återförsäljare
9 § Registrarens gränssnitt mot domännamnsregistret för den myndighet som förvaltar domännamnsregistret	Punkt 3.6 Registrarens gränssnitt mot domännamnsregistret för den myndighet som förvaltar domännamnsregistret	Formuleringen har preciserats
10 § Överföring av domännamn till en annan användare	Punkt 3.7 Överföring av domännamn till en annan användare	En skyldighet att anmäla domännamnsanvändaren hur och var användaren kan få domännamnets

		överföringskod har fogats
11 § Byte av registrar	Punkt 3.8 Byte av registrar	En skyldighet att anmäla domännamnsanvändaren hur och var användaren kan få koden för registrarbyte har fogats
16 § Datamaterial	Punkt 5.3 Datamaterial och säkerhetskopiering	Skyldighet om säkerhetskopiering har fogats
19 § Hantering av ändringar	Punkt 5.6 Hantering av ändringar	Skyldighet om säkerhetsuppdateringar har fogats
22 § Ikraftträdande	Punkt 7 Ikraftträdande	Föreskriften träder i kraft samtidigt som den nationella lagstiftning som ges med anledning av NIS 2-direktivet
23 § Erhållande av upplysningar och publicering	-	Strukits som onödigt

Motiveringspromemorian till domännamnsföreskriften har också uppdaterats.

Transport- och kommunikationsverkets föreskrift baserar sig på lagen om tjänster inom elektronisk kommunikation. Bestämmelser om domännamn ingår främst i 21 kap. i lagen samt i följande kapitel:

- 1 kap. 3 § Definitioner, 21 och 35 punkten

- 36 kap. 295 § Domännamnsavgift

- 39 kap. 312 § Elektronisk delgivning

- 43 kap. 343 § Överklagande hos marknadsdomstolen

- 45 kap. 351 § Ikraftträdande

I 21 kap. i lagen om tjänster inom elektronisk kommunikation föreskrivs om Transport- och kommunikationsverkets befogenheter enligt följande:

Transport- och kommunikationsverket får enligt 165 § 3 mom. i lagen om tjänster inom elektronisk kommunikation meddela närmare föreskrifter om hur anmälan ska göras och om innehållet i den. I 1 mom. i paragrafen åläggs registrar en skyldighet att göra en anmälan om inledande av registrarverksamhet. I 2 mom. åläggs registrar skyldighet att informera om ändringar i de uppgifter som

anmälts, nedläggning av verksamheten och förbudsbeslut som Transport- och kommunikationsverket meddelat med stöd av 171 § 2 mom.

Transport- och kommunikationsverket får enligt 166 § 3 mom. i lagen om tjänster inom elektronisk kommunikation meddela föreskrifter om de konfigurationer som är nödvändiga för att domännamnet ska fungera och om domännamnets form, antal tecken och tillåtna tecken. Enligt 1 mom. i paragrafen får ett domännamn bestå av minst två och högst 63 tecken. En bestämmelse om domännamnets form finns i 2 mom. i paragrafen.

Transport- och kommunikationsverket får enligt 167 § 5 mom. i lagen om tjänster inom elektronisk kommunikation utfärda närmare föreskrifter om hur registreringen tekniskt ska genomföras och om de uppgifter som ska lämnas i samband med registreringen samt om identifiering av domännamnsanvändaren och säkerställandet av uppgifterna om domännamnsanvändaren. Enligt 1 mom. i paragrafen ska registraren eller den som handlar på registrarens vägnar i domännamnsregistret anteckna korrekta och uppdaterade uppgifter som identifierar domännamnsanvändaren och det registrerade domännamnet samt den e-postadress som ska användas för hörande och delgivning.

Transport- och kommunikationsverket får enligt 168 § 4 mom. i lagen om tjänster inom elektronisk kommunikation meddela föreskrifter om det tekniska genomförandet och tidsfristerna i fråga om överföring av domännamn och byte av registrar. Enligt 1 mom. i paragrafen kan domännamnsanvändaren överföra domännamnet till en annan användare under domännamnets giltighetstid. Registraren ska göra överföringen inom rimlig tid från mottagandet av begäran. Enligt 2 mom. i paragrafen kan domännamnsanvändaren byta registrar under domännamnets giltighetstid. Registraren ska vidta de åtgärder som krävs för att byta registrar inom rimlig tid från mottagandet av begäran.

Transport- och kommunikationsverket får enligt 170 § 2 mom. i lagen om tjänster inom elektronisk kommunikation meddela närmare föreskrifter om information som ges till användare av domännamn, om information som ska göras offentligt tillgänglig, om givande av åtkomst till uppgifter, samt om riktlinjer och förfaranden, om informationssäkerheten i registrarens verksamhet samt om när en störning som avses i 1 mom. 7 punkten ska anses vara betydande och om innehållet i anmälan samt anmälans utformning och hur den lämnas in. Enligt 1 mom. 1 punkten i paragrafen ska en registrar innan ett domännamn registreras tillhandahålla behövlig information enligt lagen om tjänster inom elektronisk kommunikation om kraven på domännamnets innehåll och form. Enligt 1 mom. 6 punkten i paragrafen ska en registrar sörja för informationssäkerheten i sin verksamhet. Enligt 1 mom. 7 punkten i paragrafen ska en registrar utan dröjsmål meddela Transport- och kommunikationsverket om dess förmedling av domännamn är utsatt för betydande kränkningar av eller hot mot informationssäkerheten eller för någonting annat som väsentligen förhindrar eller stör den. Enligt punkten ska registraren också anmäla hur länge störningen eller hotet beräknas pågå, om vilka verkningar störningen eller hotet har, om avhjälpande åtgärder samt om åtgärder för att förhindra att störningen upprepas. Enligt 1 mom. 8 punkten i paragrafen ska en registrar göra sina riktlinjer och förfaranden för att säkerställa att uppgifterna i domännamnsregistret överensstämmer med bestämmelserna i 167 § 1 mom. offentligt tillgängliga. Enligt 1 mom. 9 punkten i paragrafen ska registraren utan obefogat dröjsmål göra andra registreringsuppgifter om domännamn än personuppgifter offentligt

tillgängliga. Enligt 1 mom. 10 punkten i paragrafen ska registraren i enlighet med dataskyddslagstiftningen och avgiftsfritt ge åtkomst till registreringsuppgifter om domännamn samt svara den som legitimt begär åtkomst till registreringsuppgifter utan obefogat dröjsmål och senast inom 72 timmar från mottagandet av en laglig och på tillbörligt sätt motiverad begäran. Enligt 1 mom. 11 punkten i paragrafen ska registraren göra riktlinjer och förfaranden för utlämnande av registreringsuppgifter om domännamn offentligt tillgängliga.

Beredning av föreskriften

Utkastet till föreskriften har beretts vid Transport- och kommunikationsverket. Intressentgrupperna ges möjlighet att lämna skriftliga utlåtanden om föreskriftsutkastet under perioden x.x. - x.x.2025. Begäran om utlåtande, utkastet till föreskrift och motiveringspromemorian till föreskriften har publicerats på adressen utlåtande.fi. Transport- och kommunikationsverket har på sina webbsidor informerat om remissbehandlingen samt via e-post till registrarerna. I samband med remissbehandlingen har även kommunikationsministeriet, finansministeriet och Ålands landskapsregering per e-post begärts att lämna ett utlåtande.

Remissrespons

Remissresponsen beskrivs här eller på en separat bilaga till promemorian.

Bedömning av föreskriftens konsekvenser

De viktigaste ändringarna hänför sig till registrarernas ökande informationsskyldigheter samt till säkerställandet av att domännamnsanvändarnas uppgifter är korrekta. Genom ändringarna blir även tillsynsmyndighetens och användarnas tillgång till information bättre. Genom ändringen av föreskriften bedöms också att antalet fel i domännamnsregistret minskar.

Föreskriften bedöms ha positiva effekter för hanteringen av registrarernas informationssäkerhet. Syftet med föreskriften är att ändra anmälningsblanketten för registrarer bland annat så att en ny registrar ska uppfylla ett självutvärderingsverktyg eller en -metod som Transport- och kommunikationsverket angett för att det ska vara möjligt att utvärdera informationssäkerhetsnivån i registrarens verksamhet. Föreskriftsändringarna bedöms höja mognadsnivån för domännamnsregistrarernas informationssäkerhet när nya registrarer ska bedöma sin informationssäkerhet och dokumentera sina observationer innan registrarverksamheten inleds. Avsikten är att även de nuvarande registrarerna ska fylla i självutvärderingsverktyget inom ramen för övergångsperioden. Ifyllandet av verktyget bedöms medföra en liten administrativ börda för registrarer. Ändringen bedöms inte medföra några avsevärda ekonomiska konsekvenser för registrarer därför att registrarerna redan i dag måste sörja för informationssäkerheten i sin verksamhet, och kraven för hanteringen av informationssäkerheten har preciserats redan i den gamla föreskriften.

I framtiden skulle registrarerna i samband med anmälan om registrarverksamheten eller i samband med anmälan om ändringar i registrarverksamheten meddela om registraren är leverantör av DNS-tjänster, och om den är, meddela namnen för de namnservrar den förvaltar. Med stöd av 25 § 1 mom. i cybersäkerhetslagen utövar Transport- och kommunikationsverket

tillsyn förutom över registrarer också över leverantörer DNS-tjänster av vilka en stor del är registrarer. Ändringen av föreskriften bedöms ha en positiv konsekvens med tanke på tillsyn över DNS-tjänsteleverantörer. Ändringen bedöms främja en sanningsenlig bild av de DNS-tjänsteleverantörer som Transport- och kommunikationsverket har tillsyn över när anmälan om tillhandahållandet av DNS-tjänster görs så enkelt som möjligt för aktörerna i samband med anmälan om registrarverksamheten eller i samband med anmälan om ändringar i registrarverksamheten. Ändringen bedöms inte ha några betydande konsekvenser för registrarerna.

Skyldigheterna som åläggs registrarerna och gäller att identifiera domännamnsanvändaren, säkerställa att uppgifterna lämnats i domännamnsregistret är korrekta och att domännamnsanvändarens e-postadress fungerar tekniskt bedöms ha positiva konsekvenser på säkerställandet av att domännamnsanvändarnas uppgifter är korrekta. Syftet är att man inte ska införa några felaktiga uppgifter i domännamnsregistret. Genom att säkerställa e-postadressens tekniska funktion strävar man efter att förbättra domännamnsanvändarnas tillgång till information och rättsskydd med beaktande av att Traficom på basis av 312 § i lagen om tjänster inom elektronisk kommunikation har rätt att delge domännamnsanvändaren en handling per e-post. Ändringen av föreskriften bedöms medföra en del kostnader för registrarer med anledning av eventuell process- och systemutveckling. Registrarerna kommer dock att avgöra sätten att identifiera domännamnsanvändarna och sätten att verifiera uppgifterna, så registrarerna kan själva avgöra hur de uppfyller föreskriftens skyldigheter på det mest ändamålsenliga sättet för att åstadkomma det eftersträvade resultatet. Om det inte är möjligt att uppnå de önskade konsekvenserna genom denna föreskrift kan Transport- och kommunikationsverket senare bestämma närmare om identifiering av användare och om verifiering av uppgifterna.

Att bedöma kostnaderna och den administrativa bördan som uppfyllandet av föreskriftens skyldigheter medför är svårt därför att registrarerna sinsemellan är olika samt därför att registrarerna själva kan bedöma hur de genomför åtgärderna på ett ändamålsenligt sätt. Vissa aktörer har redan fungerande processer och för den delen medför de nya skyldigheterna nödvändigtvis inte några väsentliga extra kostnader. De eventuella kostnader och administrativa skyldigheter som föreskriften medför är sannolikt större i början än på lång sikt. De nu ålagda skyldigheterna och eventuella ytterligare kostnader som beror på dem är i en ändamålsenlig relation i förhållande till syftena med lagen om tjänster inom elektronisk kommunikation samt med domännamnsanvändarnas bättre ställning.

Föreskriftsändringarna bedöms förbättra domännamnsverksamhetens kvalitet när mognadsnivån för informationssäkerheten och skyldigheterna att lämna ut uppgifter ökar, vilket även återspeglas som positiva konsekvenser för domännamnsanvändare. Ändringarna bedöms dock eventuellt medföra tilläggskostnader för domännamnsanvändare, om registrarerna höjer sina priser med anledning av ändringarna i föreskriften. Med anledning av skyldigheten att identifiera användare kan registreringen av domännamn vara något arbetssammare och långsammare för användare beroende på vilka sätt för identifiering och säkerställande som registrarerna väljer.

Föreskriftsändringarna bedöms öka Transport- och kommunikationsverkets administrativa börda. Genomgången av registrarens självbedömningsverktyg eller -metod som fylls i samband med anmälan om registrarverksamhet kräver betydligt mer tid än i dag av dem som handlägger anmälningar om registrarverksamheten. Transport- och kommunikationsverket ska dessutom ge råd till registrarer om föreskriftens innehåll.

Detaljmotivering

1 Tillämpningsområde

Domännamnsföreskriften tillämpas på domännamn under toppdomänen fi och ax samt på förmedling och administrering av dem.

Domännamn under toppdomänen fi och toppdomänen ax

Enligt 3 § 35 punkten i lagen om tjänster inom elektronisk kommunikation avses med *domännamn* en adress på internet under den nationella toppdomänen fi eller toppdomänen ax för landskapet Åland i form av ett namn som består av bokstäver, siffror eller andra tecken eller en kombination av dem.

Lagen om tjänster inom elektronisk kommunikation tillämpas inte på andra toppdomäner och inte heller på domännamnsverksamhet i samband därmed, och därför lämnas de utanför denna föreskrifts tillämpningsområde. Andra toppdomäner är exempelvis de generiska domännamnen .com och .net samt de nationella toppdomänerna som .se för Sverige.

Förmedling och administrering av domännamn samt bedrivande av verksamhet som registrar

Med förmedling av domännamn avses registreringar i domännamnsregistret. Enligt 164 § 2 mom. i lagen om tjänster inom elektronisk kommunikation får endast verksamhetsutövare som enligt 165 § har lämnat in en anmälan om registrarverksamhet, (registrar), får göra registreringar i domännamnsregistret. Enligt 167 § 1 mom. i lagen om tjänster inom elektronisk kommunikation ska ett domännamn registreras på domännamnsanvändaren. Registraren ska i domännamnsregistret anteckna korrekta och uppdaterade uppgifter som identifierar domännamnsanvändaren samt den e-postadress som ska användas för hörande och delgivning.

Domännamnsförvaltning omfattar alla åtgärder som en registrar vidtar för att upprätthålla uppgifterna om domännamn i domännamnsregistret. Enligt exempelvis 170 § 1 mom. 2 punkten i lagen om tjänster inom elektronisk kommunikation ska en registrar uppdatera uppgifterna i domännamnsregistret och enligt 5 punkten på begäran av domännamnsanvändaren avregistrera ett domännamn innan dess giltighetstid har löpt ut (uppsägning). Med domännamnsförvaltning avses även förmågan att göra anteckningar i domännamnsregistret med hjälp av tekniska arrangemang som Transport- och kommunikationsverket har fastställt.

Förutom förmedling och förvaltning av domännamn omfattar registrarernas verksamhet andra skyldigheter som inte direkt hänför sig till förvaltning eller förmedling av ett enskilt domännamn. Enligt 165 § 2 mom. i lagen om tjänster inom elektronisk kommunikation ska Transport- och kommunikationsverket utan dröjsmål informeras om ändringar i de uppgifter som registraren har anmält. Enligt 170 § 1 mom. 6 och 7 punkten ska en registrar utan dröjsmål meddela Transport- och kommunikationsverket om dess förmedling av domännamn är utsatt för betydande kränkningar av eller hot mot informationssäkerheten eller för någonting annat som

väsentligen förhindrar eller stör den. I 21 kap. i lagen om tjänster inom elektronisk kommunikation har registrarerna även ålagts andra informationsskyldigheter.

Föreskriftens tillämpningsområde i fråga om domännamn under toppdomänen ax

Enligt punkt 1 i föreskriften tillämpas föreskriften också på domännamn under toppdomänen ax, på förmedling och administrering av dem samt på ax-registrarernas verksamhet. Transport- och kommunikationsverket vill dock påminna om att regleringen om domännamn under toppdomänen fi och ax i punkt 3.6 i föreskriften avviker från varandra i fråga om registrarernas tekniska gränssnitt mot domännamnsregistren. En registrar som förmedlar och administrerar domännamn under toppdomänen fi kan anteckna domännamn i Transport- och kommunikationsverkets domännamnsregister via verkets EPP-gränssnitt. Om registraren använder Transport- och kommunikationsverkets EPP-gränssnitt som ett tekniskt gränssnitt, måste den uppfylla Katakri-kraven som gäller informationssäkerhet enligt punkt 5.7 i föreskriften. Vid registrering och administrering av domännamn under toppdomänen ax är det enda tillgängliga tekniska gränssnittet, åtminstone för tillfället, webbläsargränssnittet på adressen whois.ax. Föreskriften kan vid behov senare kompletteras med tekniska gränssnittsspecifikationer som gäller förmedling och administrering av domännamn under toppdomänen ax.

Enligt 163 § 1 mom. i lagen om tjänster inom elektronisk kommunikation tillämpas 21 kap. om domännamn också på domännamn under toppdomänen för landskapet Åland (toppdomänen ax) samt på domännamnsverksamhet och registreringstjänster för domännamn i samband därmed. Enligt 163 § 2 mom. ska regleringen om det domännamnsregister som förvaltas av Transport- och kommunikationsverket också tillämpas på registret över domännamn under toppdomänen ax. Enligt motiveringen till paragrafen ska överföring av befogenhet mellan riket och landskapet Åland när det gäller administrering av toppdomänen ax i enlighet med nuvarande praxis regleras genom en särskild avtalsförordning.

I motiveringen till lagen om tjänster inom elektronisk kommunikation konstateras det även att en anmälan om inledande av registrarverksamhet enligt 165 § 1 mom. i lagen för toppdomänen ax ska göras till Ålands landskapsregering.

Grundlagsutskottet har i sitt utlåtande (18/2014 rd - RP 221/2013 rd) konstaterat att i ett ärende där riket har lagstiftningsbehörighet har rikets myndighet i regel också behörighet i landskapet Åland. Genom en överenskommelseförordning enligt 32 § i självstyrelselagen för Åland kan dock uppgifter som hör till riksförvaltningen överföras på landskapets förvaltningsmyndigheter. Med den myndighet som förvaltar domännamnsregistret och nämns i 165 § 1 mom. i lagen om tjänster inom elektronisk kommunikation avses för toppdomänen ax således Ålands landskapsregering.

2 Definitioner

I punkt 2 i föreskriften beskrivs de definitioner som används i föreskriften. I föreskriften definieras inte igen de begrepp som definierats i lagen om tjänster inom elektronisk kommunikation, och å andra sidan har definitionerna utformats så att de inte står i strid mot definitionerna i lagen.

Domännamnets överföringskod

Med domännamnets överföringskod avses en av den myndighet som förvaltar domännamnsregistret (Transport- och kommunikationsverket eller Ålands

landskapsregering) angiven kod med vilken ett domännamn kan överföras från en användare till en annan.

Kod för registrarbyte

Med kod för registrarbyte avses i föreskriften en kod med vilken förvaltningen av ett domännamn kan överföras från en registrar till en annan. I regel skapas koden av den gamla registraren. I undantagsfall kan den myndighet som förvaltar domännamnsregistret skapa en kod om den gamla registraren av någon anledning försummar sina skyldigheter enligt lagen om tjänster inom elektronisk kommunikation.

Gammal registrar

Med gammal registrar avses i föreskriften en registrar som avstår från förvaltningen av ett domännamn vid registrarbyte.

Ny registrar

Med ny registrar avses i föreskriften en registrar som tar emot förvaltningen av ett domännamn vid registrarbyte.

Domännamnsregister

Med domännamnsregister avses enligt 164 § 1 mom. i lagen om tjänster inom elektronisk kommunikation Transport- och kommunikationsverkets register över domännamn under toppdomänen fi och med fi-rot en databas med teknisk information om domännamn för styrning av internettrafiken. Ax-domännamnsregistret och ax-roten drivs enligt nuvarande praxis av Ålands landskapsregering på basis av en överenskommelseförordning som föreskrivs med stöd av 32 § i självstyrelselagen för Åland (1144/1991).

Leverantör av DNS-tjänster

Med leverantör av DNS-tjänster avses en aktör som tillhandahåller a) allmänna rekursiva tjänster för att lösa domännamnsfrågor till internetslutanvändare, eller b) auktoritativa tjänster för att lösa domännamnsfrågor för användning av tredje part, med undantag för rotnamnsservrar. Om registraren utövar verksamhet enligt antingen den ena eller den andra definitionen är registraren en leverantör av DNS-tjänster oberoende av dess storlek. Definitionen motsvarar definitionen i NIS 2-direktivet.

Övriga definitioner

Till övriga delar iakttas i föreskriften definitionerna i 21 kap. i lagen om tjänster inom elektronisk, t.ex. *domännamnsanvändare*. En domännamnsanvändare är en juridisk person, en enskild näringsidkare eller en annan sammanslutning eller en fysisk person som ett domännamn kan registreras på.

3 Krav som gäller registrarer

I 3 punkten i föreskriften fastställs registrarernas anmälnings- och rådgivningsskyldigheter, de uppgifter som identifierar domännamnsanvändaren, kraven på gränssnitt för domännamnsregistret samt proceduren för överföring av domännamn och byte av registrar.

Med avvikelse från den gamla föreskriften listas i föreskriften inte längre några uppgifter som identifierar registraren eftersom bestämmelser som gäller uppgifter om registrarer anges i 165 § i lagen om tjänster inom elektronisk kommunikation.

En registrar kan frivilligt anmäla andra uppgifter i domännamnsregistret, till exempel en särskild e-postadress för skötseln av dagliga frågor av teknisk karaktär.

Enligt 165 § 2 mom. i lagen om tjänster inom elektronisk kommunikation ska Transport- och kommunikationsverket utan dröjsmål informeras om ändringar i de uppgifter som registraren har anmält. Enligt motiveringen till bestämmelsen ska registrarerna uppdatera ändringar i uppgifterna omedelbart. Transport- och kommunikationsverket rekommenderar att registrarerna uppdaterar ändringar i uppgifterna i Transport- och kommunikationsverkets databas inom tre (3) dagar.

3.1 Anmälans form och inlämnande av den till den myndighet som förvaltar domännamnsregistret

Enligt 165 § 1 mom. i lagen om tjänster inom elektronisk kommunikation ska en registrar göra en anmälan till den myndighet som förvaltar domännamnsregistret innan den inleder sin verksamhet. Enligt motiveringen till lagen om tjänster inom elektronisk kommunikation avses med den myndighet som förvaltar domännamnsregistret i praktiken Transport- och kommunikationsverket för toppdomänen fi och Ålands landskapsregering för toppdomänen ax. I lagrummet specificeras de uppgifter som man ska ge i samband med anmälan.

I punkt 3.1 i föreskriften ingår en bestämmelse om på vilket sätt anmälan om bedrivande av registrerarverksamhet enligt 165 § 1 mom. i lagen om tjänster inom elektronisk kommunikation ska göras. Paragrafen gäller också anmälningar om ändringar i de uppgifter som registrarerna har lämnat. Anmälningarna för fi-domännamn ska lämnas i Transport- och kommunikationsverkets elektroniska webbtjänst på www.traficom.fi. Anmälningarna för ax-domännamn ska lämnas på adressen www.whois.ax.

Den som ska göra en anmälan om bedrivande av registrarverksamhet får i Transport- och kommunikationsverkets elektroniska system basinformation om alla rättigheter och skyldigheter för registrarer. Senast i anslutning till anmälan kan den som gör anmälan ta del av de rättigheter och skyldigheter som bygger på författningar och som gäller den anmälda verksamheten. Information finns också på förhand tillgänglig på Transport- och kommunikationsverkets webbplats för att verket ska kunna säkerställa att de som bedriver eller har för avsikt att bedriva registrarverksamhet är medvetna om rättigheterna och skyldigheterna i anslutning till verksamheten.

Enligt 170 § 1 mom. 6 punkten i lagen om tjänster inom elektronisk kommunikation ska en registrar sörja för informationssäkerheten i sin verksamhet. Enligt 171 § 1 mom. 4 punkten i lagen om tjänster inom elektronisk kommunikation har Transport- och kommunikationsverket till uppgift att övervaka registrarverksamheten.

När en ny registrar gör anmälan om registrarverksamhet bör den på förhand kunna bedöma sin informationssäkerhetsnivå. För bedömningen ska den myndighet som hanterar domännamnsregistret ange verktyget eller metoden självutvärdering. Avsikten är att registraren med hjälp av verktyget eller metoden själv observerar om den har sådana brister i sin säkerhetsnivå som ska åtgärdas. Den dokumentation som uppstår som ett resultat av självutvärderingsverktyget eller -metoden bör lämnas in till den myndighet som förvaltar domännamnsregistret. Dokumentationen behövs för tillsyn, eftersom med den kan myndigheten bedöma vilka registrarer som speciellt bör prioriteras när det gäller övervakning av och stöd med informationssäkerheten.

Förut om de uppgifter som anges i 165 § 1 mom. i lagen om tjänster inom elektronisk kommunikation ska registraren uppge om den också är en leverantör av DNS-tjänster samt namnen på de namnservrar registraren förvaltar. Med stöd av 26 § 1 mom. i cybersäkerhetslagen utövar Transport- och kommunikationsverket tillsyn även över leverantörer DNS-tjänster. Majoriteten av de leverantörer av DNS-tjänster som Traficom har tillsyn över är i praktiken också registrarer, och tillsynsuppgifterna är delvis överlappande. För att undvika lämnandet av överlappande uppgifter samlas uppgifterna om registrarer och leverantörer av DNS-tjänster samtidigt och förvaras i samma system.

Uppgiften om huruvida en registrar över huvud taget är en leverantör av DNS-tjänster är viktig med tanke på tillsyn eftersom Transport- och kommunikationsverkets tillsyn enligt cybersäkerhetslagen endast riktas in på leverantörer av DNS-tjänster. Vad gäller registrarer som inte är leverantörer av DNS-tjänster riktar Transport- och kommunikationsverket in sin tillsyn enligt lagen om tjänster inom elektronisk kommunikation. Registrarerna åläggs också ge namnen på de namnservrar de förvaltar, om sådana finns. Att ge namnen på namnservrarna hjälper att bedöma om registraren de facto också är en leverantör av DNS-tjänster. Uppgifterna om namnen på namnservrar och förvaltarna av dem hjälper att utreda eventuella incidenter och problem.

De registrarer som anmält sig i domännamnsregistret innan föreskriften träder i kraft bör anmäla uppgifter som saknas på en ändringsanmälan eller på något annat sätt som myndigheten som förvaltar domännamnsregistret har angett.

Transport- och kommunikationsverket publicerar på sina internetsidor och på andra elektroniska tjänster uppgifter om registrarer så som beskrivs i dataskyddsbeskrivningen för register med fi-domännamn och lösningar för fi-domännamnstvister. Transport- och kommunikationsverket lämnar ut uppgifter som inte publiceras på elektroniska tjänster under de förutsättningar som anges i lagen om offentlighet i myndigheternas verksamhet (621/1999) eller med stöd av annan specialreglering.

3. 2 Anmälningar till kunder om ändringar i registrarens verksamhet

I punkt 3.2 i föreskriften fastställs närmare de anmälningar som en registrar ska ge till sina kunder, om den lägger ned sin verksamhet eller har fått uppgift om ett beslut som den myndighet som förvaltar domännamnsregistret har fattat och där registraren förbjuds att bedriva registrarverksamhet under högst ett år.

I punkt 3.2 i föreskriften fastställs att om verksamheten läggs ned ska registraren informera varje kund om detta. Syftet är att säkerställa att kunden de facto får informationen. Information som enbart läggs ut på exempelvis registrarens webbplats kan inte anses vara tillräcklig, även om den bör läggas ut även där. Med hjälp av kundernas e-postadresser kan registraren effektivt rikta informationen, men det kan också vara nödvändigt att försöka nå kunderna per telefon.

Enligt 165 § 2 mom. i lagen om tjänster inom elektronisk kommunikation ska Transport- och kommunikationsverket och kunderna, om verksamheten läggs ned, informeras om detta minst två veckor i förväg. Enligt motiveringen till lagrummet gäller detsamma om verksamheten avbryts. Såsom det konstaterats i lagmotiveringen om anmälningar om inledande av verksamhet görs även anmälningar om upphörande av verksamhet som gäller ax-domännamn till Ålands landskapsregering. Syftet med bestämmelsen är att säkerställa domännamnsanvändarens tillgång till ett fungerande domännamn och att säkerställa att användaren hinner byta domännamnsadministratör innan registrarens

verksamhet upphör. Transport- och kommunikationsverket rekommenderar att registrarerna, av de skäl som framgår av motiveringen till lagen, informerar Transport- och kommunikationsverket och kunderna även när verksamheten avbryts tillfälligt.

I punkt 3.2 i föreskriften åläggs registrarerna att informera varje kund även när registrarens verksamhet avbryts tillfälligt med anledning av förbudsbeslut som den myndighet som förvaltar domännamnsregistret har fattat. Om registraren bryter mot lag eller bestämmelser, föreskrifter eller beslut som utfärdats med stöd av lag, kan Transport- och kommunikationsverket enligt 171 § 2 mom. i lagen om tjänster inom elektronisk kommunikation förbjuda registraren att registrera domännamn eller göra anteckningar som gäller domännamn i domännamnsregistret. Enligt bestämmelsen ger Transport- och kommunikationsverket dessförinnan en anmärkning där Transport- och kommunikationsverket ålägger registraren att inom en rimlig tid rätta till felet eller försummelsen.

Enligt motiveringen till lagrummet kan ett förbudsbeslut överklagas och det skulle verkställas i praktiken genom att hindra att registraren via tekniska gränssnitt kommer åt att göra registreringar eller ändringar i domännamnsregistret. Kunderna måste i en sådan situation hitta en ny registrar och kravet att registraren ska informera om saken är sålunda ett viktigt minimikrav från domännamnsanvändarens synpunkt. Syftet med föreskriften är att säkerställa att kunden de facto får informationen.

3.3 Registrarens rådgivningsskyldighet gentemot användare

I punkt 3.2 i föreskriften fastställs närmare på vilket sätt registrarerna ska sörja för den informations- och rådgivningsskyldighet som avses i 170 § 1 mom. 1 punkten i lagen om tjänster inom elektronisk kommunikation. Enligt bestämmelsen ska en registrar innan ett domännamn registreras tillhandahålla behövlig information enligt lagen om tjänster inom elektronisk kommunikation om kraven på domännamnets innehåll och form. I punkt 3.3 i föreskriften fastställs närmare vilka lagstadgade uppgifter som ska lämnas till användarna.

Enligt punkt 3.3 i föreskriften ska en registrar, utöver vad som bestäms i 3 § 21 punkten och 166 § i lagen om tjänster inom elektronisk kommunikation, innan den registrerar ett domännamn, ge användare följande närmare uppgifter om de förutsättningar som gäller domännamnets innehåll och form:

1) krav på domännamnets form enligt punkt 4.1 i föreskriften

2) uppgifter om namn som är införda i Finlands handels-, förenings-, stiftelse- eller partiregister

3) uppgifter om varumärken som är införda i Finlands eller Europeiska gemenskapens varumärkesregister

4) uppgifter om geografiska beteckningar införda i Europeiska unionens register över produkter med skyddad beteckning.

I motiveringen till 170 § 1 mom. 1 punkten i lagen om tjänster inom elektronisk kommunikation beskrivs registrarernas informations- och rådgivningsskyldighet. En registrar ska ge sina kunder och aktörer som vill registrera domännamn den information om förutsättningarna för registrering av domännamn som avses i 166 § i en lättillgänglig och utförlig form innan domännamnet registreras. Informationen bör vara tillgänglig på ett sådant sätt att domännamnssökanden kan förvissa sig om de

krav som gäller domännamnens utformning och innehåll innan domännamnet registreras. I synnerhet när det gäller skyddade namn och märken bör kunderna känna till förutsättningarna innan domännamnen registreras. Syftet med bestämmelsen är att felaktiga och lagstridiga domännamnsregistreringar ska kunna undvikas. Registraren måste för egen del aktivt se till att domännamnsregistreringar är förenliga med lagen. I motiveringen till bestämmelsen konstateras det särskilt att det slutliga ansvaret för att ett domännamn är lagligt fortfarande kommer att finnas hos domännamnsanvändaren.

Enligt 166 § 1 mom. i lagen om tjänster inom elektronisk kommunikation får ett domännamn bestå av minst två och högst 63 tecken. Enligt 2 mom. 1 punkten i bestämmelsen får ett domännamn vid registreringstidpunkten inte motsvara någon annans skyddade namn eller märke, om inte domännamnsanvändaren kan ge en godtagbar grund för registreringen av domännamnet. I 2 punkten i bestämmelsen anges att domännamnet inte vid registreringstidpunkten får likna någon annans skyddade namn eller märke, om domännamnet registreras i uppenbart vinnings- eller skadesyfte.

Enligt definitionen i 3 § 1 mom. 21 punkten i lagen om tjänster inom elektronisk kommunikation avses med skyddat namn eller skyddat märke ett namn eller märke som är infört i handels-, varumärkes-, förenings-, stiftelse- eller partiregistret eller en inarbetad firma, ett sekundärt kännetecken eller ett varumärke enligt firmalagen (128/1979) eller varumärkeslagen (544/2019) samt namnet på ett offentligt samfund, ett statligt affärsverk, en självständig offentligrättslig inrättning, en offentligrättslig förening samt på en främmande stats beskickning eller på ett organ i dem.

Uppgifter om de namn som är införda i Finlands handels-, förenings-, stiftelse- eller partiregister finns i Patent- och registerstyrelsens (PRS) register och är tillgängliga för allmänheten i PRS webbtjänster. De varumärken som har skyddats genom registrering i Finland finns antingen i PRS varumärkesdatabas eller i Europeiska unionens immaterialrättsmyndighets (EUIPO, European Intellectual Property Office) register. Registrerade produkter med skyddad beteckning finns i EU-kommissionens eAmbrosia-register.

Enligt definitionen i 3 § 1 mom. 21 punkten i lagen om tjänster inom elektronisk kommunikation avses med skyddat namn eller skyddat märke även en inarbetad firma, ett sekundärt kännetecken eller ett varumärke enligt firmalagen eller varumärkeslagen. Sådana icke-registrerade namn och märken finns därför inte i registren ovan. Transport- och kommunikationsverket har i sin avgörandepraxis förhållit sig återhållsamt till sådana krav på återkallande som bygger på ett påstående om att en firma eller ett varumärke hade inarbetats innan det omstridda domännamnet registrerades. Transport- och kommunikationsverkets tvistelösning är en administrativ process där det inte är möjligt att göra en bedömning av en omfattande kännetecknsrättslig bevisning. Kännetecknsrättsliga tvister ska lösas i domstol, medan Transport- och kommunikationsverket ingriper i tydliga rättskränkningar.

I föreskriftens punkt 3.3 ges en hänvisning till krav på domännamnets form i punkt 4.1. Kraven innefattar specificeringar av tillåtna tecken i domännamn, som är bokstäverna a–z och siffrorna 0–9. Tillåtna tecken är också de nationella tecken som räknas upp i föreskriften samt bindestreck-minus. I punkt 4.1 i föreskriften föreskrivs dessutom om andra tekniska detaljer i domännamnens form.

Transport- och kommunikationsverket bestämmer inte på vilket sätt registrarerna ska fullgöra sin informationsskyldighet enligt lag när det gäller de obligatoriska

uppgifterna ovan. Skyldigheten kan fullgöras exempelvis på så sätt att registraren på sin webbplats länkar ett uppdaterat informationsinnehåll som fastställts av Transport- och kommunikationsverket. Transport- och kommunikationsverket har på sin webbplats uppdaterad information om uppgifter som enligt lag är obligatoriska för användarna, och andra nödvändiga anvisningar, till exempel information om Transport- och kommunikationsverkets tvistelösning.

I motiveringen till lagen om tjänster inom elektronisk kommunikation betonas registrarernas ansvar och skyldigheter i den nuvarande verksamhetsmodellen, där registrarerna har en viktig ställning. I motiveringen betonas att domännamnsanvändarnas rättigheter ska värnas om och att domännamnen ska bli korrekt registrerade i domännamnsregistret. Därför anser Transport- och kommunikationsverket att lagen medför en skyldighet för registrarer att omsorgsfullt vägleda sina kunder.

3.4 Anteckning av uppgifter om användare i domännamnsregistret

Punkt 3.4 i föreskriften innehåller närmare föreskrifter om vilka identifieringsuppgifter en registrar ska anteckna om användare vid registrering av domännamn. I fråga om fysiska personer är dessa identifierings- och kontaktuppgifter, användarens för- och efternamn och de uppgifter om adress och telefonnummer som behövs för att nå personen. Till de identifieringsuppgifter om en fysisk person som ska antecknas i registret hör även personbeteckning eller, i avsaknad av den, annan uppgift som identifierar användaren. Utländska fysiska personer har inte nödvändigtvis någon finsk personbeteckning och i så fall anges personens födelsetid som annan uppgift som identifierar användaren.

Identifierings- och kontaktuppgifterna för juridiska personer och övriga organisationer som ska registreras som användare i domännamnsregistret är användarens firma och de adress- och telefonnummeruppgifter som behövs för att nå personen. Som identifieringsuppgift för juridiska personer registreras ett finskt FO-nummer eller, i avsaknad av den, annan uppgift som identifierar användaren, till exempel något annat registreringsnummer. I föreskriften åläggs inte längre till registrering av kontaktpersonens namn, telefonnummer och e-postadress i domännamnsregistret. Registreringen av dessa uppgifter rekommenderas dock fortfarande så att registraren ska få kontakt direkt med rätt instans i eventuella problemsituationer.

Enligt 167 § 1 mom. i lagen om tjänster inom elektronisk kommunikation ska en registrar registrera ett domännamn på domännamnsanvändaren. I motiveringen till momentet konstateras det att en kunds domännamn t.ex. inte får registreras på en registrar och att det med avseende på den faktiska domännamnsanvändarens rättigheter är viktigt att användarregistreringen har gjorts på ett korrekt sätt, särskilt när Transport- och kommunikationsverket utreder oklarheter eller tvister som hänför sig till denna lag.

Föreskriftens punkt 3.4 hänvisar till en bestämmelse i lagen om tjänster inom elektronisk kommunikation, som ålägger registrarerna att alltid i domännamnsregistret anteckna den e-postadress som enligt 167 § i lagen ska användas för hörande och delgivning. I 312 § 2 mom. i lagen om tjänster inom elektronisk kommunikation föreskrivs om Transport- och kommunikationsverkets absoluta rätt att för hörande och delgivning använda den e-postadress som är införd i domännamnsregistret. Därför kan en handling eller ett beslut som gäller domännamn alltid delges genom e-post. Denna så kallad processadress har stor rättslig betydelse och enligt 167 § i lagen är det obligatoriskt för registrarerna att ange den. Med hjälp av en processadress kan Transport- och kommunikationsverket

snabbt delge bindande beslut, eftersom beslutet eller handlingen enligt 312 § 2 mom. i lagen då anses ha delgivits den tredje dagen efter det att meddelandet sändes, om inte något annat visas. En rätt processadress för en domännamnsanvändare är en viktig uppgift och med tanke på användarens rättsskydd är det högst viktigt att den hålls uppdaterad.

Enligt lagen om tjänster inom elektronisk kommunikation är det obligatoriskt att registrera enbart en e-postadress, men lagen eller föreskriften utgör inget hinder för att anmäla andra e-postadresser än de som används för officiella höranden eller delgivningar. Även andra e-postadresser kan anges för Transport- och kommunikationsverkets elektroniska system, om en registrar anser att det är nödvändigt att exempelvis hålla de e-postadresser som används vid behandling av dagliga ärenden av teknisk karaktär i anslutning till domännamnet åtskilda från de obligatoriska processadresserna.

Enligt 167 § i lagen om tjänster inom elektronisk kommunikation ska en registrar anteckna uppdaterade uppgifter om domännamnsanvändare. Enligt motiveringen till paragrafen ansvarar registraren för att de uppgifter som anmäls är korrekta och för att uppgifterna hålls uppdaterade. Om registrarens försummelser leder till att domännamnsanvändaren orsakas skador kan användaren yrka på skadestånd via domstol. Transport- och kommunikationsverket rekommenderar att registraren utan dröjsmål uppdaterar ändringar i användarens uppgifter i domännamnsregistret.

Transport- och kommunikationsverket konstaterar att alla registrarer av domännamn under toppdomänen fi och ax är skyldiga att iaktta dataskyddslagstiftningen i tillämpliga delar vid behandlingen av personuppgifter. Enligt 170 § 1 mom. 9 punkten i lagen om tjänster inom elektronisk kommunikation ska registraren utan obefogat dröjsmål göra andra registreringsuppgifter om domännamn än personuppgifter offentligt tillgängliga. Genom denna föreskrift föreskriver Transport- och kommunikationsverket inte närmare om uppgifter som ska göras offentligt tillgängliga. Enligt 170 § 1 mom. 10 punkten i lagen om tjänster inom elektronisk kommunikation ska registraren ge åtkomst till registreringsuppgifter om domännamn och svara på begäranden om uppgifter. Dataskyddslagstiftningen ska iakttas när det gäller att ge åtkomst till uppgifter och att svara på begäranden om uppgifter. Genom denna föreskrift föreskriver Transport- och kommunikationsverket inte närmare om tillgång till uppgifterna.

Transport- och kommunikationsverket konstaterar också att det är en förvaltningsmyndighet förpliktad av annan lagstiftning som gäller myndighetsverksamhet, t.ex. förvaltningslagen (434/2003). På utlämnande av personuppgifter ur Transport- och kommunikationsverkets domännamnsregister tillämpas lagen om offentlighet i myndigheternas verksamhet (1999/621). Vad gäller offentliggörande av domännamnsuppgifterna på Transport- och kommunikationsverkets webbplats eller i någon annan elektronisk tjänst samt om Transport- och kommunikationsverkets skyldighet att svara på begäranden om domännamnsregistret eller i någon annan elektronisk tjänst anges i 167 § 3 mom. i lagen om tjänster inom elektronisk kommunikation. Transport- och kommunikationsverket publicerar på sina internetsidor och på andra elektroniska tjänster uppgifter om användare av domännamn så som beskrivs i dataskyddsbeskrivningen för register med fi-domännamn och för avgörande av tvister om fi-domännamn.

Enligt 167 § 1 mom. i lagen om tjänster inom elektronisk kommunikation ska registraren eller den som handlar på registrarens vägnar i domännamnsregistret anteckna korrekta och uppdaterade uppgifter som identifierar domännamnsanvändaren samt den e-postadress som ska användas för hörande och

delgivning. I punkt 3.4 i föreskriften anges att en registrar ska identifiera domännamnsanvändaren och säkerställa att uppgifterna som lämnats i domännamnsregistret är korrekta. Genom skyldigheterna i föreskriften säkerställs att i registret antecknas korrekta uppgifter om domännamnsanvändaren. Syftet är att man inte ska införa några felaktiga uppgifter i domännamnsregistret. Om registraren tillhandahåller domännamnsregistreringstjänster både privatpersoner och sammanslutningar ska registraren ha förfaranden för identifiering av både privatpersoner och sammanslutningar och verifiering av uppgifter.

Domännamnsanvändaren ska identifieras åtminstone när domännamnsanvändaren är ny kund hos registraren. Föreskriften förpliktar inte registraren att identifiera domännamnsanvändaren i samband med varje ny registrering i situationer där kunden samtidigt registrerar flera domännamn. Utöver den första registreringen av ett domännamn kan registraren identifiera domännamnsanvändaren riskbaserat. Transport- och kommunikationsverket rekommenderar att domännamnsanvändaren identifieras efter att domännamnet registrerats i situationer där man anmält att domännamnet har använts för olaglig verksamhet. Uppgifter som antecknats om domännamnsanvändaren i domännamnsregistret ska uppdateras.

Privatpersoner kan identifieras på olika sätt, till exempel genom besök då en privatperson styrker sin identitet (t.ex. med pass), med stark autentisering, såsom med nätbankskoder eller med andra elektroniska identifieringstjänster, till exempel med en nationell elektronisk identitet eller med en europeisk e-identitetsplånbok. Om en privatperson styrker sin identitet med en handling bör handlingen inte accepteras om inte den instans som identifierar personen inte får tillräcklig säkerhet om att den uppvisade handlingen verkligen hör till den person som uppvisar den eller om det finns misstanke om att handlingen är förfalskad. Det skulle till exempel inte vara tillräckligt att användaren endast lämnar en bild av sitt identitetsbevis utan någon direkt interaktion med den instans som identifierar personen. Uppgifter om sammanslutningar kan säkerställas till exempel genom att kontrollera att sammanslutningen existerar och att uppgifterna stämmer ur tillförlitliga register, såsom ur handelsregistret, och sedan identifiera identiteten för personen med firmateckningsrätt.

Eftersom det finns många olika sätt för identifiering anger Transport- och kommunikationsverket inte genom denna föreskrift närmare om vilken identifieringsmetod registraren ska använda. Transport- och kommunikationsverket rekommenderar att man använder tjänster för stark autentisering eller någon annan motsvarande identifieringstjänst. Enligt 170 § 1 mom. 8 punkten ska en registrar göra sina riktlinjer och förfaranden för att säkerställa att uppgifterna i domännamnsregistret överensstämmer med bestämmelserna i 167 § 1 mom. offentligt tillgängliga.

Vid identifieringen och säkerställandet av uppgifterna kan registraren anlita tredje parter, till exempel genom att avtala med sin återförsäljare om att återförsäljaren identifierar domännamnsanvändaren. Registraren ansvarar dock för kvaliteten av den tredje parts identifieringstjänster och uppgifternas certifikattjänst om det i domännamnsregistret har antecknats felaktiga uppgifter med anledning av en sådan tredje parts oaktsamhet eller fel.

I punkt 3.4 i föreskriften anges också att en registrar ska säkerställa att e-postadress för domännamnsanvändaren fungerar tekniskt. Den tekniska funktionen säkerställs genom att man till domännamnsanvändarens elektroniska processadress skickar ett e-postmeddelande som förutsätter bekräftelse med en verktygsbaserad identifieringsmetod, såsom en individuell kod som ska returneras på det sätt som

registraren anvisat. Den tekniska funktionen ska säkerställas åtminstone när man registrerar ett nytt domännamn och när registraren får en anmälan om att domännamnsanvändarens e-postadress inte fungerar. Uppgifterna om domännamnsanvändaren ska dock hållas uppdaterade och därför rekommenderar Transport- och kommunikationsverket att registraren med jämna mellanrum kontrollerar e-postadressens tekniska funktion och åtminstone när domännamnet överförs från en registrar till en annan. Transport- och kommunikationsverket rekommenderar också att registraren kontrollerar att domännamnsanvändarens telefonnummer fungerar tekniskt.

3.5 Anteckning av uppgifter om återförsäljare i domännamnsregistret

Till föreskriften fogas en ny punkt som gäller återförsäljare av domännamn. Återförsäljare kan till exempel vara en instans som sköter kundservicen för fi-domännamn och fakturerar kunderna men som inte är en registrar så som avses i lagen om tjänster inom elektronisk kommunikation. Om registraren anlitar återförsäljare i fi-domännamnsverksamheten, är registraren också ansvarig för deras verksamhet.

Registraren ska i domännamnsregistret anteckna uppgifter om man anlitat en återförsäljare vid registrering och administrering av domännamn, och vem denna återförsäljare är. Det har varit möjligt att anteckna uppgifter om återförsäljare i domännamnsregistret även tidigare men i framtiden skulle uppgiften vara obligatorisk. Registraren ska se till att uppgifterna om sina återförsäljare är uppdaterade.

Avsikten med den nya skyldigheten är att förbättra kundservicen för domännamnsanvändare. På basis av meddelanden från kunder kan Transport- och kommunikationsverket konstatera att domännamnsanvändare nödvändigtvis inte vet vem deras registrar är då användarna har skött sina ärenden endast med återförsäljaren. I framtiden kunde Transport- och kommunikationsverket vägleda domännamnsanvändare direkt till återförsäljaren.

3.6 Registrarens gränssnitt mot domännamnsregistret för den myndighet som förvaltar domännamnsregistret

I punkt 3.6 i föreskriften anges krav som gäller hur anteckningar i domännamnsregistret ska genomföras i tekniskt hänseende. Som tekniskt gränssnitt mot Transport- och kommunikationsverkets domännamnsregister ska en registrar använda antingen samma webbläsargränssnitt som Transport- och kommunikationsverkets webbplats har eller det EPP-gränssnitt (Extensible Provisioning Protocol) som Transport- och kommunikationsverket har specificerat och driver.

EPP är ett XML-baserat tekniskt gränssnitt som specificeras i RFC-dokument och som en registrar kan ansluta till från sitt eget kundprogram. Transport- och kommunikationsverket tillhandahåller inget färdigt kundprogram, utan registraren ska själv programmera sitt kundprogram eller anskaffa ett sådant. EPP-gränssnittet är inte obligatoriskt, utan det är ett alternativt sätt till webbläsargränssnittet att göra registreringar och förvalta domännamn. Registrarerna kan också använda båda gränssnitten.

Registrarens kundprogram ska vara kompatibelt med det EPP-gränssnitt som Transport- och kommunikationsverket har specificerat, om registraren använder Transport- och kommunikationsverkets EPP-gränssnitt. Transport- och

kommunikationsverkets EPP-gränssnitt bygger på flera RFC-dokument och är förenligt med dessa till den del det är möjligt.[2]

Kontakta Transport- och kommunikationsverkets kundservice för att få gränssnittsbeskrivningen. Föreskriften ålägger registrarer att genomföra EPP-gränssnittet i enlighet med gränssnittsbeskrivningen. Överensstämmelse med krav ska enligt föreskriften säkerställas med hjälp av Transport- och kommunikationsverkets EPP-testsystem. För att en registrar ska kunna börja använda ett EPP-kundprogram, ska programmet testas först. Programmet ska genomgå de tester i EPP-miljön som Transport- och kommunikationsverket kräver innan registraren kan införa Transport- och kommunikationsverkets EPP-gränssnitt.

Punkt 3.6 i föreskriften innehåller också närmare föreskrifter om de krav som gäller det tekniska genomförandet av registrering och administrering av domännamn under toppdomänen ax. Enligt bestämmelsen ska registraren som tekniskt gränssnitt använda det webbläsargränssnitt som finns på www.whois.ax. Det är ett tekniskt gränssnitt som Ålands landskapsregering tillhandahåller registrarer som gör registreringar i domännamnsregistret och administrerar domännamn under toppdomänen ax.

Om Ålands landskapsregering senare beslutar införa ett eget EPP-gränssnitt, kan föreskriften kompletteras i fråga om tekniska gränssnittsspecifikationer som gäller förmedling och administrering av domännamn under toppdomänen ax.

Enligt 170 § 1 mom. 3 punkten i lagen om tjänster inom elektronisk kommunikation ska en registrar kunna göra anteckningar i domännamnsregistret med hjälp av tekniska arrangemang som Transport- och kommunikationsverket har fastställt. Enligt motiveringen till punkten ska registraren ha tekniska förutsättningar att göra anteckningar i registret och att vidta andra åtgärder. Med tanke på den praktiska verksamheten har de tekniska förutsättningarna en avgörande betydelse, eftersom registraren på domännamnsanvändarens vägnar kan vidta alla åtgärder som gäller domännamnet.

3.7 Överföring av domännamn till en annan användare

I punkt 3.7 i föreskriften fastställs det förfarande som ska tillämpas när en domännamnsanvändare vill överföra sitt domännamn till en annan användare. Den som registrerats som användare i domännamnsregistret ska begära överföring av registraren. Efter att registraren har fått begäran om överföring ska registraren säkerställa att användaren har rätt att överföra domännamnet och begära att den myndighet som förvaltar domännamnsregistret sänder domännamnets överföringskod till användaren.

---

[2] Dokument som gäller EPP-gränssnittet:
IETF RFC 3375 - Generic Registry-Registrar Protocol Requirements: https://www.ietf.org/rfc/rfc3375.txt
IETF RFC 3735 - Guidelines for Extending EPP: https://tools.ietf.org/rfc/rfc3735.txt
IETF RFC 5910 - Domain Name System (DNS) Security Extensions Mapping for the Extensible Provisioning Protocol (EPP): https://tools.ietf.org/rfc/rfc5910.txt
IETF RFC 5730 - Extensible Provisioning Protocol (EPP): https://tools.ietf.org/rfc/rfc5730.txt
IETF RFC 5731 - Extensible Provisioning Protocol (EPP) Domain Name Mapping: https://tools.ietf.org/rfc/rfc5731.txt
IETF RFC 5732 - Extensible Provisioning Protocol (EPP) Host Mapping: https://tools.ietf.org/rfc/rfc5732.txt
IETF RFC 5733 - Extensible Provisioning Protocol (EPP) Contact Mapping: https://tools.ietf.org/rfc/rfc5733.txt
IETF RFC 5734 - Extensible Provisioning Protocol (EPP) Transport over TCP: https://tools.ietf.org/rfc/rfc5734.txt

Registraren genomför överföringen tekniskt. Av registraren krävs ändamålsenlig och tillräcklig noggrannhet för att säkerställa att ingen annan än den som har registrerats som användare av domännamnet ber om överföring. Skyldigheten att försäkra sig om användarens rätt att begära överföring av domännamn är motiverad för att registraren omsorgsfullt ska kunna genomföra denna åtgärd som är viktig med tanke på användarens rättsskydd. Om någon annan än en fysisk person som registrerats som användare av ett domännamn begär överföring av domännamnet, ska registraren be om en ändamålsenlig fullmakt som getts av användaren. Om en juridisk person som registrerats som användare av ett domännamn begär överföring av domännamnet, ska registraren försäkra sig om att den som lämnat begäran är berättigad att handla på användarens vägnar. Med detta avses begäran om nödvändiga ytterligare uppgifter, om de uppgifter som lämnats i anslutning till begäran om överföring av domännamn inte stämmer överens med registrarens uppgifter eller om registraren av något annat skäl har anledning att misstänka exempelvis existensen av användarens viljeuttryck. Transport- och kommunikationsverket rekommenderar starkt att man skriftligen säkerställer att begäran är korrekt.

Registraren ska begära att den myndighet som förvaltar domännamnsregistret sänder domännamnets överföringskod till användaren efter att säkerställt att användaren har rätt att begära överföring. Domännamnets överföringskod definieras i 2 punkten i föreskriften. Enligt definitionen är domännamnets överföringskod en kod angiven av den myndighet som förvaltar domännamnsregistret med vilken ett domännamn kan överföras från en användare till en annan. Därför kan registraren inte själv skapa någon kod. Syftet med förfarandet är att säkerställa att registraren inte utan användarens begäran kan överföra domännamn till en annan användare. Den myndighet som förvaltar domännamnsregistret sänder överföringskoden till användaren som i sin tur kan ge koden till registraren för överföring av domännamnet. Syftet med förfarandet är att säkerställa att användaren av ett domännamn uttryckligen framfört sitt viljeuttryck, när domännamnet överförs till en annan användare.

Enligt punkt 3.7 andra stycket i föreskriften ska registraren överföra domännamnet till den nya användaren inom fem vardagar från det att domännamnsanvändaren har lämnat domännamnets överföringskod och uppgifterna om den nya användaren till registraren. Denna tidsfrist anses vara ett rimligt krav för servicenivå, även om det inte finns något hinder för en snabbare överföring. Enligt 166 § 1 mom. i lagen om tjänster inom elektronisk kommunikation ska registraren göra överföringen inom rimlig tid från mottagandet av begäran.

Om domännamnet inte har överförts inom rimlig tid kan den myndighet som förvaltar domännamnsregistret göra överföringen. I praktiken innebär det till exempel att Transport- och kommunikationsverket sänder domännamnets överföringskod till användaren på användarens begäran. Avsikten är att rollen för den myndighet som förvaltar domännamnsregistret är sekundär. Det är emellertid nödvändigt att säkerställa möjligheten att överföra domännamn i situationer där en registrar av något skäl inte sörjer för sina lagstadgade skyldigheter.

Transport- och kommunikationsverkets uppgift är att övervaka att lagen i fråga om fi-domännamn iakttas, och vid behov kan verket ingripa i registrarernas verksamhet. Vid tillsynen kan Transport- och kommunikationsverket vidta åtgärder enligt 171 § 2 mom. i lagen om tjänster inom elektronisk kommunikation. Transport- och kommunikationsverket kan ge en registrar en anmärkning, ett bindande beslut eller i sista hand ett förbudsbeslut, om registraren bryter mot bestämmelserna i lagen om tjänster inom elektronisk kommunikation eller bestämmelser, föreskrifter och beslut som utfärdats med stöd av den. Förbudsbeslutet innebär att registraren för en tid av

högst ett år förbjuds att registrera domännamn eller göra anteckningar som gäller domännamn i domännamnsregistret. För ax-domännamn skulle tillsynsmyndigheten enligt nuvarande praxis vara Ålands landskapsregering.

Enligt 168 § 1 mom. i lagen om tjänster inom elektronisk kommunikation kan ett domännamn inte överföras om ett ärende som gäller avregistrering av domännamnet är anhängigt vid Transport- och kommunikationsverket. Detta beror på att vid behandling av ett pågående ärende ska man fatta beslut som gäller parterna, vilket inte skulle vara möjligt om parterna kunde bytas under processen. När ett ärende anhängiggörs suspenderar Transport- och kommunikationsverket domännamnet, vilket innebär att detta inte kan överföras till någon annan. Suspenderingen medför inte några andra konsekvenser för användningen av domännamnet, och till exempel tjänster som är anslutna till domännamnet, såsom webbsidor, kan fungera normalt.

Enligt 168 § 2 mom. i lagen om tjänster inom elektronisk kommunikation kan Transport- och kommunikationsverket återföra domännamnet till dess ursprungliga användare om domännamnet har överförts till någon annan utan användarens samtycke och denne begär att registreringen ska korrigeras, och mottagaren av överföringen inte inom utsatt tid anför en godtagbar grund för överföringen. Enligt motiveringen till momentet skyddar bestämmelsen domännamnsanvändaren mot överföringar som uppsåtligen eller av vårdslöshet är felaktiga. Transport- och kommunikationsverkets möjlighet att korrigera en överföring av ett domännamn som inte gjorts i god tro förutsätter enligt motiveringen till momentet starka bevis för att domännamnet har överförts utan den ursprungliga användarens samtycke. Registrarerna ska sörja för en tillräcklig dokumentering av sina överföringsrutiner så att det med tanke på domännamnsanvändarens rättsskydd är möjligt att utreda ärenden i efterhand.

Registrarerna åläggs en ny skyldighet att meddela domännamnsanvändaren tydligt hur och var användaren får domännamnets överföringskod. I det praktiska myndighetsarbetet har det framgått flera situationer där det varit oklart för domännamnsanvändare vad användaren ska göra för att få domännamnets överföringskod. Den nya skyldigheten bidrar till att trygga de domännamnsanvändarens rättigheter som anges i 168 § i lagen om tjänster inom elektronisk kommunikation. Registraren ska göra det möjligt för domännamnsanvändare att skriftligen begära överföring. Registraren kan till exempel på sina webbsidor ge anvisningar om förutsättningar och förfaranden för att få överföringskod.

3.8 Byte av registrar

I punkt 3.8 i föreskriften fastställs det förfarande som ska tillämpas när en domännamnsanvändare vill byta registrar. I princip har domännamnsanvändaren två alternativa sätt att göra det. Användaren kan begära att den nya registraren skaffar koden för registrarbyte från den gamla registraren. Alternativt kan användaren också begära koden för registrarbyte från den gamla registraren, och sända den till den nya registraren. Med andra ord får den nya registraren koden antingen av den gamla registraren eller av användaren, vartefter den kan börja förvalta domännamnet.

Koden för registrarbyte definieras i punkt 2 i föreskriften. Enligt definitionen avses med kod för registrarbyte en kod med vilken förvaltningen av ett domännamn kan överföras från en registrar till en annan. I regel skapas koden av den gamla registraren. Begreppen gammal registrar och ny registrar definieras också i den ovan nämnda punkten. Med gammal registrar avses en registrar som avstår från

förvaltningen av ett domännamn vid registrarbyte, och med ny registrar en registrar som tar emot förvaltningen av ett domännamn vid registrarbyte.

Enligt bestämmelsen i föreskriften ska den gamla registraren säkerställa att användaren eller den nya registraren har rätt att begära koden för registrarbyte. I praktiken krävs ändamålsenlig och tillräcklig noggrannhet av den gamla registraren för att säkerställa att ingen annan än den som har registrerats som användare av domännamnet ber om byte av registrar. Om någon annan framställer begäran, ska denne visa upp en tillräcklig fullmakt för att kunna vidta rättshandlingen. Vid behov kan registraren exempelvis kontakta användaren för att kontrollera ärendet.

Den gamla registraren ska sända koden till den som begärt att få den inom fem vardagar från att den berättigade begäran lämnades. Om den gamla registraren inte har sänt koden för registrarbyte till den nya registraren eller till användaren inom utsatt tid, kan den nya registraren begära att den myndighet som förvaltar domännamnsregistret sänder koden för registrarbyte till användaren.

Enligt motiveringen till 168 § 3 mom. i lagen om tjänster inom elektronisk kommunikation om byte av registrar ska registraren, efter att domännamnsanvändaren har underrättat registraren om sin vilja att byta registrar, inom en rimlig tid vidta de åtgärder som krävs för bytet och främja bytet. Med rimlig tid avses i Transport- och kommunikationsverkets föreskrift fem vardagar, men det finns inget hinder för en snabbare service. Om domännamnet inte inom rimlig tid skulle överföras till en ny registrar för förvaltning, kunde den myndighet som förvaltar domännamnsregistret göra överföringen. I praktiken skulle till exempel Transport- och kommunikationsverket sända koden för registrarbyte till användaren.

I punkt 3.8 i föreskriften förutsätts det också att begäran om registrarbyte ska göras skriftligen, till exempel per e-post. På så sätt är det vid behov i efterhand möjligt att utreda om tidsfristen har gått ut eller inte, eller andra oklarheter vid förfarandet.

Registrarerna åläggs en ny skyldighet att meddela domännamnsanvändaren tydligt hur och var användaren får koden för registrarbyte. I det praktiska myndighetsarbetet har det framgått flera situationer där det varit oklart för domännamnsanvändare vad användaren ska göra för att få koden för registrarbyte. Den nya skyldigheten bidrar till att trygga de domännamnsanvändarens rättigheter som anges i 168 § i lagen om tjänster inom elektronisk kommunikation. Registraren ska göra det möjligt för domännamnsanvändare att skriftligen begära överföring. Registraren kan till exempel ge anvisningar om förutsättningar och förfaranden för att få koden för registrarbyte på sina webbsidor.

Enligt motiveringen till 168 § 3 mom. i lagen om tjänster inom elektronisk kommunikation om byte av registrar kan en domännamnsanvändare fritt byta registrar när som helst. Det krävs inga särskilda skäl för byte av registrar. Momentet reglerar inte domännamnsanvändarens och registrarens avtalsförhållande, utan de avtals- eller konsumenträttsliga frågor som sammanhänger med överföringen avgörs med stöd av annan lagstiftning. I motiveringen till 171 § i lagen om tjänster inom elektronisk kommunikation konstateras att Transport- och kommunikationsverket inte har befogenhet att avgöra avtalstvister mellan domännamnsanvändare och registrarer. Enligt 303 § 2 mom. i lagen om tjänster inom elektronisk kommunikation omfattar Transport- och kommunikationsverkets beslutanderätt inte frågor som gäller avtalsförhållanden eller ersättningsansvar mellan företag och abonnenter. På avtalen mellan ett företag och en konsument tillämpas konsumentskyddslagen (38/1978) som innehåller reglering t.ex. av avtalsvillkor, marknadsföring av tjänster och distansförsäljning. Behörig myndighet i

konsumentreglering är konsumentombudsmannen vars centrala uppgift är att övervaka att konsumentskyddslagen och flera andra lagar som stiftats för att skydda konsumenter följs. Konsumentombudsmannen behandlar i regel inte enstaka tvister. De behandlas av konsumenträttsrådgivare och konsumenttvistenämnden. Mer information om konsumentskyddet finns på Konkurrens- och konsumentverkets webbplats www.kkv.fi.

4 kap. Krav som gäller domännamn

4.1 Domännamnets form

I punkt 4.1 i föreskriften fastställs de tecken som är tillåtna i domännamn, nämligen bokstäverna a–z, siffrorna 0–9 och bindestreck-minus. Tabellen i punkt 4.1 i föreskriften omfattar i regel de tecken där finska, svenska och samiska bokstäver skiljer sig från latinska. Enligt föreskriften är tillåtna tecken de nationella tecken som specificeras i listan.

Bindestreck-minus specificeras med en Unicode-kod i tabellen. Enligt punkt 4.1 i föreskriften får ett domännamn inte börja eller sluta med ett bindestreck-minus. Detta bygger på RFC-dokumentet 1035[3]. Dessutom föreskrivs det att ett domännamn inte får börja med tecknen xn--. Detta beror på att de är reserverade som förtecken för ACE-kodade IDN-domännamn (Internationalized Domain Names) som innehåller nationella tecken. Enligt föreskriften börjar ett domännamn som innehåller nationella tecken i ACE-format (ASCII Compatible Encoding) alltid med tecknen xn--. Kraven baserar sig på RFC-dokumenten RFC 3492[4] och RFC 3490[5].

Enligt 166 § 1 mom. i lagen om tjänster inom elektronisk kommunikation får ett domännamn bestå av minst två och högst 63 tecken. Denna begränsning är förenlig med RFC-dokumentet 1034[6].

4.2 Namnservrar

I punkt 4.2. i föreskriften föreskrivs om konfigurationer av namnservrar med domännamn. Kravet gäller enbart domännamn som är införda tillsammans med namnservrar i domännamnsregistret. Domännamn behöver inte ha några konfigurationer av namnservrar. Namnservrar ska avregistreras i domännamnsregistret om en domännamnsanvändare fortfarande vill reservera sitt domännamn utan att det har några anslutna funktioner som en e-post eller en webbplats.

Minst två av varandra oberoende namnservrar ska konfigureras med ett domännamn. Detta säkerställer att domännamnet fungerar även om det uppstår ett fel i en av namnservrarna. Transport- och kommunikationsverket har fastställt att antalet namnservrar får vara högst tio. Namnservrarna är oberoende av varandra när namnservrarna fungerar på olika servrar och IP-adresser och bakom olika internetförbindelser.

Alla namnservrar ska kunna nås av datornätet internet och Transport- och kommunikationsverket ska kunna granska konfigurationerna med namnserverförfrågningar. Transport- och kommunikationsverket kontrollerar

[3] IETF 1035 Domain names - implementation and specification: http://www.ietf.org/rfc/rfc1035.txt
[4] IETF RFC 3492 Punycode: A Bootstring Encoding of Unicode for Internationalized Domain Names in Applications (IDNA): http://www.ietf.org/rfc/rfc3492.txt
[5] IETF RFC 3490 Internationalizing Domain Names in Applications (IDNA): http://www.ietf.org/rfc/rfc3490.txt
[6] IETF RFC 1034 Domain names - concepts and facilities: https://www.ietf.org/rfc/rfc1034.txt

regelbundet för alla namnservrar att de fungerar. Om en eller flera namnservrar inte fungerar eller om konfigurationerna av namnservrarna är felaktiga, skickar Transport- och kommunikationsverket ett e-postmeddelande med anmärkning till registraren eller till den av registraren uppgivna e-postadressen till den som underhåller namnservrarna.

Enligt föreskriften ska namnservrarna vara försedda med NS-poster (Name Server) där alla namnservrar för ett domännamn har konfigurerats. NS-posterna ska anvisa till servrar för vilka en IP-adress har konfigurerats i A-posten eller i AAAA-posten eller båda i namntjänsten. NS-posterna kan endast vara namnservrar för vilka ett domännamn de facto har konfigurerats. NS-posterna ska vara förenliga med uppgifterna i fi-roten.

Enligt föreskriften ska den SOA-post (Start of Authority) som bestämmer konfigurationen av namnservern för ett domännamn motsvara följande krav:

1) i fältet MNAME (Master Name) ska namnet på den primära namnservern för domännamnet finnas,

2) i fältet RNAME (Responsible Name) ska en fungerande e-postadress finnas för den aktör som ansvarar för underhåll av namnservrarna. E-postadressen ska konfigureras utan tecknet @, som ersätts med punkt, till exempel hostmaster.domain.fi. Bästa sättet att konfigurera en hostmaster-adress i fältet RNAME är att följa RFC 2142.[7]

Transport- och kommunikationsverket rekommenderar att serienumren och klockorna för SOA-posten inte väsentligt avviker från de internetstandarder och -rekommendationer som publicerats. Transport- och kommunikationsverkets rekommendationer är följande:

```
example.com.  3600  SOA  dns.example.com. hostmaster.example.com. (
                           1999022301          ; serial YYYYMMDDnn
                           86400               ; refresh (  24 hours)
                           7200                ; retry   (   2 hours)
                           3600000             ; expire  (1000 hours)
                           172800 )            ; minimum (   2 days)
```

Den rekommenderade formen för serienummer är YYYYMMDDnn, där YYYY avser år, MM månad, DD dag och nn är ett löpande nummer vars värde ökar med ett vid varje uppdatering. Dagens första version är 01. Med hjälp av serienummer är det möjligt att kontrollera att domännamnets samtliga namnservrar har samma zone-poster. Ett serienummer får inte vara noll (0).

Värdena refresh och retry inverkar på hur ofta de sekundära namnservrarna kontrollerar om domännamnets namnserverinformation har ändrats på den primära namnservern. Värdet retry fastställer den tid under vilken namnserverinformationen söks på nytt, om den föregående sökningen misslyckats.

[7] IETF RFC 2142 Mailbox Names for Common Services, Roles and Functions: http://www.ietf.org/rfc/rfc2142.txt

Värdet expire anger hur lång tid en namnserver förvarar en gammal zone-fil i en situation där det inte är möjligt att söka en ny fil.

Värdet Minimum TTL (time to live) fastställer en standard livslängd för RR-posterna (resource record). I vissa fall är det motiverat att fastställa ett lägre TTL-värde än det rekommenderade, till exempel vid förändringar av namnservrar.

Transport- och kommunikationsverkets rekommendationer:

Transport- och kommunikationsverket rekommenderar att överföring av domännamnsinformation (AXFR, DNS zone transfer protocol) förhindras för utomstående.

Dessutom rekommenderar Transport- och kommunikationsverket att namnservrarna inte returnerar rätt information vid förfrågan om namnserverns programversion. Att återställa den rätta programversionen kan riskera informationssäkerheten, om det exempelvis finns ett känt informationssäkerhetsproblem i den version av namnserverprogrammet som används.

5 Hantering av registrarens informationssäkerhet

I punkt 5 i föreskriften behandlas kraven för informationssäkerhet vid förmedling av domännamn. Kraven bygger på 170 § 1 mom. 6 punkten i lagen om tjänster inom elektronisk kommunikation, enligt vilken en registrar ska sörja för informationssäkerheten i sin verksamhet. Enligt motiveringen till punkten ska registraren fastställa detaljerade och tillräckliga anvisningar med tanke på hot mot informationssäkerheten. Registraren ska förvissa sig om att händelser som är relevanta för informationssäkerheten noteras. Dessutom ska registraren ingripa när det konstateras problem och avvikelser i informationssäkerhetssituationen.

Med informationssäkerhet avses enligt 3 § 1 mom. 28 punkten i lagen om tjänster inom elektronisk kommunikation administrativa och tekniska åtgärder genom vilka det säkerställs att information är tillgänglig endast för dem som har rätt att använda den, att informationen inte kan ändras av andra än dem som har rätt till detta samt att informationen och informationssystemen kan utnyttjas av dem som har rätt att använda informationen och systemen. Informationssäkerhet innebär m.a.o. åtgärder för att säkerställa informationens konfidentialitet, integritet, autenticitet och tillgång till information.

I föreskriften beskrivs de minimikrav för hantering av informationssäkerheten som alla registrarer ska uppfylla i sin verksamhet. Syftet med kraven är att säkerställa en grundläggande informationssäkerhetsnivå i registrarverksamheten, som i sin tur ligger till grund för att säkerställa informationssäkerheten i servicen. Kraven fokuserar i synnerhet på att informationssäkerhet hanteras med hjälp av kontinuerlig utveckling, planering, genomförande och bedömning. Syftet med föreskriften är även att minska på negativa konsekvenser av informationssäkerhetsriskerna för registrarverksamheten och användarna av domännamn.

Leverantör av DNS-tjänster ska förutom skyldigheterna i domännamnsföreskriften även iaktta kommissionens genomförandeförordning 2024/2690. I bilagan till förordningen fastställs de tekniska och metodologiska specifikationerna för riskhanteringsåtgärder för cybersäkerhet för de entiteter som omfattas av förordningens tillämpningsområde. Europeiska unionens cybersäkerhetsbyrå ENISA och de nationella behöriga myndigheterna enligt direktivet (EU) 2022/2555 kan ge vägledning för att stödja berörda entiteter vid identifieringen, analysen och bedömningen av risker i samband med genomförandet av de tekniska och

metodologiska specifikationer som rör fastställandet och upprätthållandet av en ändamålsenlig riskhanteringsram.

5.1 Hänsynstagande till informationssäkerheten

Informationssäkerheten utgör en viktig del av kvaliteten på den registrarverksamhet som registraren bedriver. Hänsynstagandet till de olika delområdena i informationssäkerheten vid förmedling är viktigt i alla livscykler för tjänsten: vid planering, genomförande och underhåll av tjänsten samt när tjänsten tas ur bruk. För att informationssäkerheten ska ombesörjas rutinmässigt varje dag, är det motiverat att registraren fastställer processer och rutiner för att genomföra informationssäkerheten.

Registraren ska ha dokumenterade metoder för att sörja för informationssäkerheten. De uppdaterade dokumenten skapar en grund för en systematisk utveckling och hantering av informationssäkerheten och hjälper till att rikta investeringarna i informationssäkerhet. Utifrån dokumentationen kan också Transport- och kommunikationsverket vid behov verifiera att registraren iakttar sina skyldigheter att sörja för informationssäkerheten.

Det finns flera olika faktorer som ska beaktas vid genomförandet av informationssäkerheten och i de dokument som beskriver det. I föreskriften räknas upp de sakhelheter som ska beaktas, men det ställs inga exakta krav på hur helheterna egentligen ska beaktas. Orsaken är att företagen genomför den ändamålsenliga informationssäkerheten på olika sätt, beroende på bl.a. vilka tjänster som företaget tillhandahåller. Minimikraven, som ingår i flera av sakhelheterna i 5.1, behandlas någon annanstans i föreskriften. Det väsentliga i punkt 5.1 i föreskriften är att registraren ska identifiera de krav som gäller för dess verksamhet samt de rutiner som ska tillämpas för att kraven ska uppfyllas.

Nedan finns exempel enligt sakhelhet på faktorer för att sörja för informationssäkerheten. Förteckningen innehåller också hänvisningar till de minimikrav som Transport- och kommunikationsverket har uppställt.

1. Administrativ säkerhet

   - Styrdokument för informationssäkerhet (vanligen t.ex. informationssäkerhetspolicy och -arkitektur), genom vilka organisationens ledning visar de övergripande målen och de allmänna principerna för informationssäkerheten samt sitt engagemang i att genomföra informationssäkerheten.

   - Processer och hantering av dessa

   - Riskhantering och kontinuitet (se punkt 5.2 i föreskriften)

   - Dokumentationsrutiner och -system

   - Auditerings- och övningsförfaranden

2. Personalsäkerhet

   - Ansvar och skyldigheter i anslutning till personalens informationssäkerhet

   - Personalens informationssäkerhetskompetens och utveckling av den

- Bakgrundskontroller
- Nyckelpersonsrisker
- Förebyggande av farliga ansvars- och uppgiftshelheter
- Arbetsrotation i syfte att upptäcka missbruk
- Anvisningar för förfarandet när arbetsförhållandet slutar
- Missbruk och underlåtenhet att iaktta instruktioner från personalens sida

3. Maskinvaru-, programvaru- och telekommunikationssäkerhet
   - Hantering av sårbarheter
   - Observation av informationssäkerhetsincidenter se punkterna 5.4–5.5 i föreskriften)
   - Hantering av ändringar (se punkt 5.6 i föreskriften)
4. Datamaterial- och driftsäkerhet
   - Säkerställande av informationens konfidentialitet, integritet, autenticitet och tillgänglighet
   - Klassificering av datamaterial och behandling enligt klassificeringen (se punkt 5.3 i föreskriften)
   - Ansvar för registret för användarrättigheter: delning, ändring och radering av användarrättigheter
   - Förebyggande av att användarrättigheter samlas på hög
   - Förhindrande av att utomstående kommer åt den hanterings- och konfigurationsinformation som anknyter till förmedling av domännamn samt kundernas fakturerings-, kund- och logguppgifter
   - Förvaring och förstöring av datamaterial
5. Fysisk säkerhet
   - Fysiskt läge för lokaler och omgivningens säkerhet
   - Åtkomsthantering
   - Strukturellt skydd

Föreskriften förutsätter att ovan angivna sakhelheter (1–5) ska beaktas i de olika skedena av livscykeln för förmedling av domännamn. Det innebär att registraren ska beakta informationssäkerheten när den planerar, genomför och underhåller tjänsten samt när den tar tjänsten ur bruk.

Föreskriften förutsätter att registraren ska ha uppdaterade dokument om på vilket sätt den genomför informationssäkerheten i sin verksamhet. Föreskriften fastställer inte vilka alla olika dokument registraren ska ha, utan registraren får själv bedöma

det. Det viktiga är att dokumentationen är uppdaterad och att det utifrån dokumentationen är möjligt att fastslå att alla de delområden av informationssäkerheten som räknas upp i punkt 5.1 i föreskriften har beaktats i verksamheten. Leverantörerna av DNS-tjänster ska dock dessutom iaktta kommissionens genomförandeförordning 2024/2690 och på så sätt utfärda åtminstone de dokument som krävs i genomförandeförordningen.

5.2 Riskhantering

Med informationssäkerhetsrisker avses en sådan oavsiktlig eller avsiktlig faktor som äventyrar konfidentialitet, integritet, autenticitet eller tillgänglighet vid förmedlingen av domännamn. Skillnaden mellan informationssäkerhetsrisker och informationssäkerhetshot är att informationssäkerhetsriskernas sannolikhet och verkningar har bedömts.

Informationssäkerhetsrisker kan t.ex. orsakas av

- mänskliga misstag
- brister i eller underlåtenhet att iaktta instruktioner till personalen
- stölder eller skadegörelser
- fel eller funktionsstörningar i apparater, system eller program
- spridning av skadliga program
- förstöring av datamaterial
- brand eller vattenskada,
- fel och försummelser begångna av en underleverantör eller en aktör som ingår i samarbetsnätverket.

Med riskhantering avses en process som syftar till att identifiera risker, minska sannolikheten för risker och/eller konsekvenser av risker till en godtagbar nivå och bibehålla den uppnådda nivån. Syftet med riskhanteringen är att skydda organisationen och dess förmåga att utföra sina funktioner med beaktande av ekonomiska omständigheter.

Genom kraven på riskhanteringen strävar man efter att säkerställa att registraren är medveten om följderna om riskerna realiseras och huruvida de riskminskande åtgärderna är tillräckliga. Målsättningen för riskhanteringen är bland annat att

- snabba upp återhämtningen efter informationssäkerhetsproblem
- minska kostnader och skador som förorsakas av informationssäkerhetsproblem
- rikta investeringar som förbättrar informationssäkerheten vid förmedlingen av domännamn
- förbättra kvaliteten och produktiviteten i förmedlingen av domännamn
- ekonomiskt optimera de risker som hänför sig till förmedlingen av domännamn

- förebygga risker mot förmedling av domännamn.

Bland annat följande standarder och publikationer om riskhantering har getts ut: ISO/IEC 27005[8], ISO/IEC 27001[9], NIST 800-30 Risk Management Guide[10] och NIST CSF 2.0[11].

Standarder, anvisningar och bästa praxis ändras tidvis. I föreskriften åläggs ingen skyldighet att iaktta en viss standard. Riskhanteringsmodeller skiljer sig hos olika aktörer, och en enda modell som skulle passa för alla finns inte.

Föreskriften förutsätter att registraren ska identifiera riskerna i sin verksamhet och verksamhetens kontinuitet och att den ska hantera riskerna. Med hantering avses att registraren fastställer en godtagbar risknivå för sin verksamhet och genomför nivån med ändamålsenliga metoder (ofta genom s.k. kontroller). I praktiken ska registraren fastställa ansvar och tidsscheman för riskhantering. Dessutom ska den följa upp hur riskhanteringen genomförs och vilka konsekvenser riskerna medför.

Föreskriften förutsätter också att riskhanteringen ska vara regelbunden, dvs. risker och metoder för hantering av risker ska bedömas regelbundet. Registraren kan själv fastställa lämpliga uppföljningscykler. Normalt görs riskbedömningar i företag när nya tjänster eller funktioner definieras, årligen och alltid efter att en eventuell risk har realiserats.

För att övervaka att kraven på riskhanteringen iakttas, ska registraren dokumentera den fastställda processen för riskhantering och resultaten från riskhanteringen.

Leverantörerna av DNS-tjänster ska dessutom iaktta kommissionens genomförandeförordning 2024/2690 och på så sätt utfärda åtminstone de dokument som krävs i genomförandeförordningen.

5.3 Datamaterial och säkerhetskopiering

För att information med anknytning till förmedlingen av domännamn ska vara tillgänglig endast för dem som har rätt att använda den, ska registraren ha ett klassificeringssystem och hanteringsförfaranden för sådant datamaterial som är viktigt för förmedlingen av domännamn. En väsentlig del av klassificering och hantering av datamaterial är åtkomsthantering i enlighet med klassificeringen av datamaterialet.

Registraren ska fastställa sådana kriterier för klassificeringen av datamaterial som lämpar sig för dess verksamhet. Materialet kan exempelvis klassificeras på följande sätt: offentligt, konfidentiellt och sekretessbelagt. Dessutom ska registraren fastställa på vilket sätt företaget hanterar (skyddar) materialet som har indelats i olika klasser.

Klassificeringen och den tillhörande anvisningen för hantering av datamaterial ska dokumenteras. Faktorer som ska beaktas när klassificeringen fastställs och dokumenteras är exempelvis följande:

[8] ISO/IEC 27005:2022 Informationssäkerhet, cybersäkerhet och integritetsskydd - Vägledning om riskhantering inom informationssäkerhet.
[9] ISO/IEC 27001:2022 Informationssäkerhet - Cybersäkerhet och integritetsskydd - Ledningssystem för informationssäkerhet - Krav
[10] NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems.
[11] NIST CSF 2.0 Cybersecurity framework 2.0.

- allmänna principer för bedömning av datamaterialets säkerhetsklass och konfidentialitet samt hemlighållandet av datamaterial
- hanterings- och ändringsrättigheter vad gäller fördelningen av läsrättigheter till datamaterialet, ändringsrättigheter och fördelningen av dessa rättigheter
- fastställande av konfidentialitetsklass
- offentlighet av uppgifter eller dokument: till exempel rätten att tala om ett ärende offentligt
- dokumentets egenskaper: papper, stämpel och andra märkningar
- förvaring och kryptering
- utskrifter och kopiering
- säkerhetskopiering
- mottagning, distribution, sändning och transport
- dokumentering av hanteringen av uppgifter och dokument
- arkivering och hantering av dokument eller upphörande av hanteringsrätten samt förstörande av uppgifter och dokument.

Registrarerna åläggs en ny skyldighet att införa och upprätthålla en praxis för säkerhetskopiering. I praxisen för säkerhetskopiering ska man beakta de data och system som är kritiska för registrarens egen verksamhet. Registraren bör på basis av riskhanteringen specificera nödvändiga säkerhetskopior på data och system. Säkerhetskopiorna bör bevaras tillräckligt länge och tas tillräckligt ofta så att de kritiska funktionerna kan återställas tillräckligt snabbt för registrarverksamhetens behov vid en eventuell störning eller kris. Säkerhetskopieringens och återställandets funktion ska testas regelbundet för att garantera funktionen. Det är dessutom mycket att rekommendera att säkerhetskopiorna skyddas så att de inte utsätts för samma hot som de system som säkerställs. Praxisen för säkerhetskopiering kan dokumenteras till exempel genom att foga en beskrivning som en del av de övriga anvisningarna om informationssäkerhet.

Leverantör av DNS-tjänster ska dessutom iaktta kommissionens genomförandeförordning 2024/2690 och beakta åtminstone de frågor som krävs i genomförandeförordningen i sin dokumentation.

5.4 Övervakning av informationssäkerheten

I punkt 5.4 i föreskriften preciseras delvis informativt registrarens skyldighet enligt 170 § 1 mom. 6 punkten i lagen om tjänster inom elektronisk kommunikation att sörja för informationssäkerheten i sin verksamhet. Enligt motiveringen till punkten ska registraren förvissa sig om att händelser som är relevanta för informationssäkerheten noteras. En förutsättning är sålunda att kränkningar av och hot mot informationssäkerheten vid registrarverksamheten ska kunna upptäckas. I praktiken innebär detta att registraren ska underhålla systemet för administration av sin tjänst.

Det är viktigt att registraren på eget initiativ agerar snabbt om den upptäcker fel och störningar. Då kan registraren snabbt vidta åtgärder för att utreda, begränsa och avhjälpa fel och störningar i informationssäkerheten och dessutom behöver den inte vänta tills kunderna börjar klaga. Syftet med förebyggande av fel och störningar i informationssäkerheten är att man så tidigt som möjligt försöker upptäcka även de minsta kännetecknen för begynnande problem. Med hjälp av förebyggande åtgärder

kan effekterna på registrarverksamheten minimeras och i bästa fall märks inga effekter alls.

Registraren ska kontinuerligt övervaka informationssäkerheten i sin registrarverksamhet. Registraren ska ha lämpliga mekanismer för hantering av förmedlingen av domännamn, med vilka den så snabbt som möjligt kan upptäcka problem i informationssäkerheten. Som exempel på sådana situationer kan nämnas överbelastningsangrepp, försök till dataintrång, informationsläckor och för omfattande behörigheter. Registraren ska också sträva efter att upptäcka situationer som håller på att utvecklas till problem i så tidigt skede som möjligt med hjälp av sina mekanismer för hantering av tjänsten. Indikatorer som förutspår störningar är till exempel mjukvarularm och kvalitetsmätare för tjänster som meddelar en avvikelse från det normala trots att de inte indikerar omedelbara störningar. Registraren är dock själv ansvarig för att specificera användbara mjukvarularm och kvalitetsmätare. Föregripande information som hjälper registraren att undvika problem med informationssäkerheten är bland annat anmälda observationer av sårbarheter i hårdvara eller mjukvara.

Registraren ska dokumentera de mekanismer som den använder för att övervaka registrarverksamheten, så att registraren vid behov kan visa med vilka åtgärder den uppfyller de fastställda kraven. Registraren ska dokumentera sina system och förfaranden för mottagning och analys av olika larm- och anmälningsuppgifter och dokumentationen ska hållas uppdaterad. Med andra ord ska registraren ha en beskrivning av de tekniska system och verksamhetssätt med vilka den mottar, hanterar och analyserar uppgifter eller anmälningar om läget i sin tjänst.

5. 5 Hantering av situationer som stör eller hotar informationssäkerheten

I punkt 5.5 i föreskriften behandlas registrarens interna procedurer vid störningar. Syftet med procedurerna är att skapa färdigheter så att registrarer kan utreda orsaken till problemen i informationssäkerheten så snabbt som möjligt och minimera deras verkningar. Procedurerna har också praktisk betydelse när registraren t.ex. utbildar ny personal.

En registrar ska i förväg utfärda tydlig dokumentation över procedurer för att reda ut situationer som stör eller hotar informationssäkerheten i registrarverksamheten samt för att minimera och avlägsna verkningarna utan obefogat dröjsmål. Procedurerna ska åtminstone omfatta

- organisering av hanteringen av informationssäkerhet, och
- ansvarsfördelning, inklusive åtminstone uppgifter som behövs för att nå de personer som svarar för informationssäkerheten.

Procedurerna ska naturligtvis också beakta eventuella speciella anvisningar för avhjälpande av betydande störningar. Sådana speciella anvisningar kan vara till exempel arrangemang för jour eller arbetsberedskap.

Organisationen av hanteringen av informationssäkerheten beskrivs oftast i företagets interna informationssäkerhetspolicy, m.a.o. i ett dokument som godkänts av företagets ledning och som beskriver målbilden och genomförandet av företagets informationssäkerhet.

Leverantörerna av DNS-tjänster ska dessutom iaktta kommissionens genomförandeförordning 2024/2690 och beakta bestämmelserna om incidenthantering i den.

5.6 Hantering av ändringar

I punkt 5.6 i föreskriften föreskrivs att en registrar ska genomföra ändringarna i nät, mjukvara, hårdvara, konfigurationer, gränssnitt och utrustningsutrymmen på ett väl avvägt och planmässigt sätt så att registrarverksamheten störs i minsta möjliga grad vid ändringarna. För ändrings-, service- och uppdateringsåtgärder måste reserveras tillräckligt med tid så att den planerade åtgärden kan utföras på ett behärskat sätt. Registraren ska även specificera och dokumentera de processer och förfaranden som styr ändringarna.

Utgångspunkten är att registraren ska minimera störningar, såsom driftavbrott, som ändringarna orsakar. Avbrotten kan dock vara nödvändiga och de planerade ändringarna ska kunna göras så felfritt som möjligt. Därför betonas i punkt 5.6 i föreskriften att avbrotten ska dimensioneras så att teleföretaget förutom behov av tjänster också tar hänsyn till det realistiska behovet av tid som ett omsorgsfullt ändringsarbete kräver. I föreskriften föreskrivs i synnerhet om ett s.k. underhållsfönster och förutsätts att teleföretaget reserverar tillräckligt med tid för åtgärderna.

För att hantera ändringar och minimera olägenheter ska registraren, innan den börjar genomföra ändringen, omsorgsfullt planera hur ändringsarbetet fortskrider och behövliga resurser, uppskatta ändringsarbetets inverkan och varaktighet samt i förväg planera åtgärder som vidtas om ändringen inte sker som planerat. Om registraren t.ex. byter program för utrustningen eller gör ändringar i konfigurationerna lönar det sig att, om möjligt, simulera ändringens inverkan på förhand, till exempel för att ta reda på var felen kan finnas och avhjälpa dem i förväg.

Registraren ska i förväg definiera och dokumentera de processer och förfaringssätt som hänför sig till ändrings- och uppdateringsarbeten så att alla ändringsarbeten utförs på ett planenligt och förutsebart sätt.

För varje ändrings-, service- eller uppdateringsåtgärd ska registraren i enlighet med sina fastställda processer och förfaringssätt beräkna den tid som behövs för arbetena och reservera denna tid för att slutföra arbetet.

Registrarerna åläggs en ny skyldighet att följa informationssäkerhetsmeddelanden för de system de använder samt skyldighet att installera nödvändiga säkerhetsuppdateringar. Med relevanta uppdateringar kan registraren förebygga att eventuella sårbarheter utnyttjas. En registrar ska ha lämpliga förfaranden med vilka den kan följa kritiska säkerhetsuppdateringar i sina operativsystem, applikationer och inbyggda program och installera dem utan dröjsmål på basis av riskbedömning. System som inte kan uppdateras omedelbart ska skyddas med andra metoder och uppdateringarna ska installeras på ett väl avvägt sätt när det är möjligt.

Leverantörerna av DNS-tjänster ska dessutom iaktta kommissionens genomförandeförordning 2024/2690 och bland annat beakta bestämmelserna om incidenthantering i den.

5.7 Katakri-kraven vid användning av Transport- och kommunikationsverkets EPP-gränssnitt

I punkt 5.7 i föreskriften beskrivs de krav som en fi-registrar ska uppfylla, om den använder Transport- och kommunikationsverkets EPP-gränssnitt som ett tekniskt gränssnitt. I så fall är kravet att registraren uppfyller kriterierna härledda från skyddsnivå (IV) enligt delområde I, teknisk informationssäkerhet, i den version av Katakri (verktyg för informationssäkerhetauditering) som gäller vid respektive tidpunkt, till följande delar:

1) Telekommunikationssäkerhet

2) Säkerhet i informationssystem.

Katakri är ett auditeringsverktyg för myndigheter när de bedömer den berörda organisationens förmåga att skydda myndighetens sekretessbelagda information. I Katakri har man samlat in de minimikrav som grundar sig på nationella författningar och internationella förpliktelser. Katakri har utvecklats under åren och den fjärde och samtidigt den senaste versionen är Katakri 2020 som uppdaterats av samarbetsgruppen för den nationella säkerhetsmyndigheten.

Som sådant ställer Katakri inte några absoluta krav för informationssäkerheten, utan de insamlade kraven baserar sig på gällande lagstiftning och de informationssäkerhetsförpliktelser som är bindande för Finland. Kraven i Katakri är markerade med en källhänvisning för att säkerställa insyn.

Kraven i Katakri är uppdelade i tre delområden:

Delområde (T) som gäller säkerhetsledning vill säkerställa att organisationen har tillräckliga färdigheter och förmåga för säkerhetsledning.

Delområde (F) som gäller fysisk säkerhet beskriver säkerhetskraven för den fysiska användningsmiljön för sekretessbelagd information.

Delområde (I) som gäller teknisk informationssäkerhet beskriver säkerhetskraven för den tekniska databehandlingsmiljön. Detta delområde uppdelas i tre säkerhetsklasser enligt den information som behandlas (II - IV).

Föreskriften förutsätter att registrarer som använder Transport- och kommunikationsverkets EPP-gränssnitt uppfyller kraven på den tekniska informationssäkerhetens delområde gällande telekommunikationssäkerhet och säkerhet i informationssystem. Syftet med föreskriften är att säkerställa en hög informationssäkerhetsnivå hos registrarernas kunder.

Transport- och kommunikationsverket konstaterar också att kraven i föreskriften uttryckligen gäller förmedling av domännamn. Om den som förmedlar domännamn också utövar annan verksamhet, gäller föreskriften inte den andra verksamheten.

Transport- och kommunikationsverkets föreskrift hänvisar till gällande kriterier. Den gällande versionen av Katakri finns på utrikesministeriets webbplats på um.fi.

6 kap. Anmälningsskyldighet vid störningar

Registrarens störningsanmälan till den myndighet som förvaltar domännamnsregistret

I punkt 6 i föreskriften anges närmare om innehållet i registrarens anmälningsskyldighet vid störningar i informationssäkerheten.

Enligt 170 § 1 mom. 7 punkten i lagen om tjänster inom elektronisk kommunikation ska en registrar utan dröjsmål meddela Transport- och kommunikationsverket om dess förmedling av domännamn är utsatt för betydande kränkningar av eller hot mot informationssäkerheten eller för någonting annat som väsentligen förhindrar eller stör den. Samtidigt ska registraren också anmäla hur länge störningen eller hotet beräknas pågå, om vilka verkningar störningen eller hotet har, om avhjälpande åtgärder samt om åtgärder för att förhindra att störningen upprepas. I motiveringen till punkten nämns exempelvis en situation där någon har gjort intrång i registrarens system. Det är nödvändigt att tillsynsmyndigheten utan dröjsmål får veta om det,

emedan risken är att den som står bakom intrånget fritt kan komma åt att ändra uppgifter om domännamn som registraren i fråga förvaltar, såsom namnservrar. I motiveringen till punkten konstateras det att hotet begränsas till denna registrars kunder, men att det ändå kan gälla en stor kundkrets. För ax-domännamn skulle tillsynsmyndigheten enligt nuvarande praxis vara Ålands landskapsregering och störningsanmälningarna skulle lämnas till den.

I en anmälan om betydande informationssäkerhetsstörning ska en registrar, förutom de uppgifter som förutsätts i lagen, också i mån av möjlighet redogöra för orsaken till störningen eller hotet och hur störningen har framkallats. Störningsanmälan ska göras inom 24 timmar från det att registraren har fått veta om störningen. Anmälan ska kompletteras senare till den del alla de uppgifter som krävs inte finns tillgängliga vid anmälningstidpunkten.

Betydande kränkningar av informationssäkerheten

Enligt 170 § 2 mom. i lagen om tjänster inom elektronisk kommunikation får Transport- och kommunikationsverket meddela närmare föreskrifter om när en störning som avses i 1 mom. 7 punkten ska anses vara betydande samt om innehållet i anmälan samt anmälans utformning och hur den lämnas in.

I detta skede anser Transport- och kommunikationsverket att det inte finns någon anledning att meddela närmare föreskrifter om när en störning i informationssäkerheten är betydande. Anmälningströskeln kan senare fastställas närmare genom en ändring i föreskriften, om det utifrån tillsynserfarenheter visar sig vara nödvändigt. Enligt Transport- och kommunikationsverkets uppfattning är det emellertid nödvändigt att lyfta fram vissa synpunkter som ska beaktas vid bedömning av om en störning är betydande eller inte.

I kommissionens genomförandeförordning 2024/2690 anges när en incident som hänför sig till en DNS-tjänsteleverantör är betydande. Den störning som avses i lagen om tjänster inom elektronisk kommunikation och i domännamnsföreskriften ska inte tolkas i överensstämmelse med genomförandeförordningen, utan en störning som kräver anmälningsskyldighet kan även förekomma i andra incidenter än i de som beskrivs i genomförandeförordningen. Den störning som avses i lagen om tjänster inom elektronisk kommunikation och i domännamnsföreskriften ska tolkas på ett mer omfattande sätt med beaktande av synpunkterna nedan.

Vid bedömning av om en kränkning av informationssäkerheten eller någon annan händelse är betydande eller inte ska hänsyn tas till vilka negativa konsekvenser händelsen har eller hur allvarligt hotet mot informationssäkerheten till följd av händelsen är. Kränkningar av informationssäkerheten kan ha konsekvenser för uppgifternas eller datasystemens konfidentialitet, integritet, autenticitet eller tillgänglighet.

Med konfidentialitet avses i detta sammanhang att uppgifter och verifieringsuppgifter om användarnamn endast är tillgängliga för dem som är berättigade att få uppgifterna. Med integritet avses att det inte är möjligt att obehörigt göra ändringar i uppgifter och att utomstående inte har möjlighet att inverka på datasystemens funktion. Med tillgänglighet avses att en tjänst eller uppgifter i tjänsten är tillgängliga för dem som är berättigade till den.

En störning i informationssäkerheten är alltid betydande om den drabbar följande objekt:

- de informations- och kommunikationssystem som används för registrarens tjänster och produktion av tjänster
- informationssäkerheten, skyddet av personuppgifter eller skyddet av företagshemligheter hos registrarens kunder
- Fi-roten i Finland, som administreras av Transport- och kommunikationsverket till följd av en direkt eller indirekt kränkning av informationssäkerheten hos en registrar.

Som en betydande störning betraktas också verksamhet som är ofta återkommande eller exceptionellt långvarig eller verkar avsiktlig och som har negativa konsekvenser för en registrars förmåga att sörja för informationssäkerheten i registrarverksamheten.

Detsamma gäller också när en störning inte kan undanröjas enbart genom registrarens egna åtgärder.

Exempel på sådana typer av kränkningar i informationssäkerheten som omfattas av anmälningsskyldighet

Nedan finns exempel på sådana typer av kränkningar i informationssäkerheten som enligt Transport- och kommunikationsverkets uppfattning ska meddelas utifrån 170 § 1 mom. 7 punkten i lagen om tjänster inom elektronisk kommunikation. Förteckningen är inte täckande utan syftet är att beskriva allvarlighetsgraden för de fall som ska anmälas. Gränsöverskridande exempel på betydande störningar i informationssäkerheten är:

Dataintrång i registrarens informationssystemsystem

- Obehörig åtkomst till registrarens system
- Sårbarheter eller konfigurationsfel som riskerar informationssäkerheten i registrarens system

Tredje parter får kännedom om inloggningskoder

- utomstående kommer över de inloggningskoder som används till Transport- och kommunikationsverkets system

Obehöriga ändringar

- Möjlighet att obehörigt ändra uppgifter om de domännamn som registrarer förvaltar
- Ändringar som en registrars anställda obehörigt gör i domännamnsregistret
- Obehörig åtkomst till en självbetjäningsportal som en registrar tillhandahåller sina kunder och där kunderna själva kan uppdatera uppgifterna om sina domännamn

Överbelastningsangrepp

- En registrars system lamslås och/eller kundernas åtkomst till systemet förhindras
- En systemstörning påverkar funktionen i Transport- och kommunikationsverkets system.

Rekommendation om frivilliga anmälningar

Transport- och kommunikationsverket rekommenderar att registrarerna efter gottfinnande underrättar Transport- och kommunikationsverket också om

kränkningar av och hot mot informationssäkerhet som är av mindre betydelse. Sådan information kan ha betydelse för att Transport- och kommunikationsverket ska kunna inleda åtgärder enligt 172 § i lagen om tjänster inom elektronisk kommunikation, eller för att Transport- och kommunikationsverket ska kunna sköta andra informationssäkerhetsuppgifter som föreskrivs i 304 § 1 mom. 1, 7, 8 och 10 punkten i lagen om tjänster inom elektronisk kommunikation. Transport- och kommunikationsverket rekommenderar också att DNS-tjänsteleverantörer efter gottfinnande gör tillsynsmyndigheten frivilliga anmälningar med stöd av 15 § i cybersäkerhetslagen.

Enligt 172 § 1 mom. i lagen om tjänster inom elektronisk kommunikation har Transport- och kommunikationsverket rätt att vidta nödvändiga åtgärder för att upptäcka, förhindra och utreda sådana betydande kränkningar av informationssäkerheten som innebär att fi-domännamn utnyttjas och som är riktade mot allmänna kommunikationsnät eller kommunikationstjänster eller mot användare av dem, samt för att inleda förundersökning med anledning av kränkningarna. Transport- och kommunikationsverket får vidta dessa åtgärder utan att höra domännamnsanvändaren.

Enligt 2 mom. i paragrafen kan de nödvändiga åtgärder som avses i 1 mom. utföras med avseende på namnserverinformationen i fi-roten och kan omfatta

1) åtgärder för att förhindra eller begränsa den trafik som riktas till domännamnet;
2) åtgärder för att dirigera den trafik som riktas till domännamnet till en annan webbadress, samt
3) andra med 1 och 2 punkten jämförbara åtgärder av teknisk natur.

Enligt 3 mom. ska de åtgärder som avses i 172 § utföras omsorgsfullt och de ska stå i proportion till allvaret i den kränkning av informationssäkerheten som ska avvärjas. Åtgärderna ska utföras utan att yttrandefriheten, skyddet av konfidentiella meddelanden eller integritetsskyddet begränsas mer än vad som är nödvändigt med tanke på säkerställandet av möjligheterna att uppnå målen enligt 1 mom. Åtgärderna ska avbrytas, om det inte längre finns förutsättningar enligt denna paragraf att vidta dem.

I 304 § i lagen om tjänster inom elektronisk kommunikation föreskrivs om Transport- och kommunikationsverkets särskilda uppgifter. Enligt lagrummet ska Transport- och kommunikationsverket bland annat

- främja den elektroniska kommunikationens funktion, störningsfrihet och trygghet (1 punkten),
- samla in information om kränkningar och hot om kränkningar av informationssäkerheten för nättjänster, kommunikationstjänster och mervärdestjänster samt om fel och störningar i kommunikationsnät och kommunikationstjänster (7 punkten),
- informera om frågor som gäller informationssäkerhet samt om kommunikationsnäts och kommunikationstjänsters funktion (8 punkten),
- utreda kränkningar och hot om kränkningar av informationssäkerheten för nättjänster, kommunikationstjänster och mervärdestjänster (10 punkten).

Anmälningsförfarande

Upptäckt av en störning i informationssäkerheten ska anmälas till den myndighet om förvaltar domännamnsregistret så fort som möjligt, dock enligt föreskriften senast

inom 24 timmar. Anmälan till Transport- och kommunikationsverket görs i första hand på blanketten för anmälan om störning för domännamnsregistrarer.

Om inte all information som efterfrågas i blanketten finns till handa och situationen kräver noggrannare utredning, ska registraren senast inom 24 timmar lämna en preliminär anmälan som kompletteras så fort som möjligt, och senast inom tre (3) dagar.

Om registraren trots utredningar inte kan lämna alla uppgifter inom tre dagar efter den preliminära anmälningen, ska den inom den fastställda tidsfristen uppge de uppgifter som finns tillhanda samt motivera varför den lämnar resten av uppgifterna efter att fristen har gått ut.

Uppgifter som lämnats in ska uppdateras vid behov och så fort som möjligt om uppgifterna ändras.

Om registraren är leverantör av DNS-tjänster och det är fråga om en betydande incident som definierats i kommissionens genomförandeförordning 2024/2690 ska registraren göra de anmälningar som cybersäkerhetslagen förutsätter på blanketten avsedd för anmälningar om betydande incidenter. I en sådan situation behöver DNS-tjänsteleverantörer som omfattas av Transport- och kommunikationsverkets tillsyn inte separat fylla i blanketten för anmälan om störning för domännamnsregistrarer.

Uppgifter som anmäls

Av anmälan till myndigheten ska framgå följande uppgifter:

- Uppgifter om registraren, dvs.
  - registrarens namn
  - namn på person som lämnar närmare uppgifter om händelsen samt dennes e-postadress och telefonnummer.
- Tidpunkt när händelsen inträffade och upptäcktes:
  - tidpunkt när händelsen inträffade och tidpunkt när den upptäcktes ska anges separat
  - tidpunkten för upptäckten ska anges med minst en dags noggrannhet
  - när det gäller tekniska systemloggar för händelsen anges också ett exakt klockslag, en tillämplig tidszon (t.ex. "UTC+2") samt ett eventuellt klockfel och dess riktning jämfört med den officiella tiden
  - Det rekommenderas att tidsstämplar för tekniska systemloggar anges i ett format som är kompatibelt med ISO 8601 (jfr http://www.w3.org/TR/NOTE-datetime), fastän det viktigaste är att data om observationer överhuvudtaget finns i förvar.
- Typ av händelse, dvs. om det är fråga om till exempel:
  - dataintrång eller olovlig användning (t.ex. intrång i ett program som är anslutet till Transport- och kommunikationsverkets EPP-gränssnitt)
  - fel i hanteringen av kunduppgifter (t.ex. oavsiktligt läckage i kunduppgifter)
  - annan händelse, som i så fall ska beskrivas med ord.
- Föremål för händelsen och åtgärder, dvs.:

- beskrivning av systemet som utsatts för händelsen
- observationer av händelserna
- uppgifter om orsaken till händelsen
- åtgärder som vidtagits eller kommer att vidtas för att eliminera eller avhjälpa följderna
- uppgift om huruvida ytterligare skador har förhindrats.

- Uppgifter om eventuella effekter för användarna, dvs.:

  - beskrivning av eventuella effekter
  - uppgifter om de domännamn som har redigerats obehörigt
  - uppgift om ifall registraren inte har kännedom om vilka obehöriga ändringar som har gjorts med registrarens koder i Transport- och kommunikationsverkets system.

7 Ikraftträdande

Syftet är att föreskriften ska träda i kraft samtidigt som de ändringar i lagen om tjänster inom elektronisk kommunikation som föreslås i regeringens proposition till riksdagen med förslag till lagstiftning om genomförande av cybersäkerhetsdirektivet (NIS 2-direktivet) (RP 57/2024). Föreskriften träder inte i kraft innan NIS 2-direktivet har implementerats i Finland.

Alla registrarer ska iaktta den nya föreskriften och anmäla de uppgifter som anges i föreskriften omedelbart efter att föreskriften trätt i kraft. De registrarer som anmält sig före föreskriftens ikraftträdande kan dock fylla i och lämna den dokumentation som gäller genomförandet av verktyget eller metoden för självutvärdering enligt punkt 3.1 i föreskriften senast den 30 januari 2026, om inte den myndighet som förvaltar domännamnsregistret begär tidigare inlämnande på basis av ett anhängigt tillsynsärende.