Guide för registrarer

Anvisningar och krav för dem som vill utöva registrarverksamhet

Versionshistorik

Version	Datum	Beskrivning/ändring	Författare
1.0	25.10.2018	Version 1	Ari-Matti Husa
1.1	21.12.2018	Version 1.1	Ari-Matti Husa
1.2	6.9.2021	version 1.2	Sami Salmensuo

Innehåll

1 Registrarens uppgifter och skyldigheter

1.1 Registrarens serviceskyldighet

En registrar hjälper och ger råd till sina kunder i frågor som gäller fi-domännamn. Registraren registrerar fi-domännamnen och gör ändringar i dem på kundernas begäran.

En domännamnsanvändare anlitar registrarens tjänster i alla situationer som hänför sig till fi-domännamn. Registraren har genom bestämmelserna i lagen om tjänster inom elektronisk kommunikation skyldighet att se till att användarens rättigheter genomförs och att användaren får nödvändig information om fi-domännamn och ändringar i registrarverksamheten.

På kundernas begäran ska registrarerna

- registrera fi-domännamn i Transport- och kommunikationsverkets domännamnsregister
- uppdatera uppgifterna om domännamnet
- förlänga domännamnets giltighetstid
- byta domännamnets registrar
- överföra domännamnet till en annan användare
- säga upp domännamnet.

Registraren är också skyldig att ge sina kunder

- allmänna råd om fi-domännamn
- information, om registrarverksamheten har upphört eller om Transport- och kommunikationsverket har meddelat ett förbudsbeslut som gäller registraren.

1.1.1 Betalning för registrering och förnyande

Registraren betalar en avgift till Transport- och kommunikationsverket för registreringar och förnyanden av kundernas domännamn via registrarens tekniska gränssnitt. Avgiften för registrering och förnyande beror på giltighetstiden och är följande:

- 1 år 9 euro
- 2 år 18 euro
- 3 år 27 euro
- 4 år 36 euro
- 5 år 45 euro.

Registreringar och förnyanden debiteras från registrarens förskottsbetalningskonto där registraren reserverar pengar för sina

transaktioner. Registraren betalar för domännamnsavgifterna i enlighet med kommunikationsministeriets förordning 660/2016.

Transport- och kommunikationsverket återbetalar avgiften inte till registraren, även om domännamnet skulle ha registrerats fel eller om Transport- och kommunikationsverket senare avregistrerar domännamnet genom beslut.

1.2 Skyldighet att ge råd till kunderna

En registrar ska ge råd till sina kunder innan fi-domännamn registreras. Kunderna ska åtminstone informeras om domännamnets form, innehåll och lagenlighet.

Registraren ska ge sina kunder information om förutsättningarna för fi-domännamn i en lättillgänglig och utförlig form innan domännamnet registreras. Skyldigheten avser endast rådgivning. Domännamnsanvändaren har det slutliga ansvaret för att domännamnet är lagligt.

Informationen ska finnas tillgänglig för såväl nuvarande som blivande domännamnsanvändare oberoende av om kunderna redan skapat ett avtalsförhållande med registraren eller inte.

Registraren ska aktivt se till att domännamnsregistreringar är förenliga med lagen. I synnerhet när det gäller skyddade namn och varumärken ska kunderna känna till förutsättningarna innan domännamnen registreras. Syftet med rådgivningsskyldigheten är att undvika felaktiga och lagstridiga domännamnsregistreringar som kan leda till att domännamnet återkallas.

1.2.1 Minimikrav för rådgivningen

Registraren får själv välja hur rådgivningsskyldigheten genomförs, men innehållsmässigt ska registraren tillhandahålla sina kunder minst följande uppgifter som avser domännamnets innehåll och form:

Vad är ett skyddat namn eller varumärke?

- Skyddade namn och märken är enligt lagen om tjänster inom elektronisk kommunikation:
- namn eller märken som är införda i handels-, varumärkes-, förenings-, stiftelse- eller partiregistret
- 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.
- en inarbetad firma, ett sekundärt kännetecken eller varumärke som avses i firmalagen och varumärkeslagen.

- EU-varumärken registrerade i EUIPO:s varumärkesregister.

Var kan man kontrollera de skyddade namnen och varumärkena?

Registraren ska tillhandahålla sina kunder länkar till Patent- och registerstyrelsens (PRS) offentliga register (företags- och organisationsdatasystemet, föreningsregistret, varumärkesregistret) samt till Europeiska unionens immaterialrättsmyndighets (EUIPO) EU-varumärkesregister.

Vad betyder domännamnets lagenlighet?

Ett domännamn får vid registreringstidpunkten inte

- motsvara någon annans skyddade namn eller märke, om inte domännamnsanvändaren kan ge en godtagbar grund för registreringen av domännamnet
- likna någon annans skyddade namn eller märke, om domännamnet registreras i uppenbart vinnings- eller skadesyfte.

Tillåtna tecken i domännamn

Registraren ska ge råd till kunderna om tillåtna tecken i domännamn, som är bokstäverna a–z och siffrorna 0–9. Tillåtna nationella tecken är också bokstäverna å, ä och ö, tecknen som används i samiska i Finland och ett bindestreck-minus.

När registrarerna marknadsför och förmedlar domännamn ska de beakta de begränsningar som gäller domännamn med nationella tecken. Kunder som ansöker om ett domännamn eller planerar att ansöka om ett domännamn måste känna till de tekniska begränsningar som är förknippade med domännamn som innehåller nationella tecken.

Speciell uppmärksamhet bör fästas vid kundens eventuella behov av att ansöka om både ett domännamn med nationella tecken och ett motsvarande domännamn utan nationella tecken, till exempel ääkkönen.fi och aakkonen.fi.

Det är möjligt att använda skrivtecken som inte ingår i det latinska alfabetet med hjälp av punycode för vilken också används benämningen ACE (ASCII Compatible Encoding). Namnserversystemet förstår ett domännamn som innehåller nationella tecken, om domännamnet tekniskt har konfigurerats med ACE-formatet.

Till exempel konvertering av ääkkönen.fi till ACE-format: xn--kknen-fraa=0m.fi.

Det finns en hel del webbsidor som tillhandahåller konverteringsverktyg. På Transport- och kommunikationsverkets webbsidor finns också ett konverteringsverktyg.

1.3 Korrekta och uppdaterade uppgifter

Registraren har aktuella uppgifter om sina kunder i fi-domännamnsregistret både vid registreringen och senare om uppgifterna ändras.

Ett fi-domännamn registreras alltid på den faktiska domännamnsanvändaren. Kundens fi-domännamn får inte registreras t.ex. på en registrar. När Transport- och kommunikationsverket utreder oklarheter eller tvister som hänför sig till fi-domännamn bedömer det alltid domännamnsanvändarens rättigheter i förhållande till andras.

Med avseende på registrarens kunds rättsskydd är det mycket viktigt att användarregistreringen har gjorts på ett sanningsenligt sätt och att domännamnet har registrerats på rätt användare.

Registraren måste hålla uppgifterna i domännamnsregistret korrekta och uppdaterade även efter registreringen. Registraren är skyldig att på kundens begäran göra följande ändringar i domännamnet:

- uppdatera domännamnsanvändarens kontaktuppgifter
- säga upp domännamn
- överföra domännamn till en annan användare
- byta registrar
- förnya domännamn.

1.3.1 Uppdatering av kontaktuppgifter

Registraren måste hålla sina fi-domännamnskunders uppgifter uppdaterade. Kontaktuppgifterna uppdateras på kundens begäran och även i övriga situationer på eget initiativ.

Registraren ansvarar för att de användaruppgifter som anmäls är korrekta och uppdaterade. Om registrarens försummelse leder till att domännamnsanvändaren (dvs. registrarens kund) orsakas skador kan användaren yrka på skadestånd.

1.3.2 Lagstadgad processadress och övriga e-postadresser

Transport- och kommunikationsverket använder för hörande och delgivning den e-postadress som är införd i domännamnsregistret. Därför kan en handling eller ett beslut som gäller domännamn alltid delges per e-post. Denna så kallad processadress har stor rättslig betydelse och det är obligatoriskt för registrarerna att ange den till Transport- och kommunikationsverket.

Med hjälp av en processadress kan Transport- och kommunikationsverket snabbt delge bindande beslut, eftersom beslutet eller handlingen då anses ha delgivits den tredje dagen efter det att meddelandet sändes.

En rätt processadress för en domännamnsanvändare är en viktig uppgift och även med tanke på registrarens rättsskydd är det högst viktigt att den hålls uppdaterad. Registraren ansvarar för att domännamnsanvändarens processadress anmäls och att den hålls uppdaterad.

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.

1.4 Förnyande av domännamn

Registraren informerar användare av fi-domännamn om att domännamnets giltighetstid löper ut.

Ett domännamn som har registrerats i domännamnsregistret gäller i minst ett år och i högst fem år. Registraren kan förnya en domänregistrering för ett, två, tre, fyra eller fem år i sänder.

1.4.1 Registrarens skyldigheter när domännamnets giltighetstid går ut

När fi-domännamnets giltighetstid håller på att löpa ut, ska registraren

- informera användaren i god tid om att giltighetstiden löper ut
- ge användaren anvisningar för att göra en begäran om förnyande av domännamnet
- redogöra för användaren vad det betyder om domännamnet inte förnyas.

Registraren och domännamnsanvändaren (kunden) kan komma överens om förnyandet av domännamnet genom avtal. Avtalet kan innebära t.ex. att registraren tar hand om domännamnets giltighet automatiskt och förnyar domännamnet årligen utan att separat informera kunden om att domännamnets giltighetstid löper ut.

Transport- och kommunikationsverket har inte befogenhet att övervaka avtal mellan domännamnsanvändare och registrarer eller avgöra avtalstvister mellan dem.

1.5 Uppsägning av domännamn

En domännamnsanvändare kan säga upp sitt fi-domännamn innan dess giltighetstid har löpt ut. På begäran avregistrerar registraren domännamnet från Transport- och kommunikationsverkets register.

Registraren tar hand om uppsägningen av domännamnet (m.a.o. avregistrering och avlägsnande ur fi-roten). Uppsägningen görs på begäran av domännamnsanvändaren.

Registraren ansvarar för att

- domännamnet sägs upp endast på begäran av domännamnsanvändaren eller dess ombud
- ingen utomstående instans avsiktligt eller oavsiktligt säger upp domännamn
- om domännamnsanvändaren är en organisation, har den som säger upp domännamnet rätt till det (t.ex. i handelsregistret antecknad firmatecknare).

1.5.1 Problem vid uppsägningen

En felaktig uppsägning av domännamn kan medföra betydande ekonomiska konsekvenser. Det allvarligaste är att registraren kan bli skadeståndsansvarig.

Domännamnslagstiftningen tar inte ställning till domännamnsanvändarens och registrarens avtalsförhållande, utan de avtals-, skadestånds- eller konsumenträttsliga frågor som sammanhänger med uppsägningen avgörs med stöd av annan lagstiftning.

1.6 Överföring av domännamn till en ny användare

Registraren överför ett fi-domännamn till en ny användare efter att ha försäkrat sig om att begäran om överföring kommer från den som är berättigad att göra det.

Domännamnsanvändaren kan överföra sitt gällande domännamn till en annan användare. Efter att ha tagit emot begäran om överföring ska registraren

- säkerställa att den som begär överföring har rätt att överföra domännamnet
- skicka domännamnets överföringskod till domännamnsanvändaren utan att se kodens innehåll
- inom fem vardagar från det att överföringskoden lämnats till registraren överföra domännamnet från en användare till en annan.

Användaren ska befullmäktiga registraren att överföra domännamnet genom att ge överföringskoden till registraren för kännedom. Detta säkerställer att domännamnsanvändaren har gett sitt samtycke till överföringen och att registraren inte kan överföra domännamnet utan att användaren gett sitt faktiska samtycke.

Användaren kan befullmäktiga antingen sin egen registrar eller domännamnsmottagarens registrar att överföra domännamnet. Domännamnsmottagarens registrar kan överföra domännamnet endast om den fått förutom överföringskoden också koden för registrarbyte med vilken registraren börjat förvalta domännamnet.

Transport- och kommunikationsverket fastställer överföringskoden, som registraren inte kan se eller ange. Överföringskoden skickas alltid till den nuvarande domännamnsanvändaren som själv måste lämna den till registraren för överföringen av domännamnet.

1.6.1 Rätten att begära överföring av domännamn

Registraren måste försäkra sig om att ingen annan än domännamnsanvändaren eller dess ombud begär överföring. Överföring av domännamn är en viktig åtgärd med tanke på användarens rättsskydd och registraren är skyldig att genomföra denna åtgärd omsorgsfullt. Även mottagaren av domännamnet (den nya användaren) har i princip rätt att lita på att det finns en laglig grund för överföringen.

Om någon annan än domännamnsanvändaren begär överföring av domännamnet, ska registraren kräva att användaren ger bemyndigande för den som lämnat begäran att handla på användarens vägnar.

1.6.2 Domännamnets överföringstid

Registraren ska göra den tekniska överföringen av domännamnet till den nya användaren inom fem vardagar från det att den gamla domännamnsanvändaren har lämnat domännamnets överföringskod och uppgifterna om den nya användaren till registraren. Tidsgränsen är ett lagstadgat krav på servicenivå.

1.7 Byte av registrar

Om en domännamnsanvändare vill byta registrar, deltar den gamla registraren i bytesprocessen när den skapar en kod för registrarbyte och ger koden till användaren eller direkt till den nya registraren för kännedom.

Domännamnsanvändaren kan fritt byta registrar när som helst. Det krävs inga särskilda skäl för byte av registrar.

Faserna vid byte av registrar

1. Om en domännamnsanvändare vill byta registrar ska användaren antingen

   – befullmäktiga den nya registraren att skaffa koden för registrarbyte från den gamla registraren eller
   – själv begära att den gamla registraren ger koden för registrarbyte till användaren och efter att ha fått den sända den till den nya registraren.
   – Begäran om registrarbyte ska göras skriftligen. Då kan man i efterhand ta reda på hur lång tid det tagit att lämna koden eller om det finns andra oklarheter.

2. Den gamla registraren ska säkerställa att användaren eller den nya registraren har rätt att begära koden för registrarbyte. Den gamla registraren ska ge koden till den som begärt att få den inom fem vardagar från att den berättigade begäran lämnades.

   Av den gamla registraren krävs noggrannhet för att säkerställa att ingen annan än den som har registrerats som domännamnsanvändare ber om byte av registrar. Om någon annan framställer begäran, ska denne visa upp en tillräcklig fullmakt för det. Vid behov kan registraren exempelvis kontakta användaren för att kontrollera ärendet.

3. Beroende på hur användaren har begärt byte av registrar får den nya registraren koden antingen av den gamla registraren eller av användaren. Sedan kan den nya registraren börja förvalta domännamnet.

1.7.1 Kod för registrarbyte

Med kod för registrarbyte avses en kod med vilken förvaltningen av ett domännamn kan överföras från en registrar till en annan. Den gamla registraren skapar koden i domännamnssystemet och sparar den. Koden skickas inte via systemet utan registraren ger den till exempel per telefon eller e-post till den nya registraren. Med gammal registrar avses en registrar som avstår från förvaltningen av ett domännamn, och med ny registrar en registrar som tar emot förvaltningen av ett domännamn.

1.7.2 Domännamn utan registrar

Kod för registrarbyte behövs också om domännamnet inte har en registrar. Då måste domännamnsanvändaren begära koden av Transport- och kommunikationsverket. Efter att ha fått koden skickar domännamnsanvändaren koden till den registrar användaren valt som sedan kan börja förvalta domännamnet.

1.7.3 Problemsituationer

Efter att domännamnsanvändaren har underrättat registraren om sin vilja att byta registrar, ska registraren inom en rimlig tid (fem vardagar) vidta de åtgärder som krävs för bytet och främja bytet.

Om den gamla registraren, trots upprepade begäranden, inte har gett koden för registrarbyte till den nya registraren eller till användaren inom utsatt tid, kan den nya registraren begära att Transport- och kommunikationsverket ger koden för registrarbyte till användaren.

Domännamnsanvändarens och registrarens avtalsförhållande omfattas inte av domännamnslagstiftningen, utan de avtals- eller konsumenträttsliga frågor som sammanhänger med överföring av domännamnet eller byte av registrar avgörs med stöd av annan lagstiftning.

1.8 Om registrarverksamheten upphör

Om registraren upphör med sin verksamhet, ska Transport- och kommunikationsverket och kunderna informeras om detta. Kunderna ska också informeras om Transport- och kommunikationsverket har meddelat ett förbudsbeslut.

Om registrarens verksamhet läggs ned ska registraren informera Transport- och kommunikationsverket och registrarens egna kunder om detta minst två veckor i förväg. På så sätt kan kunderna (användare av fi-domännamn) behålla tillgång till ett fungerande domännamn och säkerställa att de hinner byta namnserveroperatör innan registrarens verksamhet upphör.

Om verksamheten läggs ned ska registraren informera varje kund om detta. Information som enbart läggs ut på exempelvis registrarens webbsidor kan inte anses vara tillräcklig, även om det rekommenderas i andra hand. Att skicka e-post till kunderna är effektivt, men det är bra om man också försöker nå kunderna per telefon.

Transport- och kommunikationsverket rekommenderar att registraren informerar varje kund i god tid både när registrarverksamheten läggs ned och när det blir ett tillfälligt avbrott i verksamheten.

1.8.1 Information om Transport- och kommunikationsverkets förbudsbeslut

Transport- och kommunikationsverket övervakar att registrarverksamheten utövas i enlighet med lag och ger vid behov en anmärkning om registraren har försummat sina skyldigheter. Registrarverksamheten kan avbrytas för en viss tid genom ett beslut av Transport- och kommunikationsverket, om

registraren inte rättar till sitt fel eller sin försummelse trots Transport- och kommunikationsverkets anmärkningar.

Om Transport- och kommunikationsverket meddelar ett förbudsbeslut om registrarverksamheten, ska registraren utan dröjsmål informera sina kunder om detta, emedan kunderna i en sådan situation kan bli tvungna att hitta en ny registrar.

Transport- och kommunikationsverket verkställer förbudsbeslutet genom att stänga av registrarens tekniska gränssnitt antingen så att

- registraren inte längre kan registrera nya domännamn eller så att
- registraren dessutom inte ens kan administrera kundernas existerande domännamn.

1.8.2 Stängning av förskottskontot

En registrar som avslutat registrarverksamheten kan be Transport- och kommunikationsverket att återbetala det oanvända belopp som registraren sparat på förskottskontot för förnyande av domännamn.

2 Informationssäkerhet i registrarverksamheten

En registrar ska sörja för informationssäkerheten genom att förbereda sig för hot och genom att ingripa i avvikelser. Minimikraven på informationssäkerheten tryggar både registrarverksamheten och rättigheterna för användare av domännamn.

Hänsynstagandet till de olika delområdena i informationssäkerheten är viktigt i alla faser som gäller förmedling av fi-domännamn: vid planering, underhåll och avslutning av verksamheten. För att informationssäkerheten ska ombesörjas rutinmässigt varje dag, krävs det processer och rutiner.

Beredskapsplanen måste dokumenteras

Registraren ska fastställa detaljerade anvisningar med tanke på hot mot informationssäkerheten. Registraren ska förvissa sig om att man

- noterar händelser som är relevanta för informationssäkerheten
- ingriper i problem och avvikelser i informationssäkerheten.

En uppdaterad dokumentation av planer som stöder informationssäkerheten utgör en grund för hantering och utveckling av registrarens informationssäkerhet. Utifrån dokumentationen kan också Transport- och kommunikationsverket vid behov verifiera att registraren iakttar informationssäkerhetsskyldigheterna. Det vettigaste sättet att dokumentera informationssäkerhetsärendena beror på omfattningen av företagets verksamhet.

Minimikrav på informationssäkerheten

Med informationssäkerhet avses enligt 3 § 1 mom. 28 punkten i lagen om tjänster inom elektronisk kommunikation administrativa och tekniska åtgärder för att säkerställa informationens konfidentialitet, integritet och tillgänglighet. Genom åtgärderna säkerställs att

- informationen och informationssystemen kan endast utnyttjas av dem som har rätt att använda informationen och systemen
- informationen inte kan ändras av andra än dem som har rätt till detta.

I Transport- och kommunikationsverkets domännamnsföreskrift 68 beskrivs de minimikrav för hantering av informationssäkerheten som alla registrarer ska uppfylla i sin verksamhet. Syftet med kraven är att

- trygga den grundläggande nivån för informationssäkerheten i registrarverksamheten
- minska på negativa konsekvenser av informationssäkerhetsriskerna för registrarverksamheten och användare av fi-domännamn.

2.1 Informationssäkerheten i praktiken

Registraren ska dokumentera och hålla en uppdaterad beskrivning av på vilket sätt den beaktar de olika delområdena av informationssäkerheten i sin verksamhet.

Det finns flera olika ärendehelheter som ska beaktas vid genomförandet av informationssäkerheten och i de dokument som beskriver det. Dessa helheter räknas upp i Transport- och kommunikationsverkets föreskrift 68. I föreskriften ställs inga exakta krav på att genomföra informationssäkerhet. Orsaken är att företagen genomför den ändamålsenliga informationssäkerheten på olika sätt beroende på de tjänster företaget tillhandahåller..

Det väsentliga är att registraren identifierar de informationssäkerhetskrav som gäller för dess verksamhet samt de rutiner som behövs för att kraven ska uppfyllas i registrarverksamheten.

Transport- och kommunikationsverket förutsätter att registraren har uppdaterade dokument om på vilket sätt den genomför informationssäkerheten i sin verksamhet. Transport- och kommunikationsverket specificerar inte separat vilka dokument som krävs utan registraren får själv bestämma helheten. 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 paragrafen har beaktats i registrarverksamheten.

2.1.1 Delområden av informationssäkerheten

En registrar ska beakta följande i de olika skedena av förmedlingen av fi-domännamn:

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 15 § i Transport- och kommunikationsverkets föreskrift 68)
- dokumentationsrutiner och -system
- auditerings- och övningsförfaranden.

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.

Maskinvaru-, programvaru- och telekommunikationssäkerhet

- hantering av sårbarheter
- observation av kränkningar av informationssäkerheten (se 17–18 § i föreskrift 68)
- hantering av ändringar (se 19 § i föreskrift 68)
- datamaterial- och driftsäkerhet
- säkerställande av informationens konfidentialitet, integritet och tillgänglighet
- klassificering av datamaterial och behandling enligt klassificeringen (se 16 § i föreskrift 68)
- 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.

Fysisk säkerhet

- fysiskt läge för lokaler och omgivningens säkerhet
- åtkomsthantering
- strukturellt skydd.

Vid behov kan Transport- och kommunikationsverket utföra en auditering av registrarens registrarverksamhet.

Transport- och kommunikationsverkets föreskrifter finns på verkets webbsidor.

2.2 Riskhantering

En registrar ska identifiera de funktioner, data och system som är viktiga för registrarverksamhetens kontinuitet samt regelbundet bedöma och behandla informationssäkerhetsriskerna som hänför sig till dem samt riskhantering. Riskhanteringsprocessen och resultaten av riskbehandlingen ska dokumenteras.

Med säkerhetsrisk avses sannolikhet för en viss olägenhet eller skada och dess konsekvenser. Med informationssäkerhetsrisker avses en sådan oavsiktlig eller avsiktlig faktor som äventyrar konfidentialitet, integritet 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
- eldsvåda eller vattenskada
- fel och försummelser begångna av en underleverantör eller en aktör som ingår i samarbetsnätverket.

Målsättningen för riskhanteringen

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 och förebygga riskerna.

Riskidentifiering och -behandling

Bland annat följande standarder och publikationer om riskhantering har getts ut:

- ISO/IEC 27005
- NIST 800- 30 Risk Management Guide
- OCTAVE

Transport- och kommunikationsverket ålägger ingen skyldighet att iaktta en viss standard. Riskhanteringsmodeller skiljer sig i olika företag, och en enda modell som skulle passa för alla finns inte.

Transport- och kommunikationsverket förutsätter att registraren ska identifiera riskerna i sin verksamhet och verksamhetens kontinuitet och att den ska behandla riskerna. Med behandling 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.

Transport- och kommunikationsverket 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

- årligen

- när nya tjänster eller funktioner specificeras
- efter att en eventuell risk har realiserats.

Dokumentation av process och resultat

Transport- och kommunikationsverket övervakar registrarernas verksamhet och för att det ska kunna övervaka att kraven på riskhanteringen iakttas, ska registraren dokumentera den fastställda processen för riskhantering och resultaten från riskhanteringen.

2.3 Datamaterial

En registrar ska ha ett klassificeringssystem och hanteringsförfaranden i samband med klassificeringen för sådant datamaterial som är viktigt för registrarverksamheten.

Klassificeringssystemet och hanteringsförfarandet för datamaterial säkerställer att information som hänför sig till förmedlingen av domännamn är tillgänglig endast för dem som har rätt att använda den. Klassificeringskriterierna och hanteringsförfarandena ska dokumenteras och dokumentationen ska hållas uppdaterad.

2.3.1 Klassificering och hantering av material

Registraren ska fastställa sådana kriterier för klassificeringen av datamaterial som lämpar sig för dess verksamhet. Materialet kan klassificeras till exempel på följande sätt:

- offentligt
- konfidentiellt
- sekretessbelagt.

Dessutom ska registraren fastställa på vilket sätt företaget hanterar (skyddar) materialet som har indelats i olika klasser.

2.3.2 Materialdokument

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

- 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
- förstörande av uppgifter och dokument.

2.4 Övervakning av informationssäkerheten

En registrar ska kontinuerligt övervaka sin registrarverksamhet för att kunna upptäcka och förebygga situationer som stör eller hotar informationssäkerheten.

Registraren ska se till att händelser som är relevanta för informationssäkerheten noteras. En förutsättning för övervakningen är att kränkningar av och hot mot informationssäkerheten vid registrarverksamheten ska kunna upptäckas. I praktiken innebär detta att registraren ska underhålla ett system för administration av sin tjänst.

2.4.1 Upptäckt av hot

Det är viktigt att registraren på eget initiativ och snabbt agerar om den upptäcker olika slags 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.

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. Exempel på sådana situationer är

- överbelastningsangrepp
- informationsläckor
- försök till dataintrång
- för omfattande behörigheter.

2.4.2 Förebyggande av hot

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 sträva efter att upptäcka situationer som håller på att utvecklas till problem med hjälp av sina mekanismer för hantering av tjänsten. Mekanismer är t.ex.:

- 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 larm och mätare.
- anmälda observationer av sårbarheter i hårdvara eller mjukvara som förutser problem med informationssäkerheten.

2.4.3 Dokumentation av övervakningen

Registraren ska föra en uppdaterad dokumentation över övervakningsmekanismerna för 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 med vilka den hanterar och åtgärdar uppgifter och anmälningar om läget i sin tjänst.

2.5 Hantering av hot och störningar

En registrar ska utfärda egna anvisningar för situationer som stör eller hotar informationssäkerheten i registrarverksamheten. Med hjälp av anvisningarna kan man både reda ut och minimera situationerna.

Registraren ska på förhand göra upp tydliga procedurer som hjälper att reda ut störningar i eller hot mot informationssäkerheten i registrarverksamheten. Anvisningarna hjälper registraren att minimera verkningarna av situationer som nämns ovan och att återhämta sig från dem utan obefogat dröjsmål.

Procedurerna ska omfatta

- organisering av hanteringen av informationssäkerhet
- de olika aktörernas ansvar

- uppgifter som behövs för att nå de personer som svarar för informationssäkerheten.

Registraren ska dokumentera anvisningarna och hålla dem uppdaterade.

2.5.1 Procedurernas betydelse

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.

Procedurerna ska också beakta eventuella speciella anvisningar för avhjälpande av betydande störningar. Sådana 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.

2.6 Hantering av ändringar

Registrarerna ska sköta sina ändrings-, service- och uppdateringsåtgärder så att de orsakar minsta möjliga störning i registrarverksamheten.

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.

2.6.1 Planering av ändringar

Registraren ska reservera tillräckligt med tid för ändrings-, service- och uppdateringsåtgärder så att den planerade åtgärden kan utföras på ett kontrollerat sätt. Registraren ska specificera och dokumentera de processer och förfaranden som styr ändringarna.

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 att avbrotten ska dimensioneras så att registraren förutom behov av tjänster också tar hänsyn till det realistiska behovet av tid som ett omsorgsfullt ändringsarbete kräver.

För att hantera ändringar och minimera olägenheter ska registraren, innan den börjar genomföra ändringen, omsorgsfullt

- planera hur ändringsarbetet fortskrider
- beräkna behövliga resurser
- uppskatta ändringsarbetets inverkan och varaktighet
- 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.

2.6.2 Dokumentation av ändringar

Registraren ska i förväg definiera och dokumentera de processer och förfaringssätt som hänför sig till ändringsarbeten 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.

2.7 Dataskydd i registrarverksamheten

Registrarerna samlar in personuppgifter av domännamnsanvändare i syfte att registrera ett domännamn. Registrarerna antecknar uppgifterna i Transport- och kommunikationsverkets domännamnsregister och uppdaterar uppgifterna. Registrarverksamheten regleras genom EU:s dataskyddsförordning, Finlands lag och Transport- och kommunikationsverkets föreskrift.

Transport- och kommunikationsverket ingår inte avtal med registrarerna om behandlingen av personuppgifter. Registrarer av fi-domännamn som gjort en anmälan om registrarverksamhet till Transport- och kommunikationsverket förbinder sig att följa de skyldigheter som föreskrivs för registrarer i Finlands lag och Kommunikationsverkets föreskrift.

Lagen om tjänster inom elektronisk kommunikation (917/2014) samt Transport- och kommunikationsverkets föreskrift 68 utgör en rättslig grund för behandling av personuppgifter i enlighet med EU:s dataskyddsförordning (679/2014) i syfte att registrera och administrera domännamn, dvs. att bedriva registrarverksamhet.

Transport- och kommunikationsverkets lagstadgade uppgift är bl.a. att administrera toppdomänen fi och förvalta fi-domännamnsregistret. I enlighet med EU:s dataskyddsförordning är Transport- och kommunikationsverket den personuppgiftsansvarige i fråga om

personuppgifter i domännamnsregistret medan registrarerna är personuppgiftsbiträden för Transport- och kommunikationsverkets räkning.

2.7.1 Personuppgifter som samlas in i registrarverksamheten

De lagbaserade personuppgifter som samlas in i registrarverksamheten om domännamnsanvändare är:

- Namn
- Personbeteckning / annan beteckning som identifierar en person
- Postadress
- Telefon
- Kontaktperson och kontaktpersonens telefonnummer (juridiska personer)
- E-postadress (processadress)
- Registraren ska hålla uppgifterna uppdaterade.

Om registraren samlar in andra uppgifter om domännamnsanvändaren än ovan nämnda lagstadgade uppgifter, är registraren själv den personuppgiftsansvarige för dessa andra uppgifter.

2.7.2 Ändamålet för och arten av behandlingen av personuppgifter

Med förmedling av domännamn avses registreringar av fi-domännamn i domännamnsregistret och förvaltning av dessa uppgifter. Endast en verksamhetsutövare som har lämnat in en anmälan om registrarverksamheten till Transport- och kommunikationsverket, dvs. en registrar, får göra registreringar i domännamnsregistret.

Ett domännamn ska 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.

Registraren ska hålla uppgifterna korrekta och uppdaterade.

Registrarverksamheten omfattar alla de åtgärder som en registrar vidtar för att upprätthålla uppgifterna om domännamn i domännamnsregistret. Förvaltningen av domännamn omfattar att uppdatera kontaktuppgifter, förnya ett domännamns giltighet, överföra ett domännamn från en användare till en annan och byte av registrar.

Registrarverksamheten omfattar också anmälnings- och rådgivningsskyldigheter.

Om en registrar konfigurerar namnservrar för domännamnet ansvarar registraren för att namnservrarna fungerar i enlighet med Transport- och kommunikationsverkets föreskrift. Registraren har fullt ansvar över att dess

underleverantörer, andra tjänsteleverantörer eller andra som behandlar personuppgifter (t.ex. återförsäljare) uppfyller sina skyldigheter i förhållande till Transport- och kommunikationsverket.

Med domännamnsförvaltning avses även förmågan att göra anteckningar i domännamnsregistret med hjälp av tekniska arrangemang som Transport- och kommunikationsverket har fastställt samt att sörja för informationssäkerheten i verksamheten.

Registraren behandlar personuppgifter i enlighet med EU:s dataskyddsförordning, Finlands lag och Transport- och kommunikationsverkets föreskrift.

Om registraren tillhandahåller domännamnsanvändare andra tjänster än lagstadgade registrarverksamhetstjänster (t.ex. hemsidetjänster, e-posttjänster, serverutrymme, osv.) och i samband med dessa samlar in personuppgifter om domännamnsanvändaren, är registraren i fråga om dessa uppgifter själv den personuppgiftsansvarige som ska ha en behandlingsgrund för uppgifterna i enlighet med EU:s dataskyddsförordning.

Föremålet för behandlingen och behandlingens varaktighet

Registrarerna får behandla de personuppgifter som de registrerar och uppdaterar i domännamnsregistret endast för den tid som registraren i fråga upprätthåller domännamnet och/eller domännamnet är i kraft skyddstiden medräknad. Registraren ansvarar för att domännamnsanvändarnas personuppgifter raderas från sina system.

2.7.3 Registrarens skyldigheter som personuppgiftsbiträde

Vid behandlingen av domännamnsanvändarnas personuppgifter i registrarverksamheten ska registraren iaktta skyldigheterna för personuppgiftsbiträde enligt artikel 28 i EU :s dataskyddsförordning.

Om registraren anlitar återförsäljare, ska den registrera uppgifter om återförsäljare i Transport- och kommunikationsverkets domännamnsregister och uppdatera dem. Registraren är fullt ansvarig för återförsäljarnas verksamhet (artikel 28.2 i EU:s dataskyddsförordning).

Registraren får behandla domännamnsanvändarens personuppgifter endast i enlighet med lagen om tjänster inom elektronisk kommunikation och Transport- och kommunikationsverkets föreskrift 68. MPS-dokumentet, dvs. motivering till och tillämpning av föreskriften, preciserar på ett mer konkret sätt hur domännamnsföreskriften ska tillämpas i praktiken.

Registraren har inte rätt att lämna ut personuppgifter ur Transport- och kommunikationsverkets domännamnsregister utan lagstadgad grund (artikel 28.3 i EU:s dataskyddsförordning).

Transport- och kommunikationsverket har en söktjänst för de offentliga uppgifterna i domännamnsregistret.

Registraren ska till Transport- och kommunikationsverket lämna de begäranden som gäller andra uppgifter i domännamnsregistret än de offentliga (artikel 28.3 e i EU:s dataskyddsförordning).

Om registraren lämnar ut personuppgifter ur Transport- och kommunikationsverkets domännamnsregister på basis av en annan lagstiftning som tillämpas på registraren, ska registraren informera Transport- och kommunikationsverket om det rättsliga kravet innan uppgifterna lämnas ut, såvida sådan information inte är förbjuden med hänvisning till ett viktigt allmänintresse enligt denna rätt (artikel 28.3 i EU:s dataskyddsförordning).

Personer anställda hos registraren ska iaktta konfidentialitet för de personuppgifter de behandlar (artikel 28.3 b i EU:s dataskyddsförordning).

Registraren ska sörja för informationssäkerheten i sin verksamhet. Att sörja för informationssäkerheten är registrarens lagstadgade skyldighet om vilken det bestäms i 170 § 1 mom. 6 punkten i lagen om tjänster inom elektronisk kommunikation samt i artikel 32 i EU:s dataskyddsförordning. Med informationssäkerhet avses enligt 3 § 1 mom. 28 punkten i lagen administrativa och tekniska åtgärder genom vilka informationens konfidentialitet, integritet och tillgänglighet säkerställs. I 4 kap. i Transport- och kommunikationsverkets domännamnsföreskrift 68 beskrivs de minimikrav för hantering av informationssäkerheten som alla registrarer ska uppfylla i sin verksamhet.

MPS-dokumentet, dvs. motivering till och tillämpning av föreskriften, preciserar på ett mer konkret sätt hur informationssäkerhetskraven ska tillämpas i praktiken.

Registrarens skyldighet är att bistå Transport- och kommunikationsverket med att se till att skyldigheterna i EU:s dataskyddsförordning fullgörs (artikel 28.3 f i EU:s dataskyddsförordning).

Registraren ska radera domännamnsanvändarens uppgifter ur sina system efter att domännamnsanvändaren inte längre är kund hos registraren eller domännamnets giltighetstid jämte skyddstid har löpt ut (artikel 38.3 g i EU:s dataskyddsdirektiv). Transport- och kommunikationsverket lagrar arkiverade personuppgifter under tio år.

Transport- och kommunikationsverket övervakar registrarer och utför granskningar som tillsynsåtgärd. Registraren ska möjliggöra Transport- och kommunikationsverkets granskningar (artikel 28.3 h i EU:s dataskyddsdirektiv).

Registraren ska omedelbart informera Transport- och kommunikationsverket om den anser att Transport- och kommunikationsverkets instruktion strider mot bestämmelserna i EU:s dataskyddsförordning (artikel 28.3 h i EU:s dataskyddsförordning).

Om registraren överträder EU:s dataskyddsförordning genom att själv fastställa ändamålen med och medlen för behandlingen av personuppgifter, anses registraren vara personuppgiftsansvarig med avseende på den behandlingen (artikel 28.10 i EU:s dataskyddsförordning).

Registraren ska hålla domännamnsanvändarens personuppgifter korrekta och uppdaterade.

Registraren ska utan dröjsmål göra en anmälan om kränkningar av personuppgifternas informationssäkerhet till Transport- och kommunikationsverket.

Registraren ska göra upp ett dataskyddsregister över behandling (artikel 30.2 i EU:s dataskyddsförordning).

2.7.4 Domännamnsanvändarens rättigheter

Den registrerade, dvs. domännamnsanvändaren, har:

1. rätt att få uppgift om vem som använder användarens personuppgifter

Domännamnsanvändarens personuppgifter behandlas av registrarer och Transport- och kommunikationsverket. Registrarerna kan anlita underleverantörer (återförsäljare), och registrarerna har fullt ansvar över deras verksamhet.

2. rätt att få uppgift om ändamålet med behandlingen av uppgifterna

Domännamnsanvändarens personuppgifter används för registrering och förvaltning av domännamn samt för avgörande av tvister om fi-domännamn. Registrarerna registrerar och förvaltar domännamn. Transport- och kommunikationsverket förvaltar ett register över fi-domännamn och avgör tvister om fi-domännamn på yrkande av rättsinnehavarna.

3. rätt att kontrollera och rätta felaktiga uppgifter.

På Transport- och kommunikationsverkets webbsidor finns en elektronisk blankett för kontrollbegäran.

Mer information om behandlingen av personuppgifter finns på Transport- och kommunikationsverkets webbsidor.

2.8 Skyldighet att anmäla störningar i informationssäkerheten

En registrar ska göra en anmälan om dess förmedling av domännamn är utsatt för kränkningar av eller hot mot informationssäkerheten.

Registraren ska utan dröjsmål meddela Transport- och kommunikationsverket om dess förmedling av domännamn är utsatt för

- betydande kränkningar av informationssäkerheten
- hot om en betydande kränkning av informationssäkerheten eller för någonting annat som väsentligen förhindrar eller stör den.

Registraren ska också anmäla

- hur länge störningen eller hotet beräknas pågå
- konsekvenser
- åtgärder för avhjälpande
- åtgärder för att förhindra att störningen upprepas.

I en anmälan om betydande informationssäkerhetsstörning till Transport- och kommunikationsverket ska en registrar, i mån av möjlighet, redogöra för orsaken till störningen eller hotet och hur störningen har framkallats.

2.8.1 Störningsanmälan ska göras omedelbart

Störningsanmälan ska göras inom 24 timmar från det att registraren har fått veta om störningen.

Exempelvis i en situation där någon har gjort intrång i registrarens system är det nödvändigt att tillsynsmyndigheten utan dröjsmål får veta om det. Risken är att den som står bakom intrånget fritt kan komma åt att ändra uppgifter om domännamn som registraren i fråga förvaltar, såsom namnservrar. Hotet kan även gälla ett större antal kunder beroende på registrarens kundunderlag.

Anmälan görs i första hand via form.

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, dock 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.

2.8.2 Betydande kränkningar av informationssäkerheten

Transport- och kommunikationsverket ska informeras om betydande kränkningar av informationssäkerheten för registrarverksamheten.

Kränkningar av informationssäkerheten kan ha konsekvenser för uppgifternas eller datasystemens konfidentialitet, integritet eller tillgänglighet.

Tillförlitlighet: Uppgifter och verifieringsuppgifter om användarnamn är endast tillgängliga för dem som är berättigade att få uppgifterna.

Integritet: Det är inte möjligt att obehörigt göra ändringar i uppgifter. Utomstående har inte möjlighet att inverka på datasystemens funktion.

Tillgänglighet: En tjänst och uppgifter i tjänsten är tillgängliga för dem som är berättigade till den.

Bedömning av betydelsen av kränkningar av informationssäkerheten

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. En störning i informationssäkerheten är alltid betydande om den drabbar ett av följande skyddade objekt:

- de data- 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.

Typer av kränkningar av informationssäkerheten som omfattas av anmälningsskyldigheten

Förteckningen över typer av informationssäkerhetskränkningar som finns nedan är inte uttömmande utan syftet är att beskriva allvarlighetsgraden för de fall som ska anmälas. Efter gottfinnande kan registrarerna också underrätta Transport- och kommunikationsverket om kränkningar och hot om kränkningar av informationssäkerheten som är av mindre betydelse.

Betydande störningar i informationssäkerheten som ska anmälas till Transport- och kommunikationsverket är till exempel:

- dataintrång i registrarens datasystem
- 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 Transport- och kommunikationsverkets domännamnsregister
- 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 eller
- 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 sköta sina andra informationssäkerhetsuppgifter.

Transport- och kommunikationsverket har 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.

De nödvändiga åtgärder som Transport- och kommunikationsverket vidtar kan utföras med avseende på namnserverinformationen i fi-roten och kan omfatta:

- åtgärder för att förhindra eller begränsa den trafik som riktas till domännamnet
- åtgärder för att dirigera den trafik som riktas till domännamnet till en annan webbadress
- andra jämförbara åtgärder av teknisk natur.

Transport- och kommunikationsverkets särskilda uppgifter är också att:

- främja den elektroniska kommunikationens funktion, störningsfrihet och trygghet
- 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
- informera om frågor som gäller informationssäkerhet samt om kommunikationsnäts och kommunikationstjänsters funktion
- utreda kränkningar och hot om kränkningar av informationssäkerheten för nättjänster, kommunikationstjänster och mervärdestjänster.

2.9 Namnservrar

En registrar ansvarar för att de namntjänster som tillhandahålls kunderna i samband med fi-domännamn är konfigurerade enligt de tekniska kraven.

Ett fi-domännamn kan registreras antingen med fungerande namnservrar eller utan namnservrar. Om man uppger namnservrar måste de alla vara fungerande. Namnservrar ska avlägsnas ur fi-roten om en domännamnsanvändare fortfarande vill reservera sitt domännamn utan att det har några anslutna funktioner som e-post eller en webbplats (s.k. parkeringstjänst).

Krav på namnservrarna

Enligt Transport- och kommunikationsverkets föreskrift 68/2014 M ska minst två och högst tio av varandra oberoende namnservrar konfigureras med ett domännamn. Detta säkerställer att domännamnet fungerar även om det uppstår ett fel i en av namnservrarna.

Namnservrarna är oberoende av varandra när namnservrarna fungerar

- på olika servrar
- på olika IP-adresser
- bakom olika internetförbindelser.

Namnservrarna ska dessutom

- kunna nås av datornätet internet
- kunna granska konfigurationerna med Transport- och kommunikationsverkets namnserverförfrågningar.

Transport- och kommunikationsverket kontrollerar 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.

Konfigurationerna kan kontrolleras med ett namnservertest som finns på Transport- och kommunikationsverkets webbsidor.

Informationssäkerhetsrekommendationer för namnservrar

Transport- och kommunikationsverket rekommenderar att överföring av domännamnsinformation (AXFR, DNS zone transfer protocol) förhindras för utomstående. Namnservrarna bör inte heller returnera rätt information vid förfrågan om serverns programversion. Att återställa den rätta programversionen kan riskera informationssäkerheten, om det finns ett känt informationssäkerhetsproblem i den version av namnserverprogrammet som används.

2.9.1 Konfigurationer av namnservrar

Namnservrarna måste uppfylla de krav som ställts på dem. Det rekommenderas också att man använder serienummer och klockor för SOA-poster i standardformat.

Namnservrarna ska 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 antingen A- eller AAAA-posten (eller båda) i DNS-tjänsten. NS-posterna kan endast vara

namnservrar för vilka ett domännamn de facto har konfigurerats. NS-posterna ska vara förenliga med uppgifterna i fi-roten.

Krav och rekommendationer för SOA-post

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

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

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. Exempel: hostmaster.domain.fi. Bästa sättet att konfigurera en hostmaster-adress i fältet RNAME är att följa RFC 2142.

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:

```
fi.example. 3600 SOA dns.fi.example. hostmaster.fi.example. (
2018090401 ; serial YYYYMMDDnn
86400 ; refresh ( 24 hours)
7200 ; retry ( 2 hours)
3600000 ; expire (1000 hours)
172800 ) ; minimum ( 2 days)
```

Serienummer

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).

Refresh och retry

Värdena i fälten 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.

Expire

Värdet för fältet 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.

TTL

Värdet för fältet 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.

2.9.2 Säkerhetstillägget DNSSEC

DNSSEC (Domain Name System Security Extensions) är en tjänst som förbättrar informationssäkerheten för namntjänsten och som även kan införas för fi-domännamn.

DNSSEC är en utvidgning av namntjänsten med vilken det är möjligt att garantera det pålitliga ursprunget och integriteten av uppgifterna från namnservern.

När DNSSEC används för ett fi-domännamn, signeras svaren på DNS-förfrågningarna digitalt. DNSSEC säkerställer att svaren på DNS-förfrågningarna kommer från rätt avsändare och att uppgifterna inte har modifierats på vägen. Användare av en webbsida som är förknippad med domännamnet i fråga kan vara säkra på att de kommer just till den webbsida de hade för avsikt att besöka.

För att DNSSEC ska fungera måste även den använda DNS-resolvern stöda valideringen av DNSSEC-signeringar. Annars kan DNSSEC-förtroendekedjans integritet inte säkerställas.

Tillhandahållande av säkerhetstillägget till kunder

En registrar kan börja använda DNSSEC-teknik genom att signera domännamnets uppgifter. Efter det kan registraren lägga till DS-posterna för domännamnet. DS-posterna kan administreras via både EPP-gränssnittet och webbläsargränssnittet. Via EPP-gränssnittet är det möjligt att automatisera utbyte av nycklarna.

För att skapa en digital signatur behöver man

- en privat nyckel som är hemlig och bara ägaren har tillgång till den samt
- en publik nyckel som publiceras i namntjänsten i sin egen datapost.

Signaturen kan kontrolleras och valideras med en publik nyckel som motsvarar den privata nyckeln. En resolver gör valideringen på användarens vägnar.

De publika nycklarna för fi-zonen publiceras i rotzonen. Det rekommenderas att registrarer som tillhandahåller resolvrar konfigurerar rotzonens förtroendeankare med sina namnservrar. Förtroendeankaren finns på IANAs DNSSEC-sidor.

En åskådlig beskrivning av hur DNSSEC fungerar finns t.ex. i Transport- och kommunikationsverkets DNSSEC-broschyr som finns tillgänglig på Transport- och kommunikationsverkets webbsidor.

Parametrar som används vid DNSSEC-signaturer i fi-zonen

- Hashfunktion: SHA-256
- Signaturalgoritm: RSA
- NSEC3
- Opt-Out
- Zone Signing Key (ZSK): RSA 1024-bit (övergång till 2048-bit inom kort)
- Key Signing Key (KSK): RSA 2048-bit.

Med KSK signeras endast zonens DNSKEY-poster. ZSK används för signering av zonens övriga DNS-poster, såsom DS-poster för signerade underzoner samt poster som är auktoritära för fi-zonen. Livslängd för ZSK är en månad och för KSK ett år.

Ytterligare information:

Mer information om säkerhetstillägget DNSSEC får du via

`fi-domain-tech@ficora.fi.`

2.9.3 DNS-test

Med hjälp av Transport- och kommunikationsverkets verktyg för DNS-test som finns tillgängliga på verkets webbplats kan du kontrollera att domännamnets namntjänster fungerar.

Testet hjälper till att kontrollera

- om fi-domännamnet har konfigurerats med namnservrarna enligt Transport- och kommunikationsverkets krav
- om fi-domännamnets namntjänster fungerar just nu
- om domännamnet använder säkerhetstillägget DNSSEC.

Om Transport- och kommunikationsverket har skickat ett felmeddelande om namnservrar som inte fungerar, ger DNS-testet närmare information om felet.

Du kan kontrollera namnservrarnas funktion även innan du registrerar ett domännamn. Om du tänker ändra namnservrar kan du testa om de nya namnservrarna överensstämmer med Transport- och kommunikationsverkets föreskrifter.

2.10 Tekniska gränssnitt

Som tekniskt gränssnitt mot fi-domännamnsregistret använder registraren antingen ett webbläsargränssnitt eller det EPP-gränssnitt som Kommunikationsverket har specificerat.

2.10.1 Webbläsargränssnitt

Registraren kan logga in på Transport- och kommunikationsverkets fi-domännamnsregister via webbläsargränssnittet. För inloggningen används tvåfaktorsautentisering.

Tvåfaktorsautentisering betyder att det för inloggningen behövs ett engångslösenord utöver ett användar-id och lösenord. Koden för engångsinloggningen är ett lösenord som består av åtta siffror och skickas till registrarens mobiltelefon per sms.

Inloggningen förutsätter att registraren har gjort en anmälan till Transport- och kommunikationsverket.

2.10.2 EPP-gränssnitt

EPP (Extensible Provisioning Protocol) är ett XML-baserat tekniskt gränssnitt som en registrar kan ansluta till från sitt eget kundprogram.

Transport- och kommunikationsverket tillhandahåller inget färdigt kundprogram, utan registraren måste själv programmera sitt kundprogram eller anskaffa ett sådant.

Det är inte nödvändigt att använda EPP-gränssnittet. Registraren kan även använda båda gränssnitten.

Registrarens kundprogram måste vara kompatibelt med Transport- och kommunikationsverkets EPP-gränssnittsbeskrivning som baserar sig på RFC-dokument och innehåller en närmare beskrivning av de begränsningar och tillägg som gjorts i gränssnittet.

Innan en registrar kan börja använda Transport- och kommunikationsverkets EPP-gränssnitt, måste registrarens eget kundprogram genomgå testerna i Transport- och kommunikationsverkets EPP-testsystem.

EPP-gränssnittets adress är

`https://epp.domain.fi` (port 700).

2.10.3 RFC-standarder

Transport- och kommunikationsverkets EPP-gränssnitt baserar sig huvudsakligen på följande RFC-standarder:

- RFC 4310 Domain Name System (DNS) Security Extensions Mapping for the Extensible Provisioning Protocol (EPP)
- RFC 5730 Extensible Provisioning Protocol (EPP)
- RFC 5731 Extensible Provisioning Protocol (EPP) Domain Name Mapping
- RFC 5732 Extensible Provisioning Protocol (EPP) Host Mapping
- RFC 5733 Extensible Provisioning Protocol (EPP) Contact Mapping
- RFC 5910 Domain Name System (DNS) Security Extensions Mapping for the Extensible Provisioning Protocol (EPP).

2.10.4 Katakri-kraven vid användning av EPP-gränssnittet

Katakri är ett auditeringsverktyg för myndigheter när de bedömer den berörda organisationens förmåga att skydda myndighetens sekretessbelagda information.

Om registraren använder Transport- och kommunikationsverkets EPP-gränssnitt som ett tekniskt gränssnitt, måste registraren uppfylla kriterierna härledda från skyddsnivå (IV) enligt delområde I, teknisk informationssäkerhet, i den version av Katakri (verktyg för informationssäkerhetsauditering) som gäller vid respektive tidpunkt, till följande delar:

1. datakommunikationssäkerhet
2. säkerhet i informationssystem.

I auditeringsverktyget Katakri har man samlat in de minimikrav som grundar sig på nationella författningar och internationella förpliktelser. 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.

Delområdena i kraven

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 skyddsnivåer enligt den information som behandlas (ST IV, ST III, ST II).

Registrarer som använder Transport- och kommunikationsverkets EPP-gränssnitt förutsätts uppfylla kraven på den tekniska informationssäkerhetens delområde gällande datakommunikationssäkerhet och säkerhet i informationssystem.

Kraven gäller förmedling av domännamn. Registraren ansvarar för att kraven uppfylls. Vid behov kan Transport- och kommunikationsverket utföra en auditering av registrarverksamheten.

Om den som förmedlar domännamn också utövar annan verksamhet, gäller kraven inte den andra verksamheten.

Transport- och kommunikationsverkets föreskrift hänvisar till gällande kriterier. Den gällande versionen av Katakri finns på finska på försvarsministeriets webbplats.

Om registraren använder Transport- och kommunikationsverkets EPP-gränssnitt som ett tekniskt gränssnitt, måste registraren uppfylla kriterierna härledda från skyddsnivå (IV) enligt delområde I, teknisk informationssäkerhet, i den version av Katakri som gäller vid respektive tidpunkt, till följande delar:

1. datakommunikationssäkerhet
2. säkerhet i informationssystem.

2.10.5 EPP-testsystem

En registrar som använder EPP-gränssnittet måste ha ett eget kundprogram som är kompatibelt med Transport- och kommunikationsverkets EPP-gränssnitt. Registrarens kundprogram måste genomgå de tester som Transport- och kommunikationsverket kräver.

Om registraren använder Transport- och kommunikationsverkets EPP-gränssnitt ska registrarens kundprogram motsvara Transport- och kommunikationsverkets EPP-gränssnittsbeskrivning.

Innan en registrar kan börja använda Transport- och kommunikationsverkets EPP-gränssnitt, måste registrarens kundprogram genomgå testerna i Transport- och kommunikationsverkets EPP-testsystem.

Till stöd för testningen finns följande dokument på Transport- och kommunikationsverkets webbsidor:

- EPP-testanvisning
- EPP-gränssnittsbeskrivning
- XML-schemana

I frågor som gäller testningen kontakta oss i första hand per e-post: fi-domain-tech@traficom.fi.

2.10.6 Whois-tjänsten för fi-domänen

Registraren kan använda Transport- och kommunikationsverkets whois-tjänst så att registrarens kunder kan ta reda på om ett visst fi-domännamn är ledigt.

Tjänsten finns på adressen whois.fi. För tjänsten behöver registraren ett whois-kundprogram som finns i de flesta Unix- och Linux-operativsystem.

2.10.7 Domain Availability Service (DAS)

Transport- och kommunikationsverkets DAS-tjänst (Domain Availability Service) är planerad för snabba förfrågningar om fi-domännamnens tillgänglighet. Tjänsten svarar om domännamnet är ledigt för registrering. Tjänsten hämtar inte några uppgifter om användaren av domännamnet eller ger närmare information om domännamnets status.

Tjänsten är tillgänglig på adressen

`das.domain.fi` (port 715/UDP)

På Transport- och kommunikationsverkets webbplats finns en särskild tjänstebeskrivning av DAS.

2.10.8 OData

Via domännamnssystemets OData-gränssnitt är det möjligt att få information om domännamn (Domains) registrerade av organisationer och sammanslutningar. Data omfattar också uppgifter om domännamnens namnservrar (NameServers) samt kontaktinformation till dem som förvaltar domännamn.

Beakta att det via gränssnittet i regel inte erbjuds information om domännamn reserverade av privatpersoner. Därför kan gränssnittet inte användas för att kontrollera om ett visst domännamn finns tillgängligt. Denna begränsning är värd att beaktas även vid övriga sökningar. Materialet täcker i praktiken cirka 80 procent av domännamnen.

Uppgifterna i OData uppdateras en gång i dygnet.

På Transport- och kommunikationsverkets webbplats finns en särskild tjänstebeskrivning av OData.

2.11 Att anmäla sig som registrar

Den som vill bli en registrar måste, före inlämnandet av anmälan till Transport- och kommunikationsverket, omsorgsfullt bekanta sig med alla de krav som uppställts i lag.

Fi-registrarverksamheten regleras genom bestämmelserna i lagen om tjänster inom elektronisk kommunikation. Om du vill bli en registrar är det ytterst viktigt att ta reda på att du uppfyller alla de informationssäkerhetsskyldigheter och övriga skyldigheter som ålagts en registrar.

Anmälan om registrarverksamhet görs på Transport- och kommunikationsverkets elektroniska blankett. Transport- och kommunikationsverket ska utan dröjsmål informeras om ändringar i de uppgifter som registraren har anmält. Transport- och kommunikationsverket rekommenderar att registraren uppdaterar ändringarna i verkets domännamnsregister inom tre dagar.

Registraren kan använda logotypen fi-registrar i registrarverksamheten. Logotypens publiceringsbara versioner finns på Transport- och kommunikationsverkets webbsidor.

2.11.1 Lagstadgad processadress och övriga e-postadresser

Transport- och kommunikationsverket använder för alla höranden och delgivningar som gäller fi-domännamn den e-postadress som är införd i domännamnsregistret. Därför kan en handling eller ett beslut som gäller domännamn alltid delges per e-post. Denna så kallad processadress har stor rättslig betydelse och det är obligatoriskt för registrarerna att ange den till Transport- och kommunikationsverket.

Med hjälp av en processadress kan Transport- och kommunikationsverket snabbt delge bindande beslut, eftersom beslutet eller handlingen då anses ha delgivits den tredje dagen efter det att meddelandet sändes.

En rätt processadress för en registrar är en viktig uppgift och med tanke på registrarens rättsskydd är det ytterst viktigt att den är uppdaterad. Registraren ansvarar också för att domännamnsanvändarens processadress anmäls i systemet och att den hålls uppdaterad.

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.

2.11.2 Återförsäljarnas verksamhet

Transport- och kommunikationsverket övervakar registrarverksamheten. Om registraren anlitar återförsäljare, är registraren också ansvarig för deras verksamhet. En återförsäljare kan till exempel sköta kundtjänsten och faktureringen för fi-domännamn. Om registraren lägger till återförsäljarens uppgifter i fi-domännamnsregistret, visas de i de offentliga whois-uppgifterna om fi-domännamn under ”Återförsäljare”.

Bestämmelserna i lagen om tjänster inom elektronisk kommunikation förpliktar uttryckligen för den som gjort en anmälan om registrarverksamhet till Transport- och kommunikationsverket. Registraren ansvarar för att även registrarens återförsäljare iakttar de krav som uppställts för fi-domännamnsverksamheten.

2.12 PGP-nycklar

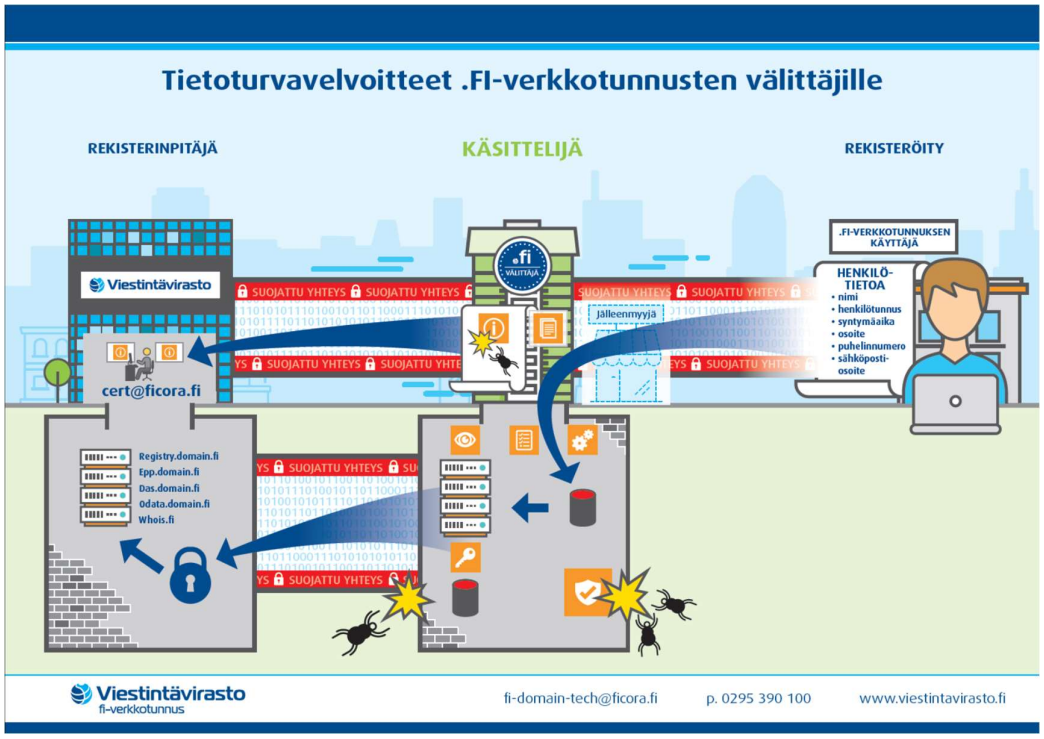
En del av de e-postmeddelanden som gäller Transport- och kommunikationsverkets fi-domännamn signeras med rollnycklar, m.a.o. PGP-nycklar.

PGP-programmet används för att kryptera eller signera e-postmeddelanden. PGP är ett program som baserar sig på den publika nyckelns infrastruktur.

E-postmeddelandet signeras med avsändarens privata nyckel.

Ett signerat e-postmeddelande kan verifieras med avsändarens publika nyckel. Med avsändarens publika nyckel kan man kontrollera att meddelandet kommer från rätt håll.

På Transport- och kommunikationsverkets webbsidor hittar du de PGP-nycklar som verket använder.



Miksi tietoturvaa?

- *Varmistutaan siitä, että merkittävät tietoturvaloukkaukset havaitaan ja hoidetaan ajoissa, mieluummin toki ennen asiakkaiden valituksia.*
- *Asiakkaat haluavat valita luotettavan välittäjän, joka pitää hyvää huolta heidän liiketoiminnastaan ja henkilötiedoistaan.*
- *Luvaton pääsy verkkotunnusrekisteriin käyttäen välittäjältä varastettuja tunnuksia vahingoittaa sekä välittäjän että verkkotunnusjärjestelmän toimintaa.*
- *Tietoturvahäiriöiden välttäminen johtaa parempaan toimintavarmuuteen, ja auttaa välttämään myös häiriöiden aiheuttamia odottamattomia kuluja.*

Tietoliikenne- ja tietojärjestelmäturvallisuus

- Suomen laki ja Viestintäviraston määräys edellyttävät, että verkkotunnusvälittäjä huolehtii järjestelmänsä tietoturvasta Viestintäviraston ohjeistamalla tavalla.
- Jos välittäjä käyttää EPP-rajapintaa, järjestelmän on myös toteutettava KATAKRI:n (tason IV) tietoliikenne- ja tietojärjestelmävaatimusosuudet. (Ajantasainen versio KATAKRI 2015, sivut 30-52) http://www.defmin.fi/puolustushallinto/puolustushallinnon_turvallisuustoiminta/katakri_2015_-_tietoturvallisuuden_auditointityokalu_viranomaisille.
- Jos välittäjä käyttää selainkäyttöliittymää, tietoturvavelvoitteet ovat vastaavat, mutta KATAKRI:n noudattaminen ei ole pakollista. Suosittelemme silti kaikille välittäjille KATAKRI:in perehtymistä.

Turvallisuusdokumentit

1. Riskienhallinnan prosessit ja tulokset

- Riskien määrittäminen ja toimenpiteet niiden huomioimiseksi on osa normaalia liiketoimintaa erityisesti silloin kun turvalliset ja luotettavat yhteydet ovat välittäjien liiketoiminnan ytimessä. Välittäjä: ovathan riskienhallinnan dokumenttinne ajan tasalla? Valmistautukaa perustelemaan valitsemanne toimenpiteet.

2. Luokittelukriteerit ja arkaluonteisten aineistojen käsittely

- Henkilötiedot ovat arkaluonteista aineistoa. Kuinka säilytätte ja suojelette sitä?
- Pääsytunnukset EPP-rajapintaan tai selainkäyttöliittymään on suojattava huolella.

3. Valvontamekanismit

- Olkaa tietoisia siitä mitä tapahtuu omassa järjestelmässänne, jotta pystytte reagoimaan ajallaan. Ovatko tunkeutumisesto- ja havainnointijärjestelmänne ajan tasalla?

4. Tietoturvaloukkausten käsittely

- Kuinka tietoturvaloukkaukset havaitaan?
- Kuinka tietoturvaloukkauksista toivutaan?
- Tietoturvaloukkauksista ilmoitetaan vapaamuotoisella sähköpostilla osoitteeseen cert@ficora.fi tai Viestintäviraston asiointilomakkeella. Ilmoittamisprosessien tulee olla ohjeistettu henkilökunnalle.

Ilmoitus tietoturvaloukkauksesta

- Arvioitu kesto
- Vaikutukset
- Korjaustoimenpiteet
- Tilanteen toistumisen ennaltaehkäisevät toimenpiteet

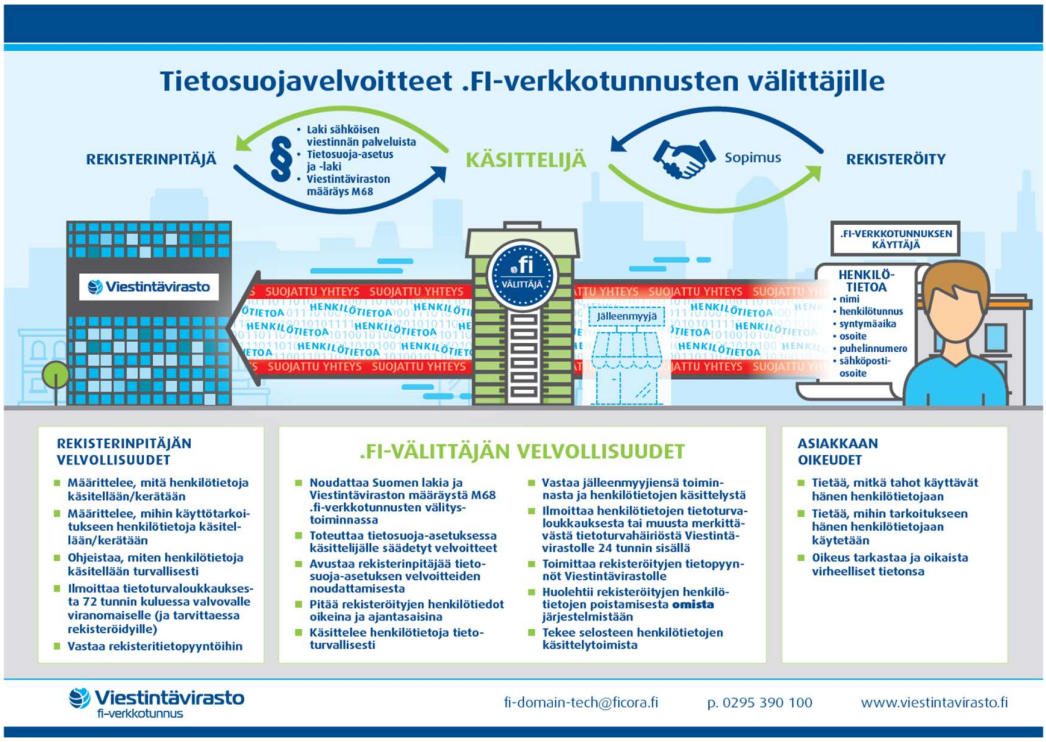
5. Muutostenhallinnan prosessit

- Muutostöiden tulee olla suunniteltuja ja huoltoikkunoiden tarpeeksi pitkiä.

Muistettavaa

- Suomen lain edellyttämä välitystoiminnan tietoturva -ohjeistus "Välitystoiminnan tietoturva" on osoitteessa https://www.viestintavirasto.fi/fiverkkotunnus.html.
- Uuden tietosuojalain vuoksi saatatte joutua muuttamaan toimintatapojanne, hankkimaan uusia ohjelmistoja tai laitteita.
- Viestintävirasto tulee kysymään teiltä yksityiskohtaisempia kysymyksiä valitsemistanne tietoturvatoimenpiteistä, joten pitäkää dokumenttinne ajan tasalla.
- Haluamme olla avuksi! Lähetämme teille sähköpostia tulevista muutoksista. Lisäohjeita ja oppaita on tulossa tietoturvavaatimuksista.

Viestintävirasto
fi-verkkotunnus
fi-domain-tech@ficora.fi
p. 0295 390 100
www.viestintavirasto.fi


Tietosuojavelvoitteet .FI-verkkotunnusten välittäjille
REKISTERINPITÄJÄ
• Laki sähköisen viestinnän palveluista
• Tietosuoja-asetus ja -laki
• Viestintäviraston määräys M68
KÄSITTELIJÄ
Sopimus
REKISTERÖITY
Viestintävirasto
.fi VÄLITTÄJÄ
Jälleenmyyjä
.FI-VERKKOTUNNUKSEN KÄYTTÄJÄ
HENKILÖ-TIETOA
• nimi
• henkilötunnus
• syntymäaika
• osoite
• puhelinnumero
• sähköposti-osoite
SUOJATTU YHTEYS
HENKILÖTIETOA
REKISTERINPITÄJÄN VELVOLLISUUDET
Määrittelee, mitä henkilötietoja käsitellään/kerätään
Määrittelee, mihin käyttötarkoitukseen henkilötietoja käsitellään/kerätään
Ohjeistaa, miten henkilötietoja käsitellään turvallisesti
Ilmoittaa tietoturvaloukkauksesta 72 tunnin kuluessa valvovalle viranomaiselle (ja tarvittaessa rekisteröidyille)
Vastaa rekisteritietopyyntöihin
.FI-VÄLITTÄJÄN VELVOLLISUUDET
Noudattaa Suomen lakia ja Viestintäviraston määräystä M68 .fi-verkkotunnusten välitystoiminnassa
Toteuttaa tietosuoja-asetuksessa käsittelijälle säädetyt velvoitteet
Avustaa rekisterinpitäjää tietosuoja-asetuksen velvoitteiden noudattamisesta
Pitää rekisteröityjen henkilötiedot oikeina ja ajantasaisina
Käsittelee henkilötietoja tietoturvallisesti
Vastaa jälleenmyyjiensä toiminnasta ja henkilötietojen käsittelystä
Ilmoittaa henkilötietojen tietoturvaloukkauksesta tai muusta merkittävästä tietoturvahäiriöstä Viestintävirastolle 24 tunnin sisällä
Toimittaa rekisteröityjen tietopyynnöt Viestintävirastolle
Huolehtii rekisteröityjen henkilötietojen poistamisesta **omista** järjestelmistään
Tekee selosteen henkilötietojen käsittelytoimista
ASIAKKAAN OIKEUDET
Tietää, mitkä tahot käyttävät hänen henkilötietojaan
Tietää, mihin tarkoitukseen hänen henkilötietojaan käytetään
Oikeus tarkastaa ja oikaista virheelliset tietonsa
Viestintävirasto
fi-verkkotunnus
fi-domain-tech@ficora.fi
p. 0295 390 100
www.viestintavirasto.fi