Bilaga B3 - Förtydliganden till bilaga B1 och B2

Inledning

I detta dokument anges förtydliganden i fråga om den förhandsprövning som ska göras av sökande som vill delta i auktionen av tillstånd att använda radiosändare i 900 MHz-, 2,1 GHz- och 2,6 GHz-banden. Förhandsprövningen syftar till att bedöma om radioanvändningen enligt tillståndsansökan kan antas komma att orsaka skada för Sveriges säkerhet, enligt 3 kap. 6 § punkten 7 LEK. Prövningen görs av Post- och telestyrelsen (PTS) efter samråd med Säkerhetspolisen och Försvarsmakten (nedan samrådsmyndigheterna).

I ansökan ska sökande svara på frågorna i bilaga B1 och redovisa för hur respektive princip samt kriterier för bedömning av aktörer i bilaga B2 beaktas.

Vissa allmänna förtydliganden

PTS och samrådsmyndigheterna ställer inte några särskilda formkrav på hur redovisningen i ansökan ska utformas. Det är önskvärt att frågorna besvaras så tydligt och lättillgängligt som möjligt. Svaren på frågorna i bilaga B1 respektive redovisningen för hur respektive princip samt kriterier för bedömning av aktörer i bilaga B2 beaktas kan lämnas i skilda dokument. Redovisningen av beaktandet av de 16 styrande principerna i bilaga B2 bör i varje avsnitt hänvisa till den eller de principer som är relevanta.

Prövningen av huruvida radioanvändningen enligt tillståndsansökan kan antas komma att orsaka skada för Sveriges säkerhet sker enligt 3 kap. 6 § lagen (2003:389) om elektronisk kommunikation – LEK. Den bedömningen påverkar inte skyldigheter som kan åligga sökanden enligt andra bestämmelser, exempelvis säkerhetsskyddslagen (2018:585) samt reglerna i 6 kap. LEK och PTS föreskrifter (2015:2) om krav på driftsäkerhet. En sökande som följer reglerna i dessa författningar bör dock ha goda förutsättningar att kunna ge in en ansökan som beaktar de styrande principerna och kriterier för bedömning av aktörer i bilaga B2.

Sökanden ska i de dokument som ges in till PTS markera vilka uppgifter som enligt sökandens bedömning är säkerhetsskyddsklassificerade, samt vilken säkerhetskyddsklass uppgifterna tillhör. Sökanden ska även ange vilka uppgifter som omfattas av sekretess enligt offentlighet- och sekretesslagen (2009:400).

Om PTS beslutar att en sökandes radioanvändning enligt ansökan kan antas komma att orsaka skada för Sveriges säkerhet kommer PTS att avslå ansökan om att få delta i auktionen.

I detta skede går det inte att bedöma huruvida det skulle kunna finnas skäl att förena en viss sökandes tillstånd med särskilda tillståndsvillkor i fråga om krav som är av betydelse för Sveriges säkerhet enligt 3 kap. 11 § första stycket 10 LEK, och hur sådana villkor kan utformas. Om det visar sig att det råder särskilda förhållanden för en enskild tillståndshavare skulle det kunna motivera införandet av särskilda villkor för den tillståndshavaren, för att säkerställa att vissa åtgärder vidtas. PTS inriktning är dock att samma tillståndsvillkor som huvudregel bör gälla för alla tillståndshavare.

Förtydliganden till bilaga B1 till Allmän inbjudan del 1

Fråga 1 i bilaga B1: Tillstånden i sig ställer inte krav på att vissa tjänster ska tillhandahållas i aktuella frekvensband. Det är upp till sökanden att ange vilka funktioner som är grundläggande från säkerhetssynpunkt. En rimlig utgångspunkt är att kritiska tjänster kan vara datakommunikation, röstsamtal och meddelandetjänster, om dessa tjänster tillhandahålls slutkunder, dvs. abonnent och användare. Tjänster utöver detta behöver inte nödvändigtvis utgöra en del av den kritiska infrastrukturen. Även drift- och underhållsnät som styr tillgängligheten kan anses vara kritisk infrastruktur. Bedömningen av vad som påverkar Sveriges säkerhet kan komma att förändras över tid beroende på hur teknik och tjänster m.m. utvecklas. Eventuella övriga tjänster som behövs för att tillhandahålla centrala funktioner ska också presenteras.

Fråga 3 i bilaga B1: Syftet med fråga 3 är att få information om vem som har inflytande och i praktiken styr och påverkar ett sökande företag. Ett börsnoterat företag kan ange att det är börsnoterat samt vilka de största ägarna är vid ansökningstillfället. De ca 10 största ägarna kan redovisas.

Fråga 5 i bilaga B1: Beskrivningen ska avse den centrala systemarkitekturen. Även systemarkitektur för transportnät kan vara nödvändigt att beskriva. Beskrivningen av nätelement kan vara övergripande, genom en nätskiss. Det krävs inte beskrivning på komponentnivå, t.ex. av antal servrar m.m. Om en specifik standard används går det bra att hänvisa till den. Innehållet i standarder behöver inte kopieras in i dokumenten.

Det bör anges hur den geografiska utbyggnaden ska ske. Geografiska platsangivelser behöver inte vara mer exakta än namn på ort.

Om artificiell intelligens – AI – ska användas för nätets drift bör det anges hur och vem som kontrollerar det och beskriva hur användningen av AI beaktar de styrande principerna enligt bilaga B2.

Det är huvudsakligen nätets arkitektur och struktur vid driftsättningen som ska redovisas. Om en sökande vet redan vid ansökan att man vid driftsättningen avser att använda sig av befintlig infrastruktur, exempelvis ett befintligt corenät, för att senare byta till ett 5G-corenät så ska det anges, och när bytet kan tänkas ske, i ansökan. Även andra förutsedda övergripande förändringar bör anges.

Förtydliganden till bilaga B2 till Allmän inbjudan del 1

Allmänt om dokumentet

Med ”nätets övergripande funktionalitet” avses övergripande funktioner i radioaccess-, core-, transmissions-, drift och underhållsnät som krävs för nätet och tjänster till slutanvändare. Funktionaliteten behöver inte beskrivas i exakt detalj med antal servrar m.m. Det som avses är hur nätet övergripande är byggt. Det går bra att referera till en standard om sådan används. Om sökanden t.ex. planerar att använda AI är det viktigt att beskriva hur funktionaliteten planeras och ska styras. ”Centrala funktioner” är på en övergripande nivå det som krävs för att tillhandahålla kommunikationstjänster.

Med begreppet ”av operatören tillhandahållna kommunikationstjänster till slutanvändare” avses mobila tal-, data- och meddelandetjänster över 4G och 5G till slutkunder. Observera att ”användare” kan innefatta fler än ”abonnenter”, t.ex. användare av tjänster som tillhandahålls i företagsabonnemang.

Med begreppet ”regulatoriska tjänster” avses t.ex. krav på tillhandahållande av nödsamtalstjänsten 112, men även andra tjänster som en operatör enligt LEK är skyldig att tillhandahålla.

Samrådsmyndigheterna ser att beaktandet av de styrande principerna enligt bilaga B2 är en garanti för Sveriges säkerhet. En grundtanke med principerna är att operatörer ska kunna använda principerna som grund för att bygga säkra nät och sedan kunna förvalta dem med hänsyn till Sveriges säkerhet. Om operatören beaktar och uppfyller de styrande principerna finns det förutsättningar att också kunna tillhandahålla tjänster till kunder som bedriver säkerhetskänslig verksamhet. Beaktas inte principerna kan radioanvändningen antas komma att orsaka skada för Sveriges säkerhet. Samrådsmyndigheterna kommer att göra en samlad bedömning utifrån det som anges i ansökan. Även icke-tekniska sårbarheter bedöms. Här avses t.ex. leverantörer och underleverantörer där samrådsmyndigheterna har kännedom om risker, bl.a. exponering för annan stats rättsordning kan beaktas.

Tillståndsvillkoret om Sveriges säkerhet kommer att gälla under hela tillståndets giltighetstid. PTS har möjlighet att utöva tillsyn över att tillståndsvillkoret uppfylls.

Styrande principer

1. Ska fungera även om anslutningar till utlandet bryts

Om den sökande har nätelement utanför riket ska nätet fungera även om förbindelserna till utlandet bryts. Detta är även en fråga om tillgänglighet eftersom den sökande ska kunna driva nätet även om gränserna stängs. Det gäller även i förhållande till våra nordiska grannländer. Principen är att nätet ska fungera självständigt utan koppling till utlandet. Något krav på att all utrustning undantagslöst måste placeras inom Sveriges gränser gäller dock inte. Om en sökande har lösningar med kopplingar till andra länder är det viktigt att i ansökan förklara de exponeringar som kan uppstå och hur sökanden agerar för att ta hand om dessa exponeringar. Sökanden ska kunna visa att sådana lösningar inte medför någon risk för skada för Sveriges säkerhet.

Operatörerna ska ha en tydlig planering för hur nätet ska fungera om störningar i förhållande till produkter och leverantörer uppstår samt att säkerhetsincidenter kan hanteras från Sverige och att system- och användardata lagras i Sverige.

Det som avses är de centrala funktionerna i nätet. Det är de tjänster som tillhandahålls av den sökande som avses, inte kommunikationstjänster som levereras av annan (t.ex. Facebook).

Med ”systemdata” avses metadata (konfiguration, parametrar m.m.) som är direkt hänförlig till den centrala funktionen och därmed har påverkan på Sveriges säkerhet. Med ”användardata” avses trafikuppgifter, lokaliserings- och abonnentdata.

2. Ska tillhandahålla funktioner som medger att förbindelser till och från utlandet enkelt, snabbt och selektivt kan brytas

Det som avses är snabba åtgärder för att t.ex. stoppa pågående cyberangrepp från utlandet.

3. Ska tillhandahålla hög tillgänglighet och sekretess

Här avses dels funktioner som identifieras i en säkerhetsskyddsanalys, men det kan även vara annat. Funktioner för att t.ex. skapa tillgänglighet i näten ska skapas så att sårbarheter inte uppstår. Här har beaktats en utveckling där tjänster flyttas längre ut i nätet, men syftet med principerna ska vara detsamma. Om 5G-utvecklingen kan generellt sägas att den kan öppna nya sårbarheter som inte kan förutses idag. Det kan därför bli aktuellt med ändringar i nätarkitekturen över tid.

Med tillgänglighet avses åtkomstkontroll men även tillgänglighet i nätet, att tjänster fungerar.

Ordet ”sekretess” har inte samma innebörd som ”konfidentialitet” i 6 kap. LEK, men PTS föreskrifter om skyddsåtgärder för behandlade uppgifter kan vara ett stöd. För att beakta kravet på sekretess ska näten byggas så att ingen annan kommer åt och kan styra dem.

För virtualiserade noder för centrala funktioner ska nodernas beroende till själva virtualiseringsplattformen beskrivas. Här avses hela virtualiseringsinfrastrukturen, från hårdvara till mjukvara.

5. Ska utformas så att otillåten styrning eller manipulering förhindras

Ordvalet ”förhindra” är starkare än ”förebygga” eller ”effektivt motverka” med hänsyn till att det rör Sveriges säkerhet och riskerna inte kan accepteras i något fall. Sökandena bör beskriva vad som görs för att i största möjliga utsträckning förhindra risker och sårbarheter. En operatör kan anses ha gjort vad man kunnat om en sårbarhet som upptäcks vid t.ex. stresstester åtgärdas omedelbart.

Administration av näten, trafikskydd men även drift- och underhållsnät ska vara separerade.

6. Ska utformas så att styrning eller manipulering från utlandet förhindras

Det är viktigt att sökanden inte bygger nätet så att det är möjligt att styra från utlandet. Funktion i näten ska inte förloras om förbindelsen till utlandet bryts.

7. Ska utformas så att otillåten kartläggning av tjänster, kapacitet, lokalisering eller användare förhindras

Punkten handlar om information om nätet och dess användare. Med begreppet ”otillåten kartläggning av tjänster” avses tjänster som operatören tillhandahåller till användare, tillgång till centrala funktioner gör att användningen går att kartlägga. Det är inte själva erbjudandet att tillhandahålla en viss tjänst som anses skyddsvärt utan vem som är användare och abonnerar på en viss tjänst.

Med ”otillåten kartläggning av kapacitet” avses kapacitet som kunder abonnerar på. Uppgiften kan vara skyddsvärd då det går att dra slutsatser vad abonnemanget kan användas till. Sådan information ska inte vara tillgänglig för en antagonist. Information om tjänster och kapacitet kan särskilt i aggregerad form utgöra en säkerhetsrisk, och detta måste beaktas redan vid planeringen.

Med ”otillåten kartläggning av lokalisering” avses både slutkunders lokaliseringsuppgifter och uppgifter om olika nätelements lokalisering.

Med ”otillåten kartläggning av användare” avses trafikuppgifter hänförliga till mobila tal-, data- och meddelandetjänster, lokaliseringsuppgifter samt innehåll i

kommunikation. Det är inte nödvändigtvis samma definition som i fråga om lagring av trafikdata för brottsbekämpande ändamål.

Virtualiseringslösningar ska beskrivas i den utsträckning de finns på plats när nätet driftsätts. Vid senare ändringar i näten får tillståndshavarna informera myndigheterna när det blir aktuellt.

8. Ska utformas så att otillåtna angrepp (såsom elektroniska attacker) förebyggs och där så inte är möjligt ska dessa upptäckas och förhindras

Principen har en vidare innebörd i förhållande till övriga principer. Det kan t.ex. vara så att det finns andra skyddsåtgärder som kan vidtas, som fysiskt skydd och skydd mot oavsiktlig påverkan. Det är önskvärt att även sådana andra skyddsåtgärder redovisas.

10. Ska ha spårbarhet för funktioner som kan påverka sekretess, tillgänglighet, insyn eller kontroll

Med ”aktiviteter från tredje part” avses även support från tillverkare.

11. Ska utformas så att utrustning där det finns risk för otillåten insyn, kontroll eller manipulation genom fysisk åtkomst ska förläggas på svenskt territorium så att svensk lagstiftning blir tillämplig

När det gäller trafikuppgifter som lagras för brottsbekämpande ändamål får sådana uppgifter lagras utanför Sverige, så länge det sker inom EU. (Se prop. 2018/19:86.) I princip finns ett krav på att ”system- och användardata ska lagras i Sverige” för uppgifter som rör Sveriges säkerhet. All information som lagras för brottsbekämpande ändamål rör inte nödvändigtvis Sveriges säkerhet, men uppgifter som kan användas för att skada Sverige ska lagras i Sverige. I många fall kommer det dock att vara samma uppgifter. Om en operatör väljer att lagra data i ett annat land måste den visa att lagringen inte kan skada Sveriges säkerhet. Om operatören kan beskriva lösningar som lagrar data i ett annat land och ändå följer principerna och skyddar Sveriges säkerhet så skulle det kunna godkännas.

Säkerhetspolisen anser att det är viktigt att uppgifter som myndigheten behöver för att utreda brott mot Sveriges säkerhet, inklusive lagrade trafik- och användaruppgifter, finns tillgängliga även om förbindelser till utlandet bryts.

12. Operatören ska kontinuerligt lämna information till utsedda mottagare hos sektorsansvarig myndighet rörande åtgärder, som vidtas i kommunikationsnäten, vilka kan påverka sekretess, robusthet, tillgänglighet, insyn eller kontroll

Begreppet ”kommunikationsnäten” har samma betydelse som tidigare nämnda ”centrala funktioner”.

13. Operatören ska lämna information i så god tid att sektorsansvarig myndighet kan avgöra vilka risker sådana åtgärder som vidtas i kommunikationsnäten innebär och om åtgärder behövs

14. Operatören ska aktivt underlätta sektorsansvarig myndighets insyn och kontroll

Punkterna 12–14 syftar till att operatörer som beviljats tillstånd ska informera om betydande ändringar i näten. Det kan t.ex. röra sig om nya automatiseringslösningar eller förändringar vad gäller tredjepartsleverantörer, där säkerhetsmyndigheterna kan ha värdefull information om sådant som kan utgöra betydande risker. Även en förändring som är liten för en operatör kan få stora konsekvenser.

Operatören måste själv bedöma om sådana förändringar sker och informera om dem. Lagstiftningen innehåller inte något obligatoriskt godkännande på förhand av förändringar i näten men det som anges i dessa punkter ska kontinuerligt beaktas. En operatör är inte förhindrad att vidta omedelbara åtgärder som är nödvändiga t.ex. med anledning av en säkerhetsincident.

När det gäller planerade åtgärder som kan få större betydelse, t.ex. upphandling av nya leverantörer eller anlitande av tredje part för nätdrift, är det värdefullt om PTS och samrådsmyndigheterna bereds tillfälle att ge stöd och informera om eventuella risker innan ändringen genomförs. Samrådsmyndigheterna kan ha värdefull information om sådant som kan utgöra betydande risker.

Post- och telestyrelsen kommer i egenskap av tillstånds- och tillsynsmyndighet att kontrollera och följa upp operatörers information om åtgärder och ändringar. PTS kan i detta sammanhang också komma att begära in specificerade uppgifter från operatörer och ange med vilken regelbundenhet dessa ska lämna information.

Det är viktigt att påpeka att information som en operatör lämnar till PTS enligt dessa punkter inte påverkar eventuell skyldighet att även lämna uppgifter enligt annan lagstiftning, t.ex. enligt säkerhetsskyddslagen (2018:585) eller lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.

15. Operatören ska ta fram, implementera, drifta samt underhålla adekvata säkerhetsskyddsåtgärder

16. Operatören ska se till att personal, som får tillgång till uppgifter vilka kan påverka konfidentialitet, riktighet, robusthet och tillgänglighet, är godkänd och utbildad i säkerhetsskydd samt medvetna om uppgifternas sekretess

Principerna 12–16 innehåller krav på åtgärder som, utöver principerna 1–11, även kan röra skydd i vidare bemärkelse. Med drift och underhåll avses i detta sammanhang även kontinuerlig kompetensutveckling, att se till att det finns rätt bemanning m.m.

Kraven i de tidigare principerna hänger kvar i principerna 12–16 genom sättet tillståndshavare förutsätts arbeta med frågorna.

Kraven i punkterna 15 och 16 kan gå utöver kraven enligt säkerhetsskyddslagen. Det kan t.ex. handla om skyddsåtgärder för vitala platser med vital utrustning samt övrigt verksamhetsskydd. Punkten 16 avser centrala funktioner, inklusive vitala tjänster. Med robusthet avses stabilitet i nätet, motståndskraft mot driftstörningar, redundans m.m. för att undvika systemkollaps.

Övrigt

Hänvisningen till den s.k. EU Toolbox (EU-verktygslåda för 5G-säkerhet[1]) är enbart i upplysningssyfte. Verktygslådan tar sikte på EU:s inre säkerhet medan de styrande principerna tar sikte på Sveriges säkerhet. Vissa av principerna i verktygslådan kan dock vara användbara även på nationell nivå. De styrande principerna utgår från vad som krävs för Sveriges säkerhet, därför finns inte samma gradering som i verktygslådan.

[1] NIS Cooperation Group. CG Publication 01/2020. Cybersecurity of 5G networks EU Toolbox of risk mitigating measures