Kammarkollegiet

Bilaga 3
Säkerhet

Innehåll

1 Allmänt

2 Säkerhet

2.1 Atea

Atea har i detta anbud samlat både egna och underleverantörers tjänster för att skapa en bra möjlighet till funktionalitet för avropande verksamheter. En viktig del i detta är att tjänsterna håller en säkerhetsnivå som minst motsvarar de krav som avropande verksamhet har.

Säkerhetskraven kan delas in i administrativa säkerhetskrav som bl.a. omfattar policy, regelverk, rutiner, revisioner och uppföljning samt tekniska säkerhetskrav inklusive fysisk säkerhet och data- och kommunikationssäkerhet. Utöver ställda krav i denna bilaga kan det även finnas specifika tekniska säkerhetskrav kopplade till enskilda efterfrågade tjänster och funktioner.

Informationssäkerhet och de risker myndigheter utsätts för är frågor som har stor betydelse. Atea jobbar sedan länge med säkerhetsfrågor runt IT-infrastruktur och levererar tjänster till många kunder inom offentlig och privat verksamhet. Vi har därför en mycket god kunskap om behov i kundernas verksamhet och hur vi som leverantör kan integrera säkerhetsarbetet i tjänsterna med kundens verksamhet.

2.2 Telenor

Telenor bygger tjänsterna utifrån de krav som ställs av avropande specifikt baserat på deras behov. Att kunna kommunicera säkert och utan avbrott kan lösas på olika sätt t.ex. med redundanta lösningar. Alla priser för detta finns presenterat i bilagd prislista och svaren för möjligheter ges i respektive del.

En hög säkerhet på Telenor är en förutsättning för att företaget skall kunna leverera service och tjänster av hög kvalitet och som möter följande krav;

- att information om våra kunder inte hamnar i obehörigas händer
- minimala störningar i våra nät och system som kan orsaka våra kunder skada eller besvär
- skydda företagets tillgångar
- skydda våra medarbetares mentala och fysiska hälsa
- följa lagar, förordningar och övriga krav

Detta görs genom införande och vidmakthållande av adekvat skydd inom de olika säkerhetsområdena:

- fysisk säkerhet
- informationssäkerhet

- personsäkerhet

Interna regler och riktlinjer för detta är samlat i ett ramverk för respektive område.

2.3 IP Only

IP-Only arbetar aktivt med säkerhetsfrågor och riskbedömningar för både elektronisk och fysisk säkerhet för att minimera risker i vår verksamhet och hålla hög kvalitet i vår leverans av tjänster.

IP-Only har ett generellt regelverk för säkerhet och policyfrågor. Processer och rutiner för verksamhetsspecifika säkerhetsregler är styrda ned på organisatorisk nivå där varje avdelningschef har ansvar för att regler och rutiner för säkerhet följs och att fel rapporteras till berörd avdelning på IP-Only.

En speciell grupp inom företaget har till uppgift att kontinuerligt följa upp och revidera säkerhetsrutinerna och reglerna utifrån analyser kring hot och sårbarhet. Ytterst ansvarig för säkerhetsreglerna och policys är VD och ledningsgruppen.

2.4 Banverket ICT

För Banverket ICT är säkerhet en viktig del för att säkra ICT-tjänsternas tillgänglighet, tillförlitlighet och för att skydda information. Det uppnår vi genom att vi har ett arbetssätt baserat på ITIL-proceserna och gällande Banverkets föreskrifter samt har ett högt säkerhetsmedvetande i organisationen.

2.5 Administrativa säkerhetskrav

2.5.1 Basnivå för informationssäkerhet

Atea arbetar sedan flera år tillbaka med ramverket Basnivå för Informationssäkerhet, BITS och har hjälpt ett flertal kunder att ta fram regelverk och policys baserade på BITS. Inom det administrativa området kan det också handla om återställningsplaner, organisation, kompetensförstärkning och kontinuitetsplanering.

Våra underleverantörer hanterar BITS enligt följande:

2.5.1.1 Telenor

Telenors ramverk för Informationssäkerhet är uppbyggt i enlighet med standarden ISO/IEC 27002:2005 Riktlinjer för styrning av informationssäkerhet och ISO/IEC 27001:2006 Ledningssystem för informationssystem – Krav.
Tjänsteutveckling och interna processer är i allt väsentligt i enlighet med denna standard vilket innebär att tjänsteproduktion och leveranser väl uppfyller grundkraven i Krigsberedskapsmyndighetens, KBM's BITS rekommendationer 2006:1.

Med kunskap om hur BITS hanteras i kundernas organisation och tjänster som stödjer dessa krav så kan Atea hjälpa våra kunder att följa de uppställda kraven.

2.5.1.2 IP Only

IP-Only följer rekommendationerna i BITS och tillämpar rutindokument och processer för verksamhetsstyrning, kontroll och kvalitetsuppfyllnad. Dessa rutiner och processer genomgår regelbunden testning, revision och förändras kontinuerligt t.ex. vid införande en ny arbetsrutin.

Säkerhetsinstruktioner och rutiner för drift är utformade för att lösa uppgifter på det mest effektiva och lämpliga sättet och följer generella och verksamhetsspecifika regler för att passa vår produktion och vår kontinuerliga leverans av tjänst dygnet runt årets alla dagar. Instruktionerna och rutinerna finns dokumenterade i företagets kvalitetshandbok. Syftet är att arbeta med metoder som på bästa sätt förenklar vår tjänsteleverans och tydligör spårbarheten i vårt arbete för kvalitetsuppföljning och vår reproducerbarhet i verksamheten. Våra rutin- och processdokument innefattar även beskrivningar för underleverantörer och inhyrda konsulter.

IP-onlys tjänsteleverans bygger på olika teknikplattformar. Dessa plattformar har olika tekniska nivåer. På varje nivå finns rutiner för skydd mot skadlig programkod på operativsystem och applikationer. Det hanteras inom IP-Only av avdelningarna Aktiva nät och IT. Dessa avdelningar utformar flera rutiner i samråd med leverantörer av utrustning (hård- och mjukvara) för att följa branschstandard vilket underlättar vårt arbete med felsökning, felavhjälpning, uppföljning uppgradering etc.

Näten underhålls kontinuerligt av IP-Only NOC (Network Operation Center), Aktiva nät och IT avdelningen. Konfiguration och konfigurationsändringar är lösenordklassade med olika behörighet beroende på organisatoriskt ansvar och tillhörighet. Lösenord hanteras med hög säkerhet och skyddas med autenticeringskontroll för rätt behörighet. Datamedia klassas beroende på krav av informationssäkerhet. Media lagras med högt skalskydd.

IP-Only driver egna datorhallar med högsta skyddsklass mot brand, naturkatastrofer och sabotage. I dessa före detta militära bergrum har IP-Only bevakade backupstationer för kunder och sin egna verksamhet. Datorhallarna är utrustade med

reservkraft i form av batterisystem och dieselgeneratorer om ett externt elavbrott skulle inträffa.

Informationshantering lyder under IP-Onlys policyregler som utgör ett regelverk för hur information får och kan utlämnas eller sändas. Dessa policys omfattar till exempel e-post, webbinformation, brandväggsloggar, krypteringsnycklar, lösenord, protokoll och telefonirutiner.

IP-Onlys NOC övervakar både nät, noder och datorhallar. Samtliga noder är kameraövervakade och styrs från vår NOC i Uppsala. In- och utsläpp till noder och hallar följer tydliga anvisningar och regler. Övervakningen sker dygnet runt årets alla dagar med egen personal. NOC personalen följer tydliga rutinbeskrivningar, följer upp och åtgärdar fel, analyserar loggar och rapporterar händelser. Loggar säkras alltid för att kunna användas som verifikat vid en eventuell senare juridisk process.

IP-Only har klassning för samtlig personal på verksamhetsnivå och organisatorisk nivå. Klassningen gäller för informationstillgång och åtkomst till system men även för tillträde till olika lokaler. Styrning av åtkomst hanteras dels på anställningsnivå men även av närmsta chef.

2.5.1.3 Banverket

Banverket ICT uppfyller alla ställda krav enligt BITS, se bifogade bilagor BVF004.1 och BVF004.2.

Vid avsteg från regelverket krävs dispens enligt befintlig rutin.

2.5.2 Uppföljning och kontroll – säkerhetsrevision

En viktig del av Ateas leverans är att tillse att avtalade säkerhetsnivåer upprätthålls. Atea erbjuder också säkerhetsrevison av erbjudna tjänster. Detta beskrivs för Atea och våra underleverantörer nedan:

2.5.2.1 Atea

Atea bedriver en kontinuerlig uppföljning och kontroll av sina tjänster och erbjuder även beställaren att genomföra säkerhetsrevision för att kontrollera att avtalade säkerhetsnivåer upprätthålls.

2.5.2.2 Telenor

Telenor bedriver ett kontinuerligt arbete med identifiering av operationella risker i verksamheten, dessa riskbedömningar görs på flera olika nivåer, allt från företagsövergripande via bedömningar av risker i de olika värdekedjorna till analyser av enskilda tjänsteproducerande plattformar och infrastruktur.

Telenor ställer sig positiv till att samverka med Atea i bedömningar kring risker för enskilda kunder och deras leveranser. För de kunder som önskar finns möjlighet att avtala om periodiska gemensamma forum för risker och säkerhet.

2.5.2.3 IP Only

IP-Only välkomnar kunden att i samråd med oss följa upp och kontrollera att avtalade säkerhetsnivåer upprätthålls.

2.5.2.4 Banverket ICT

Banverket ICT erbjuder beställaren uppföljning och kontroll efter kundens behov och önskemål. Avrop skall ske via e-post verva@banverket.se.

2.5.3 Säkerhets- och sårbarhetsanalyser

Leverantören skall ha rutiner för att göra egna respektive medverka vid Beställarens säkerhets- och sårbarhetsanalyser för berörda tjänster och funktioner. Exempelvis kan detta gälla vid större förändringar i tjänst samt om beställaren begär att säkerhets- och sårbarhetsanalyser skall genomföras.

2.5.3.1 Atea

Atea erbjuder flera former av säkerhets- och sårbarhetsanalyser som kan genomföras både internt på egna tjänster och funktioner samt erbjudas till kund. Analyserna genomförs i följande varianter:

Security Basic
En analys framtagen av Atea som omfattar en icke-påverkande testmetod för hela IT-miljön. Security Basic är baserad på ramverket BITS och ger en övergripande bild av hur en tjänst, funktion eller miljö lever upp till de säkerhetskrav som beskrivs i BITS. Vid behov kan sedan mera riktade analyser genomföras för specifika system.

Security Healthcheck
Security Healthcheck (SHC) är en teknisk säkerhetsanalys som är framtagen av Atea. I grundversionen är målet att upptäcka eventuella sårbarheter i befintliga system för att kunna åtgärda dem innan de utnyttjas på ett oönskat sätt. SHC finns också i en utökad version där genomförande konsult också försöker utnyttja de upptäckta sårbarheterna för att bättre beskriva de möjliga konsekvenserna. SHC kan omfatta hela eller endast valda delar av en IT-miljö.

Managed Security Service
Managed Security Service är en tjänst där Atea hjälper till med övervakning för att upptäcka intrångsförsök i realtid.

Webbtrafikanalys
Webbtrafikanalysen gör det möjligt att få en bild av hur företagets Internetanslutning utnyttjas. I analysen används en produkt som kan förhindra innehållsrelaterade hot från Internet.

2.5.3.2 Telenor

Telenor bedriver ett kontinuerligt arbete med identifiering av operationella risker i verksamheten, dessa riskbedömningar görs på flera olika nivåer, allt från företagsövergripande via bedömningar av risker i de olika värdekedjorna till analyser av enskilda tjänsteproducerande plattformar och infrastruktur.

Telenor ställer sig positiv till att medverka i bedömningar kring risker för enskilda kunder och deras leveranser. För de kunder som önskar finns möjlighet att avtala om periodiska gemensamma forum eller arbetsmöten med fokus på risker och säkerhet.

2.5.3.3 IP Only

På IP-Only sker regelbundet veckomöten med representanter från avdelningarna NOC, Aktiva Nät och IT. I de mötena avhandlas alltid säkerhetsfrågor och frågor som rör företagets sårbarhet. Vi kan vara behjälpliga för kunden att medverka vid kundens säkerhets- och sårbarhetsanalys av de tjänster kunden har från oss.

IP-Onlys säkerhetsanalys omfattar inventering av system och byggnader som är känsliga resurser för vår verksamhet och att identifiera bakomliggande hotbilder mot dessa känsliga resurser. Exempel på bakomliggande hotbilder kan vara vem, var och hur virus sprids mot oss, varifrån DDos attacker kommer, identifiering av hackers som sprider och planterar trojaner, maskar eller annan skadegörande programkod. Exempel på hot mot våra anläggningar kan vara sabotage eller allmän skadegörelse, brand eller yttre miljöpåverkan. Risker för de olika hoten bedöms liksom sannolikheten att hoten iscensätts.

I sårbarhetsanalysen sätter NOC, Aktiva Nät och IT gruppen de sårbara systemen och objekten i fokus och försöker identifiera vad som är skyddsvärt, vad som kan hota det skyddsvärda, vilka angreppspunkterna är och förmågan att stå emot olika former av påfrestning.

2.5.3.4 Banverket ICT

Leverantören skall ha rutiner för att göra egna respektive medverka vid Beställarens säkerhets- och sårbarhetsanalyser för berörda tjänster och funktioner. Exempelvis kan detta gälla vid större förändringar i tjänst samt om beställaren begär att säkerhets- och sårbarhetsanalyser skall genomföras.

Banverket ICT har lång erfarenhet av informationssäkerhet enligt föreskrift BVF004.2.

Banverket ICT erbjuder beställaren risk- och sårbarhetsanalyser efter kundens behov och önskemål. Avrop skall ske via e-post verva@banverket.se.

2.5.4 Styrning & rutiner motsvarande SS-ISO/IEC 27002:2005

2.5.4.1 Atea

Atea levererar både egenproducerade tjänster och tjänster ifrån underleverantörer. För att säkerställa informationssäkerheten i dessa tjänster så tillämpas styrning med policyer, processer och rutiner.

Informationssäkerhet är en viktig del i framtagning och leverans av såväl egna som tjänster via underleverantörer. Atea har för sina tjänster en tydlig struktur med tjänsteägare, producent (intern eller extern), leveransansvarig och serviceledare.

Generellt inom Atea så finns också en genomgripande säkerhetspolicy som en del av vårt kvalitetsarbete.

2.5.4.2 Telenor

Telenors modell för arbete med risker och säkerhet baseras på en centraliserad styrning och kontroll från företagsledningens sida, detta arbete leds av en centraliserad Risk- och Säkerhetsavdelning, och ett decentraliserat operativt ansvar i de olika affärsområdena och avdelningarna.

Modellens ledord är ansvarprincipen, likhetsprincipen och närhetsprincipen.

Telenor har en lång erfarenhet som teleoperatör och därmed även lång erfarenhet och god kunskap om de specifika krav som ställs vid samarbete med stora företag, myndigheter, landsting och kommuner.

2.5.4.3 IP Only

IP-Only tillämpar policyer, processer, rutiner och strukturer avseende informationssäkerhet motsvarande SS-ISO/IEC 27002:2005 för våra erbjuda tjänster och funktioner.

Informationsskydd regleras övergripande i företagets generella policyregler. IP-Onlys policyregler omfattar skydd för elektronisk information och skalskydd för byggnader och installerad utrustning. Policyregler finns på alla organisatoriska nivåer i bolaget. IP-Only har föreskrifter för hur både pappers- och elektroniska dokument ska förvaras och arkiveras. Varje avdelningschef har ansvar för att regelverket följs kring företagets säkerhetspolicy i sin respektive verksamhet.

Elektronisk informationstillgång hanteras på organisatorisk nivå genom att varje anställd direktautentiseras mot AD (active directory) 801.1X vid anslutning mot IP-Onlys interna LAN och då tilldelas sina åtkomster. Gäster eller besökare till IP-Only kan ansluta sig till IP-Onlys nät men tillåts då bara uppkoppling till Internet (surf).

IP-Onlys nätverk är skyddat med brandvägg och har IDS och IPS aktiverat. Loggfiler analyseras dagligen med rapportering och loggarna arkiveras om något okänt har inträffat. Personal från NOC, Aktiva Nät och IT avdelningarna träffas veckovis och analyserar elektroniska intrångsförsök, ser över det elektroniska skyddet och diskuterar säkerhetsåtgärder. Vid behov utfärdar denna grupp nya åtgärder och rutiner för att stärka företagets elektroniska försvar mot externa hot eller interna svagheter och risker. Vid större förändringar eller förslag som påverkar processer mot andra avdelningar kontaktas alltid ledningsgruppen för godkännande.

Servrar och data backas upp regelbundet efter ett schema till en disk/bandrobot i ett av IP-Only ägt bergrum med extra högt skalskydd (datahall). All noder i vårt nät är skyddsklassade och endast ett fåtal personer har åtkomstmöjligheter till den aktiva utrustningen som hanterar trafiken till vilken det krävs speciella lösenord och koder. Även hanteringen av lösenord och koder omfattas med regler och skydd.

Tillgång till IP-Onlys datahallar kräver föranmälan till vår NOC. Datahallarna (colocationhallarna) är bemannade dagtid. För övrig tid har IP-Only avtal med vaktbolag och egen jourpersonal som kan rycka ut vid behov. Inpasseringskontroll av besökare till datahallar och noder sker på plats med kamera. Besökarna ska alltid vara föranmälda till vår NOC för att bli insläppta. Samtliga besök loggas av NOC och bekräftas med en inpasseringskod. IP-Only har rätt att neka tillträde om behörighetskontrollen inte godkänns. Alla noder är omgärdade med stängsel, utrustade med kodlås, har yttre fjärrstyrd kamera, intrångslarm, brandskydd med inert gas och id-kamera i passersluss. NOC i Uppsala ansvarar för all övervakning och inpasseringskontroll i datahallar och i noder.

Larm som inkommer till IP-Only NOC arkiveras alltid med tid- och datumstämpel för att kunna utgöra verifikat vid en eventuell senare juridisk process. Larmrapporter informeras alltid till ledningsgruppen och VD.

Risk management hanteras av NOC i samråd med avdelningarna Aktiva Nät och IT. Juridiska föreskrifter utfärdas av företagets legala avdelning. Processer och rutiner är dokumenterade på intranätet och återfinns i företagets kvalitetshandbok.
Ytterst ansvarig för informationssäkerhet på IP-Only är ledningsgruppen och VD. Ansvar delegeras ned i organisationen på olika nivåer beroende på klassning av säkerhet och organisatorisk tillhörighet. Varje avdelningschef har ansvar för att sin verksamhet följer företagets föreskrifter och rutiner kring företagets säkerhetspolicy och utfärdar rätt rutiner för att möta de krav och ansvar som ställs i sin verksamhet.

I risk management begreppet ansvarar NOC, Aktiva Nät och IT avdelningarna också för sårbarhetsanalys. I risk- och sårbarhetsanalysen bedöms sannolikheten för att

oönskade händelser ska inträffa, såsom attacker, virus, trojaner, maskar men även fysiska attacker och sabotage mot företagets byggnader, noder och nät och vilka konsekvenser det får för IP-Only. Sannolikhets- och konsekvensbedömningen ligger därför till grund för de riskreducerande åtgärder som NOC, Aktiva Nät och IT gruppen anser behöver vidtas. Dessa åtgärder värderas utifrån ett kostnads- och nyttoresonemang men även ur en kvalitativ ansats då enbart en ekonomisk bedömning kan vara svår att genomföra på ett stort tekniskt system som hela IP-Onlys tjänsteplattform. I risk- och sårbarhetsanalysen sätter gruppen de sårbara systemen och objekten i fokus och försöker identifiera vad som är skyddsvärt, vad som kan hota det skyddsvärda, vilka angreppspunkterna är, och förmågan att stå emot olika former av påfrestning.

Informationen kring företagets säkerhetsarbete uppdaterar kontinuerligt och de anställda får information och hänvisning om uppdateringarna på informationsmöten, avdelningsmöten och på intranätet.

2.5.4.4 Banverket ICT

XBanverket ICT följer, enligt regler och rutiner i Banverkets Informationssäkerhets-föreskrift BVF004.1 och BVF004.2, kraven enligt BITS och ISO17799. Förvaltningsarbete har pågått under året och offentlig version motsvarande ISO 27002 kommer att finnas tillgänglig före januari 2009.

2.5.5 Rutiner för drift och övervakning

Anbudsgivaren **skall** vid avrop presentera rutiner för drift och övervakning till beställaren.

Atea kommer i samband med avrop att tillsammans med beställaren presentera och kundanpassa rutiner för drift och övervakning. Dessa rutiner omfattar såväl både tekniska rutiner som kontaktvägar och omfattar både kund, Atea och eventuella underleverantörer.

2.6 Allmänna tekniska säkerhetskrav

2.6.1 Fysisk infrastruktur

Leverantören skall till Beställaren tydligt kunna redogöra för den nationella fysiska infrastruktur och det egna kommunikationsnät som tjänsten är baserad på med fysisk placering av relevanta noder och nationella framföringsvägar för fysiskt media.

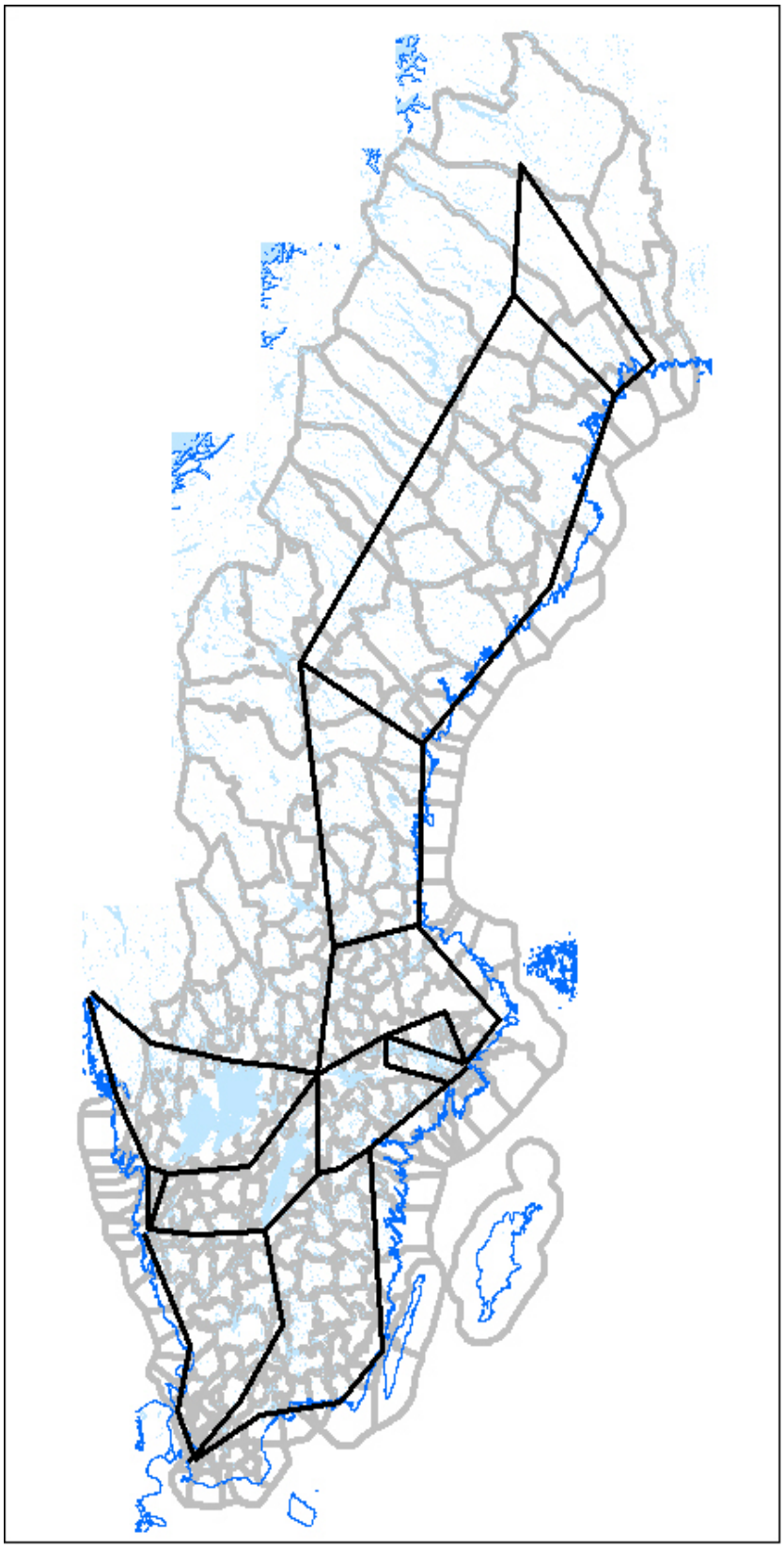
Fysisk infrastruktur tillhandahålls i detta anbud av Ateas underleverantörer. Infrastrukturen är olika för de olika underleverantörerna och redovisas nedan:

2.6.1.1 Telenor

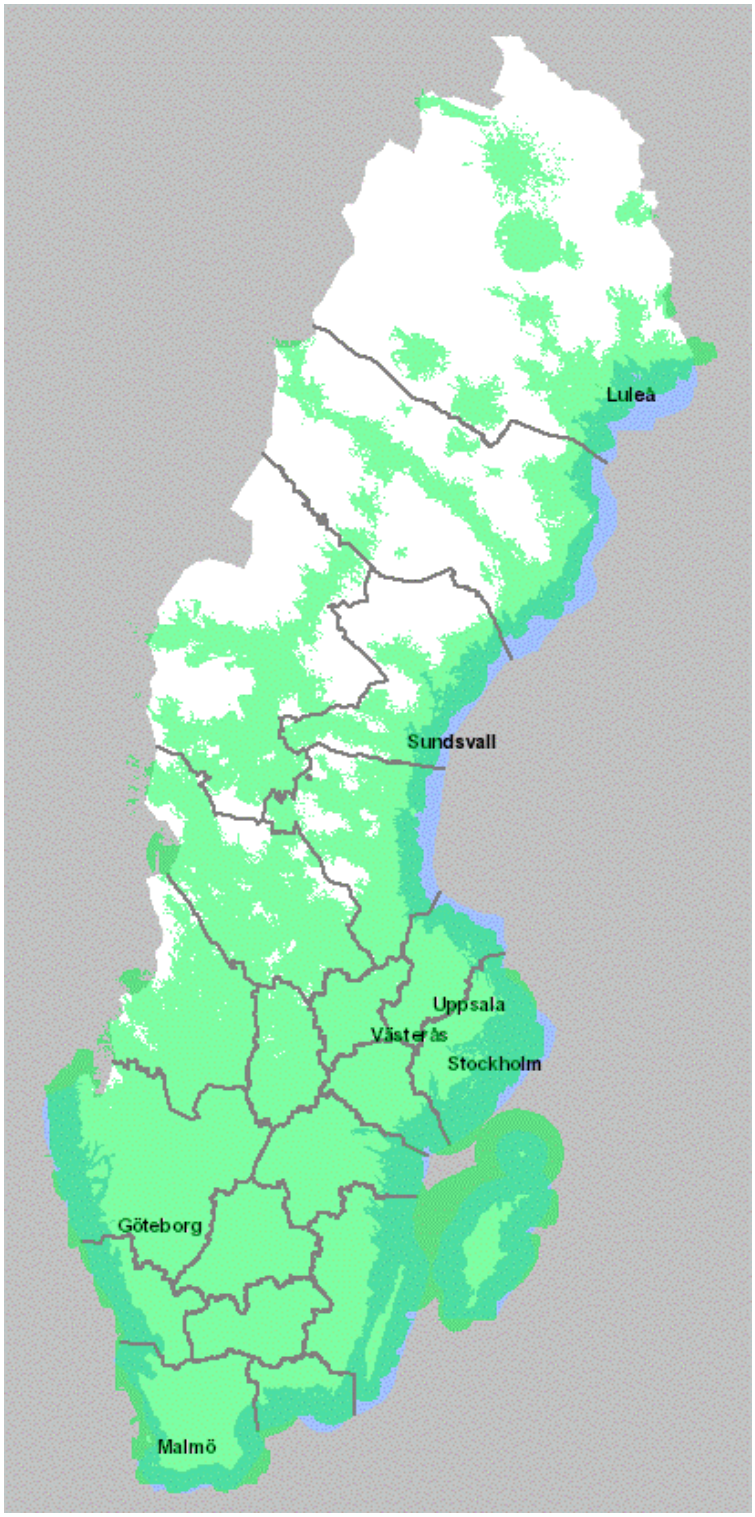
Telenors leverans av tjänster baseras i huvudsak på egen infrastruktur och i de fall det inte är möjligt på hyrd, men av Telenor kontrollerade förbindelser.

Infrastrukturen för leverans av Telenors tjänster är fördelad på ett stort antal olika anläggningar runt om i landet. Allt från fullskaliga datahallar/växelhallar i byggnader eller bergrum till enskilda containrar intill en mobilmast. Det totala säkerhetsskyddet för dessa olika typer av anläggningar varierar beroende på anläggningens storlek och funktion.

Figur 1 nedan beskriver Telenors nationella transmissionsnät och centrala huvudnoder.
Figur 2 nedan beskriver täckning för Telenor Sveriges mobilnät med syfte att beskriva mängden basstationer och dess placering. Centrala noder för mobila tjänster, är för att uppnå god redundans och tillgänglighet, fördelade på ett flertal platser i landet med tyngdpunkt på Karlskrona, Stockholm, Göteborg och Malmö.



Figur 1 **Telenors transmissionsnät**

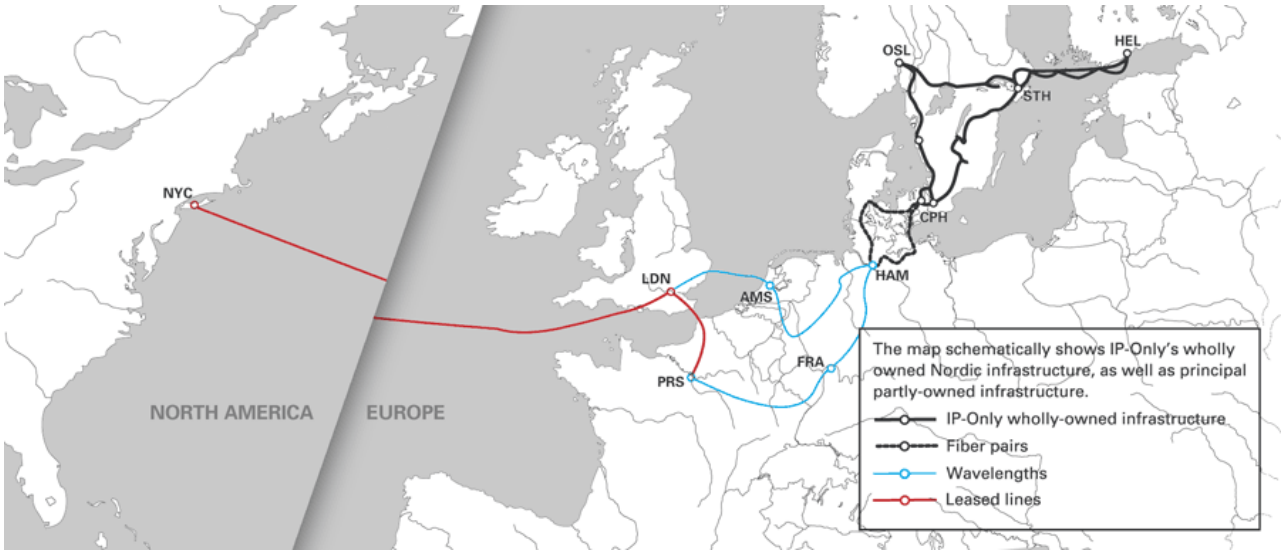


Figur 2 Täckningskarta mobilnät

2.6.1.2 IP Only

IP-Only äger ett eget, oberoende fiberstamnät som förbinder Stockholm-Oslo-Göteborg-Malmö-Stockholm. Stamnätet är i sin tur anslutet till ett stort antal lokala och regionala nät längs vägen. Utöver fiberringen äger IP-Only även sjökabelförbindelser till Köpenhamn och Helsingfors samt har del i nät i Köpenhamn och delar av Europa samt vidare till New York. IP-Only har egna datorhallar för colocationtjänster i Norden samt på södra Manhattan. I nätet levereras IP- och Ethernettjänster, våglängder och svart fiber. IP-Only kontrollerar den egna infrastrukturen från grunden - från fiber och rör, via egna fastigheter för teknikutrustning, till transmissionssystem och IP-backbone.

Om Beställaren önskar få information kring exakt placering av IP-Onlys noder kan detta ges till Beställaren.



Det optiska fiberstamnätet

IP-Onlys fiberstamnät består i grunden av två optorör. Idag utnyttjas ett av rören för en optofiberkabel innehållande 96 fiber. Kabeln är en så kallad kompositkabel och fibern i kabeln är av fabrikatet Corning, där ca en fjärdedel är av typen Leaf. Nätet är utrustat med flera separata DWDM-transmissionssystem med en total möjlig installerad kapacitet om 1,6 Tbit/s (1 600 Gbit/s). Längs fibersträckorna har IP-Only

egna byggnader utplacerade med olika utrymmen för kundutrustning samt utrustning för förstärkning och regenerering av de optiska signalerna.

Optorör
De två helägda optorören är av lågfriktionstyp, vilket gör det enkelt att lägga ytterligare fiberkablar. Med jämna mellanrum finns fiberbrunnar för skarvning och slingning av fiber. Vid varje brunn samt i ändpunkter slingas kabeln för att möjliggöra senare skarvnings- och inkopplingsarbeten (ca 20 m i brunnar och 10 m vid ändpunkter).

Fiber
Fibern i optokabeln är av typen singlemode och IP-Only har två olika varianter med olika karaktäristik. Båda varianterna är avsedda för våglängdsmultiplexering:
− 72 st fiber av typen G.652
− 24 st fiber av typen G.655 (Leaf)
All fiber är uppmätt och provad för att verifiera att ställda krav på transmissionsegenskaper i nätet är uppfyllda, både vad gäller själva optokabeln samt genomförda skarvar och kontakteringar. Utförd OTDR-mätning verifierar att fibersträckningen är felfri. Sträckdämpningsmätningen (dB-mätning) ger det mest noggranna värdet på förbindelsens totala dämpning från ändpunkt till ändpunkt. All mätdata finns samlad och dokumenterad i IP-Onlys dokumentationssystem. Generellt dämpas singlemodefiber av standardtypen G.652 ca 0.2 dB/km för en våglängd på 1550 nm. Redundans på fibernivå erhålls genom att det finns alternativa fibervägar i fiberstamnätet mellan två punkter. Skulle en fiber skadas kan trafiken gå den andra vägen.

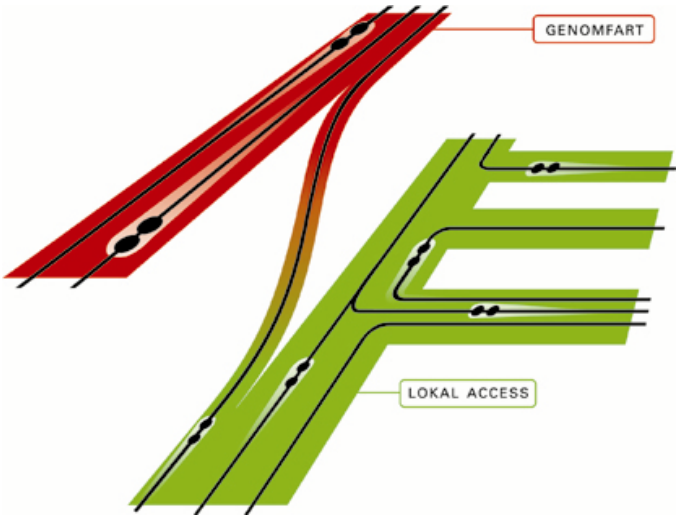
Egenägda teknikhus för transmissionsutrustning
Utmed fibersträckningen finns idag 21 förstärkarstationer och 7 regeneratorstationer, varav 4 finns i de datorhallar IP-Only har i Stockholm, Oslo, Göteborg och Malmö. Förstärkar- och regeneratorstationerna är lokaliserade var åttionde kilometer längs fibernätet. Förstärkning och regenerering av de optiska signalerna är nödvändigt eftersom signalstyrkan dämpas med avståndet. Byggnaderna är anpassade för att hysa avancerad transmissionsutrustning och är byggda i enlighet med följande riktlinjer och krav:
− Möjlighet att erbjuda eget utrymme till andra operatörer med separat ingång frånskild IP-Onlys transmissionsutrustning.
− Inbrottsskydd
− Inpasseringssystem
− Övervakning med larm till centralt system (fukt, inbrott, brand, rök, kraft)
− Kyl och klimatanläggning (reglerad temperatur 21 grader +/- 2 grader)
− Brandsäkerhet; rökdetektorer, inergengas
− Redundant 48 V kraftförsörjning till utrustningen
− Avbrottsfri kraft, dieselgenerator för mer än en veckas drifttid

Datorhallar

I Stockholm, Göteborg, Malmö, Oslo och New York har IP-Only datorhallar, de flesta om ca 1 000 kvm vardera. IP-Only äger själv all teknik och hyr enbart lokal från fastighetsägaren. Datorhallarna är gjorda för att kunna härbärgera en stor mängd kundutrustning och är utrustade med datorgolv, kyla, automatisk brandsläckutrustning, strömförsörjningsutrustning, dieselaggregat, kortläsarsystem och larmsystem. I dessa datorhallar kan tjänster såsom dygnet runt (24/7) övervakad colocation erbjudas.

IP-infrastruktur

IP-Only tillämpar en och samma homogena struktur i hela nätet, för att åstadkomma största möjliga skalbarhet och mest effektiva trafikgenomströmning. IP-Onlys IP-nät utmärker sig genom att det genomgående är byggt i flera skilda plan.



Ett plan är för de stora genomfartsflödena och ett annat för de lokala accesserna. Detta ger kunden kortare svarstider och högre bandbredd, genom att trafiken inte bromsas upp av mindre routrar för lokal distribution längs vägen. Denna struktur minimerar också behovet av arbeten i de centrala delarna av nätet eftersom de är skilda från de mindre nätförgreningarna. Lokala förändringsarbeten påverkar därför inte det centrala nätets funktion, och på så sätt minimeras risken för driftstörningar.

IP-Onlys routerstamnät är byggt på en plattform som i nuvarande konfiguration hanterar 160 Gbit/s per nod och enkelt kan byggas ut till 760 Gbit/s. De större noderna sammanbinds av 10 Gbit/s-förbindelser. IP-Onlys backbone är uppbyggt med väl definierade lager för effektiv och tillförlitlig transport av IP-paket. I access- och distributionslagret samlas trafik från kunder på respektive nod, och transporteras därefter genom backbonet i core-lagret som sammanlänkar de olika noderna. Inom backbonet har samtliga routrar full routing med BGP och ett antal fördefinierade communitysträngar som kunder kan utnyttja för att styra hur IP-Only hanterar deras prefix. Utförligare information om dessa finns i AS-objektet för AS12552 i RIPE-DB. Flap damping är konfigurerat enligt dokumentet RIPE-210, som IP-Only varit med och utvecklat. Detta minskar bland annat risken för bortfall av root-DNS:erna till följd av flappande länkar på andra delar av Internet.

2.6.1.3 Banverket

Den fysiska infrastrukturen och kommunikationslösningen kommer att se olika ut för olika beställare. Banverket ICT kan erbjuda Beställaren tydligt underlag för avropad tjänst.

2.6.2 Uthållighet

Fysisk infrastruktur tillhandahålls i detta anbud av Ateas underleverantörer. Nedan redovisas de olika underleverantörernas svar på frågan om uthållighet och tillgänglighet vid extraordinära händelser i fredstid:

2.6.2.1 Telenor

Telenor har planer och beredskap för extraordinära händelser med påverkan på vår telekommunikationsinfrastruktur och dess funktionalitet, dessa planer revideras och testats internt med regelbundet intervall.

Huvuddelen av infrastrukturen har byggts med redundans i olika nivåer och lager för att i möjligaste mån säkerställa tillgänglighet i tjänster till kund.

Test av Telenors planer och beredskap sker dels genom egna tester och övningar och dels genom regelbundet deltagande i kris- och katastrofövningar ledda av PTS.

PTS genomför periodiskt tillsyn av Telenor Sverige och dess dotterbolag, denna tillsyn har utfallit med goda resultat innebärande att PTS och Telenors bedömning av efterlevnaden av rekommendationerna är goda.

2.6.2.2 IP Only

IP-Only följer PTS allmänna råd om god funktion och teknisk säkerhet samt uthållighet vid extraordinära händelser i fredstid (PTSFS 2007:2). IP-Only bedriver ett kontinuerligt och systematiskt säkerhetsarbete och bidrar även med konsultativ verksamhet åt delar av svenska försvaret för hantering av elektroniskt informationsskydd. IP-Only arbetar med risk management och disaster recovery plans.

Arbetet med risk management och disaster recovery plans omfattar bland annat bedömningar om framtida hot och säkerhetsluckor i vårt elektroniska skydd med hjälp av analyser från bland annat logglistor i våra firewalls. Hot om skadegörelse på våra byggnader och nät bedöms också genom exempelvis analyser från larmrapporter och kameraövervakade lokaler.

Arbetsrutiner för säkerhetshantering är beskrivet i NOC personalens arbetsmanual. Incidenter identifieras med tid och datum. Omfattningen analyseras och rapporteras. Bedömning görs hur både framtida incidenter och inträffade kan komma att påverka vår drift och hur det ska hanteras och minimeras i vår verksamhet. Incidentrapporter sänds alltid vidare till ledningsgruppen och VD.

Exempel på uthållighet i vårt eget nät:
IP-Onlys eget nät består av optiska fiberkablar, nedgrävda kabelrör, sk dukter, och noder (accessnoder, distributionsnoder och backbonenoder). Om ett avbrott i elförsörjningen skulle ske avges larm direkt till IP-Onlys NOC. Samtidigt tar lokal batteribackup (sk UPS) vid och säkerställer elförsörjningen. Vid ett frånfall av el överstigande 1 timme går per automatik våra dieselgeneratorer igång och tar över elförsörjningen samtidigt som batterierna återladdas. Bränsletankar finns för kontinuerlig drift på diesel i upp till 7 dygn.

2.6.2.3 Banverket ICT

Banverket ICT bedriver ett kontinuerligt och systematiskt säkerhetsarbete vilket innebär att riskanalyser görs samt att det upprättas planer för hantering av avbrott och störningar. Arbetet bygger dels på Banverkets föreskrifter och standards och dels på processerna i Service Continuity Mgmt, Information Security Mgmt, Incident Mgmt och Problem Mgmt. Järnvägen ställer höga krav på robusthet och säkerhet i data- och telenäten samt att det skall finnas en förmåga att hantera extraordinära händelser och sätter därmed en hög nivå på vårt säkerhetsarbete som kommer alla våra kunder tillgodo.

Banverket ICT är medlem i Post- och Telestyrelsens Nationella TeleSamverkans-Grupp. NTSG är ett samarbetsforum med syfte att stödja återställandet av den nationella infrastrukturen för elektroniska kommunikationer vid extraordinära händelser i samhället. Samarbetet innebär dels att medlemmarna vid större störningar och kriser kan bistå varandra samt även koordinera insatser. Kontinuerliga möten, övningar och utbildningar innebär möjligheter till att öva samverkan mellan parterna samt att utveckla sin egen förmåga att hantera extraordinära händelser.

2.6.3 Skydd av tjänst

Ateas erbjuder skydd av egenproducerade och underleverantörers tjänster enligt nedan:

2.6.3.1 Atea

Ateas egenproducerade tjänster sker till allra störta del placerade hos kund. Skyddet för tjänsterna är därför ett samarbete med kund som omfattar såväl fysiskt skydd som konfigurationsmässigt skydd samt goda rutiner för drifts och underhåll.
En viktig del i detta är att förändringsarbete sker i enlighet med ITILs changeprocess där förändringar genomförs strukturerat och dokumenteras. Händelser i tjänsten som inte är förändringar hanteras som incidenter och/eller problem. Dessa loggas i Ateas ärendehanteringssystem POB och följs upp regelbundet för att identifiera eventuella rotorsaker och åtgärda dessa.

2.6.3.2 Telenor

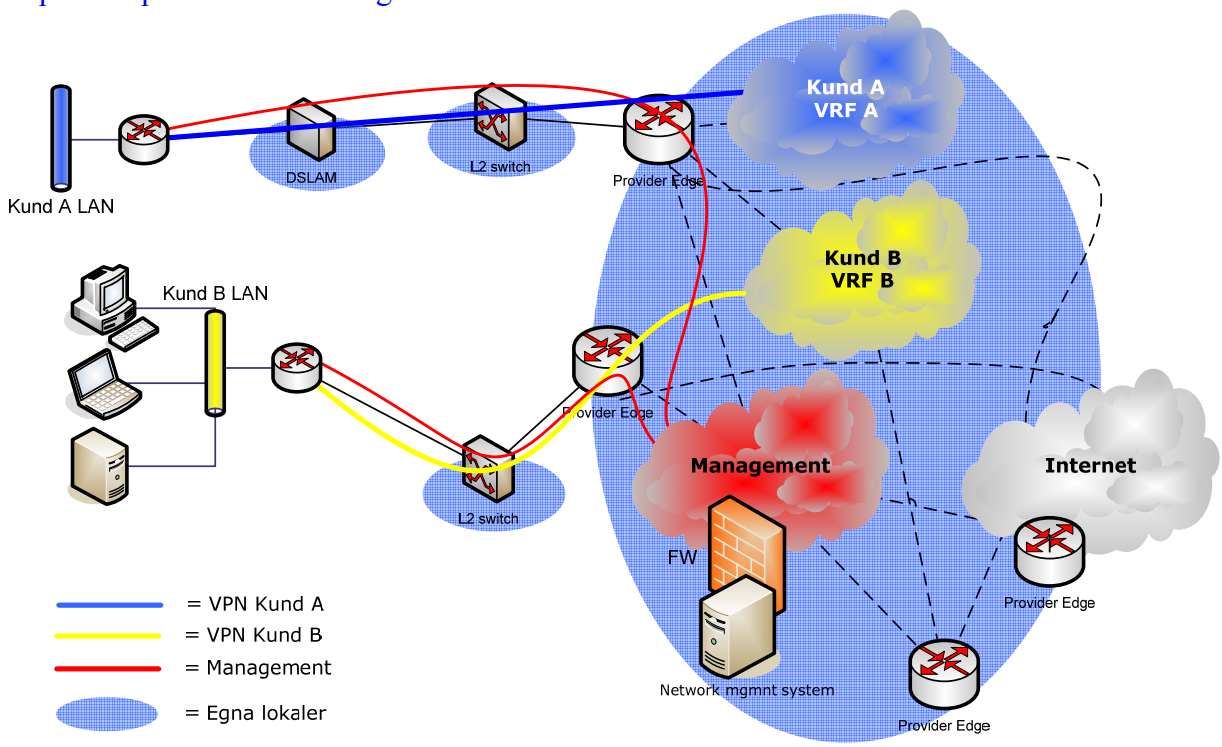
Telenor säkerställer skyddet av sina tjänster och sin infrastruktur genom en kombination av processer, kontroller och stödsystem samt logiska och fysiska skyddsmekanismer i enlighet med vid rådande tid bedömd branschpraxis.

Telenor kan för enskild kund med särskilda behov erbjuda olika tilläggstjänster inom säkerhetsområdet.

2.6.3.2.1 Fasta datanätstjänster/kommunikationstjänster

Svar: Grundsäkerheten i datanätverkstjänsterna är baserad på gällande standarder för respektive teknik.

Detaljerade beskrivningar av säkerhetsmekanismer och tekniker återfinns i respektive produktbeskrivning.



VPN tjänterna realiseras via unika VRF'er per kund/VPN på Provider Edge routers. Unik routingtabell per kund VPN. Enligt RFC 2547-biz MPLS/VPN

Säkerhet på Ethernet nivå är unikt vlan per tjänst, från PE router till kundplacerad utrustning. IEEE 802.1Q

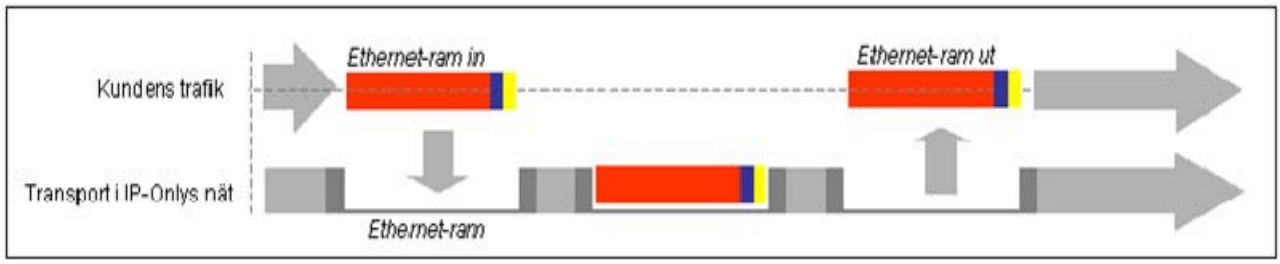
Samtliga siter och datahallar har ett fysiskt skalskydd kompletterat med larminstallationer för att förhindra obehörig fysisk åtkomst till utrustningen.

Figur 3 Grundsäkerhet i fasta datanätstjänster/kommunikationstjänster

2.6.3.3 IP Only

IP-Onlys Ethernet tjänst använder en teknik där kundens trafik separeras och isoleras från annan trafik med hjälp av Ethernet encapsulation. Ethernet encapsulation innebär att den inkommande Ethernet-ramen, vilket inkluderar IEEE Ethernet 802.1p och 802.1Q i sin helhet läggs i en yttre ram. Inkapslingen sker vid kundens avlämningspunkt utan att kunden märker av detta. IP-Only sätter Ethernet-typ 0x9100 i Ethernet-ramen, det vill säga aktiverar stöd för ”jumboframes” för att skapa ett transparent VLAN-stöd. Med jumboframes kommer transportnätet att acceptera

ramar upp till hela 9000 byte. Med hjälp av denna metod förhindrar vi kundtrafik från att läcka ut eller kommuniceras mellan varandra. Respektive kund har alltså bara tillgång till sin egen trafik och kan bara vid speciellt specificerade avlämningspunkter komma åt denna trafik. Avlyssning, intrång, sammankoppling av tjänst eller sabotage är således inte möjligt på tjänstenivå.



Alla konfigurationsförändringar som sker i samband med installation eller felsökning loggas av IP-Only i ett ärendehanteringssystem. Förändringar och larm i utrustning loggas med hjälp av syslog enheter. All information sparas på ett säkert sätt för rutinkontroll och uppföljning.

IP-Onlys våglängdstjänst är helt separerad av fysisk hårdvara för leverans av avtalad tjänst. Detta innebär att ingen avlyssning eller sammankoppling av förbindelser är möjliga för lösningen. De två interface där inkoppling av utrustning och trafik är möjlig är placerad hos kunden och det ligger därmed på kundens ansvar att skydda sin trafik från intrång på denna nivå. Avlyssning, intrång, sammankoppling av tjänst eller sabotage är således inte möjligt på tjänstenivå.

2.6.3.4 Banverket ICT

Banverket ICT följer regler och rutiner i Banverkets Informationssäkerhetsföreskrift BVF004.1 (bilaga Bilaga 3 - 2.6.3.4 Banverket BVF 004.1) och BVF004.2 (Bilaga 3 - 2.6.3.4 Banverket BVF 004.2) och upprätthåller i och med det skydd av tjänsterna.

Kundens virtuella nät är logiskt skiljt från omvärlden på nivå 2 i OSI-modellen och kan därför inte hackas eller avlyssnas från Internet eller publika delar i Banverket ICT´s nät.

2.6.4 Rapportering

Säkerhet är en del av rapporteringen som ingår i Ateas leverans till kund. Denna omfattar såväl rapportering vid incidenter (angrepp, etc) som sker direkt av Servicedesk, som uppföljning vid den regelbundna rapportering av tjänsterna som serviceledaren gör.

I samband med incidenter som bedöms säkerhetsmässigt viktiga så tar också Ateas serviceledare fram en incidentrapport. Gäller detta en incident i en tjänst från en underleverantör så sker detta arbete i samarbete med underleverantören.