Kammarkollegiet

Bilaga 3
Säkerhet

Innehåll

1 Allmänt

2 Säkerhet

Informationssäkerhet och de risker myndigheter utsätts för är frågor som har stor betydelse. Att exempelvis kunna använda telefoni och kommunicera både internt och med andra myndigheter och allmänheten är en mycket viktig del i en myndighets verksamhet.

Säkerhetskraven är indelade i dels administrativa säkerhetskrav som bl.a. omfattar policy, regelverk, rutiner, revisioner och uppföljning samt tekniska säkerhetskrav som omfattar fysisk säkerhet och data- och kommunikationssäkerhet. Utöver ställda krav i detta avsnitt kan det även finnas specifika tekniska säkerhetskrav kopplade till enskilda efterfrågade tjänster och funktioner.

Svar:

Telenor tillhandahåller tjänster till kunder med höga krav på kvalitet och service. En hög säkerhet på Telenor är en förutsättning för att företaget skall kunna leverera service och tjänster av hög kvalitet. Därför är vår målsättning att:

- information om våra kunde inte hamnar i obehörigas händer
- minimera störningar i våra nät och system som kan orsaka våra kunder skada eller besvär
- skydda företagerts 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.

2.1 Administrativa säkerhetskrav

2.1.1 Basnivå för informationssäkerhet

Leverantören bör erbjuda tjänster och funktioner som uppfyller sådana säkerhetskrav att myndigheter och organisationer kan efterleva Krisberedskapsmyndighetens rekommendation ”Basnivå för informationssäkerhet (BITS)” (KBM 2006:1) och medverka till att Beställaren kan upprätthålla en grundsäkerhet som minst motsvarar angiven basnivå. I första hand avses kapitlen 10-14 i BITS.

Svar:
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 KBM's BITS rekommendationer 2006:1.

2.1.2 Uppföljning och kontroll – säkerhetsrevision

Leverantören skall erbjuda Beställaren uppföljning och kontroll av att eventuella avtalade säkerhetsnivåer upprätthålles.

Svar: Uppfylls,
Telenor ställer sig positiva till att utverka modell och processer för kundens önskemål kring uppföljning och rapportering av säkerhetsstatus.
Detaljer utformas i samråd med respektive kund.

2.1.3 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.

Svar: Uppfylls,
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.

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

Leverantören skall för leverans och produktion av erbjudna tjänster och funktioner tillämpa policyer, processer, rutiner och strukturer avseende informationssäkerhet motsvarande SS-ISO/IEC 27002:2005.

Svar: Uppfylls,
Telenor har idag ett Ledningssystem för Informationssäkerhet som är i enlighet med SS-ISO/IEC 27002:2005 samt inrättat processer och interna kontroller motsvarande de krav som återfinns i den amerikanska Sarbane Oxley Act section 404

2.1.5 Redogörelse av Styrning & rutiner motsvarande SS-ISO/IEC 27002:2005

Svar:

Telenor Sveriges 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.

2.2 Allmänna tekniska säkerhetskrav

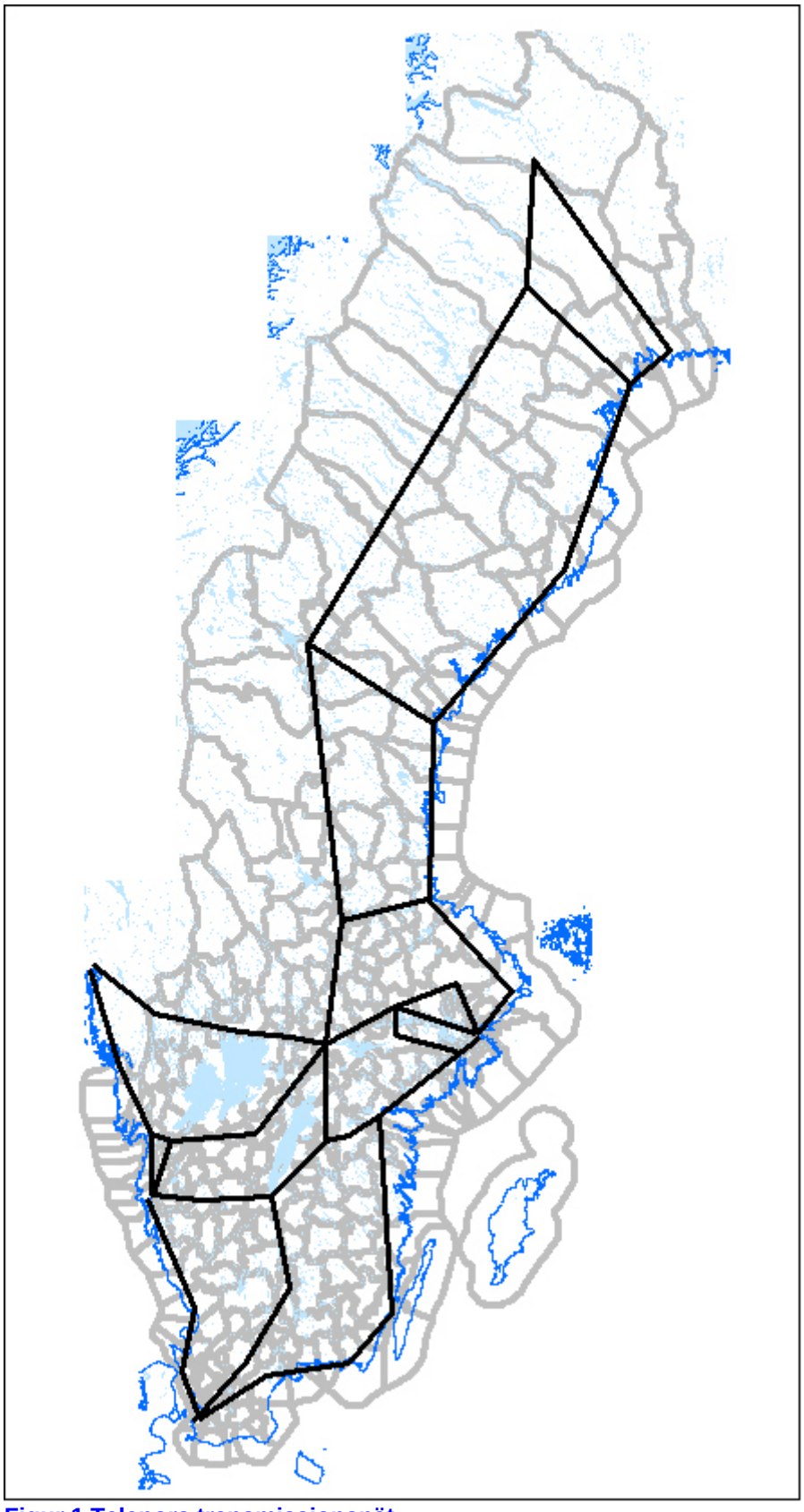
2.2.1 Fysisk infrastruktur

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.

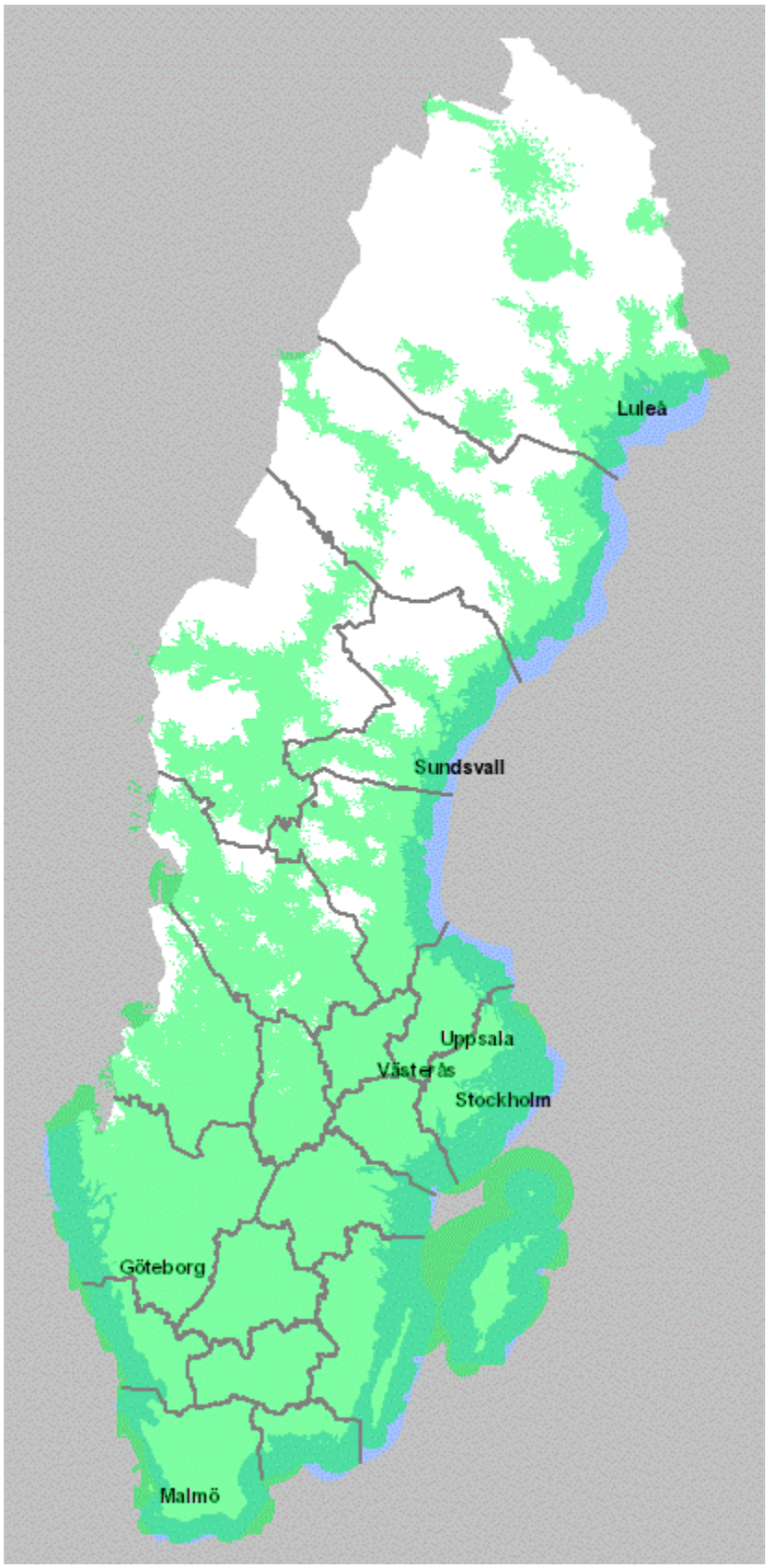
Svar: Uppfylls,
Telenors leverans av tjänster baseras i huvudsak på egen infrastruktur och i de fall det inte är möjligt på hyrd, men av Telenor kontrollerade förbindelser.

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 1 Telenors transmissionsnät



Figur 2 Täckningskarta mobilnät

2.2.2 Uthållighet

Leverantören bör följa PTS allmänna råd om god funktion och teknisk säkerhet samt uthållighet och tillgänglighet vid extraordinära händelser i fredstid efterlevs (PTSFS 2007:2).

Svar:

Telenor har rutiner/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.

2.2.3 Skydd av tjänst

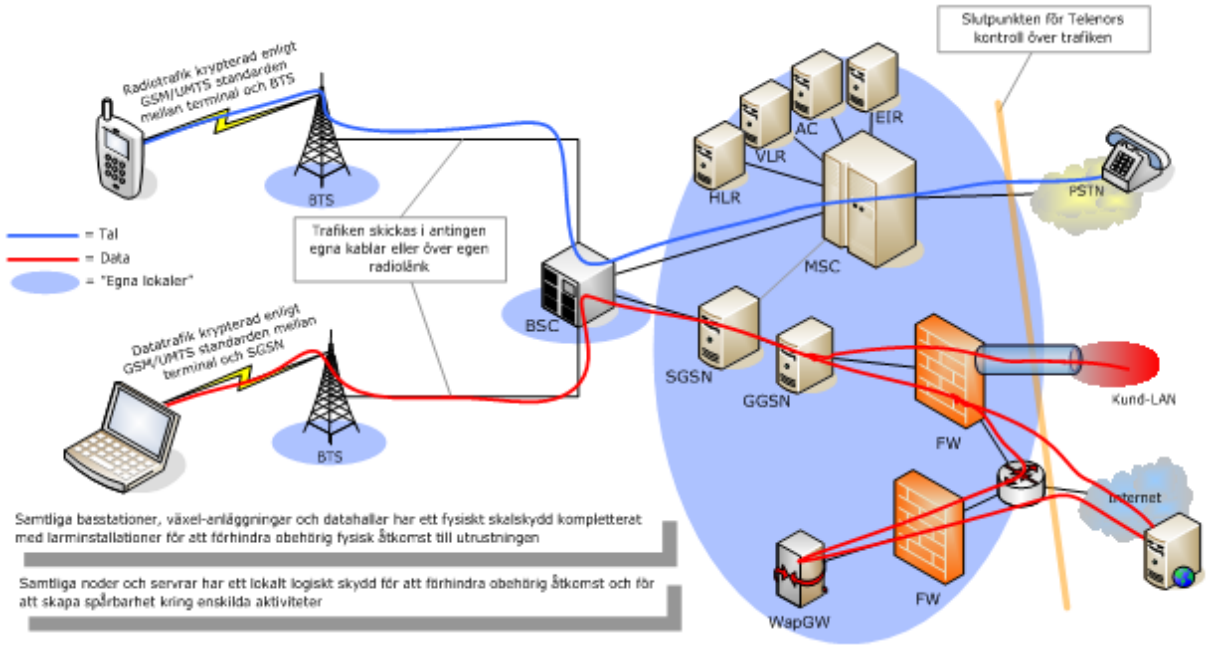
Beskriv hur tjänster skyddas mot otillbörligt nyttjande, intrång, avlyssning, annan manipulering, sabotage och sammankoppling med andra kunders kommunikationstjänster och hur spårbarhet av förändringar och händelser i tjänsten kan säkerställas.

Svar:
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.

2.2.3.1 Mobila tjänster

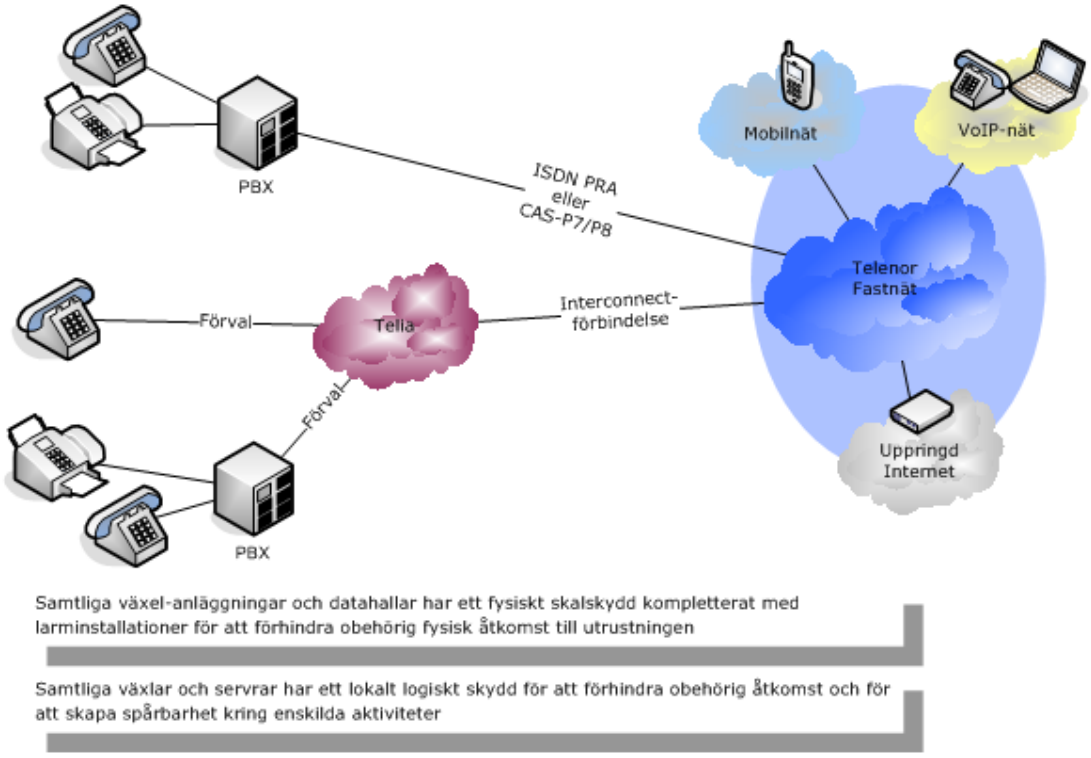
Logisk grundsäkerhet i mobiltelefoninätet är uppbyggt i enlighet med gällande standarder för GSM och UMTS.
Detaljerade beskrivningar av säkerhetsmekanismer och tekniker återfinns i respektive produktbeskrivning.



Figur 3 Grundsäkerhet i mobila tjänster

2.2.3.2 Fasta telefonitjänster, PSTN

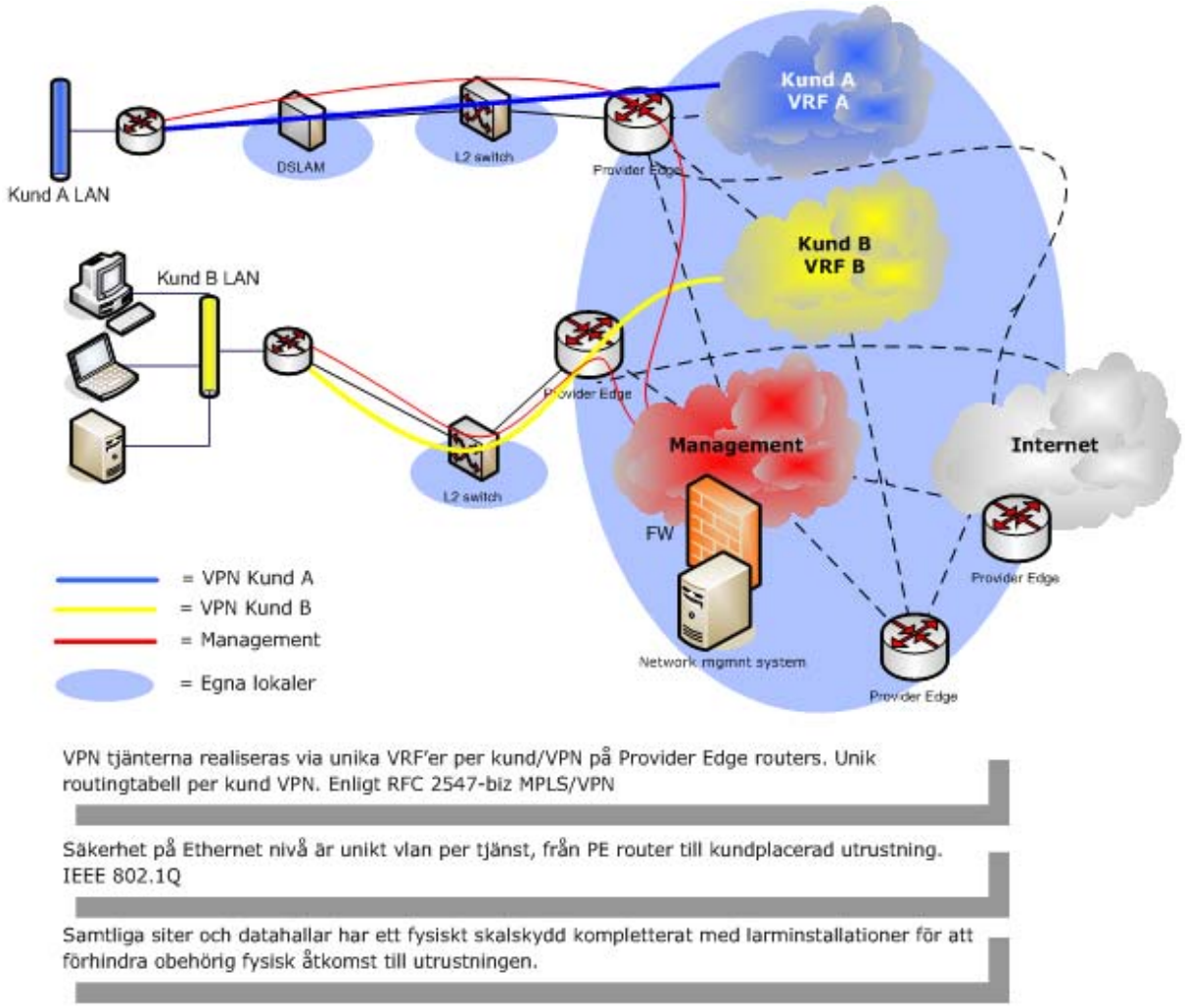
Grundsäkerheten i det fasta telefoninätet är i enlighet med branschstandard för PSTN.
Detaljerade beskrivningar av säkerhetsmekanismer och tekniker återfinns i respektive produktbeskrivning.



Figur 4 Grundsäkerhet i fasta telefonitjänster

2.2.3.3 Fasta datanätstjänster/kommunikationstjänster

Grundsäkerheten i datanätverkstjänsterna är baserad på gällande standarder för respektive teknik.
Detaljerade beskrivningar av säkerhetsmekanismer och tekniker återfinns i respektive produktbeskrivning.



Figur 5 Grundsäkerhet i fasta datanätstjänster/kommunikationstjänster

2.2.4 Rapportering

Leverantören skall omedelbart rapportera brister i skyddet av eller angrepp mot tjänsten eller till tjänsten relaterad infrastruktur till Beställaren.

Svar: Uppfylls,
Telenor erbjuder dels en generell rapportering och dels möjlighet till kundanpassad rapportering avseende säkerhetsrelaterade incidenter i tjänster, produkter och tjänsteproducerande plattformar i den mån det har en påverkan på leveransen till kund. Tidsförhållandet för rapporteringen är beroende på incidentens art och allvarlighetsgrad.