FFI-RAPPORT

16/00808

LTE i Forsvaret

sårbarheter knyttet til ulike forretningsmodeller

–

Bodil Hvesser Farsund
Anne Marie Hegland
Frode Lillevold

LTE i Forsvaret

sårbarheter knyttet til ulike forretningsmodeller

Bodil Hvesser Farsund
Anne Marie Hegland
Frode Lillevold

Forsvarets forskningsinstitutt (FFI) 18. april 2016

Emneord

LTE
Mobilkommunikasjon
Forretningsmodeller
Sikkerhet
Sårbarhet

FFI-rapport:
FFI-RAPPORT 16/00808

Prosjektnummer
1294

ISBN –
P: ISBN 978-82-464-2736-2
E: ISBN 978-82-464-2737-9

Godkjent av
Nils Agne Nordbotten, *forskningsleder*
Anders Eggen, *avdelingssjef*

Sammendrag

LTE (Long Term Evolution) er en kommersiell 4G bredbåndsteknologi som har blitt svært utbredt. Rapporten omhandler sikkerhet ved bruk av LTE i Forsvaret. Den gir en oversikt over risikoområder som bør studeres nærmere, og som beslutningstakere bør ha et forhold til. I tillegg er rapporten ment som et rammeverk for videre diskusjoner knyttet til sikkerhet og sårbarhet ved bruk av LTE i Forsvaret.

Forsvaret har behov for interoperabilitet, båndbredde og kostnadseffektive løsninger for å dekke sitt kommunikasjonsbehov. Følgelig er det naturlig å vurdere kommersielle løsninger som LTE for militær bruk. Dette diskuteres både i Norge og i andre land. Teknologien er lett tilgjengelig, utbredelsen er stor og standardene er åpne og drives fram av teleorganisasjoner og kommersielle aktører.

Brukerenhetene er rimelige, men det kreves en svært stor investering i infrastruktur dersom Forsvaret selv skal bygge ut et eget riksdekkende nett. Både utbygging av basestasjoner og tilgang til frekvenser representerer en stor kostnad. Det er derfor nærliggende å vurdere avtaler med kommersielle operatører om tilgang til deres infrastrukturer. Det finnes flere forretningsmodeller – alt fra at nettet i sin helhet opereres av den kommersielle aktøren til at Forsvaret selv er en mobil operatør med egne basestasjoner. Forretningsmodellene medfører forskjellige grader av sårbarhet.

Rapporten gir først en oversikt over LTE-arkitekturen og hvilken sikkerhet som ligger innebygget i standarden. For å kunne vurdere sårbarhet i ulike forretningsmodeller er det nødvendig å definere hvilke verdier som trenger beskyttelse. Rapporten skiller mellom verdiene brukerdata, informasjon om brukeren, samt nettverkstilgjengelighet.

Rapporten illustrerer generiske sårbarheter ved ulike forretningsmodeller. En endelig vurdering vil i tillegg kreve at det tas hensyn til hvordan LTE ønskes brukt i Forsvaret. Som en ren erstatning for dagens mobiltelefoniløsning vil noen av modellene kunne gi lavere sårbarhet enn dagens situasjon. Hvis derimot LTE skal anvendes på nye områder, må sikkerheten også vurderes opp mot de konkrete kravene i anvendelsen. Det er således viktig for Forsvaret å avklare hvordan LTE eventuelt skal anvendes.

Alle forretningsmodellene har fordeler og ulemper. Gjennomgangen viser at kontroll over basestasjoner har stor innvirkning på sikkerheten. Generelt vil sårbarheten også øke ved roaming.

Summary

LTE is a widely used commercial 4G broadband technology. The report elaborates on security issues concerning military use of Long Term Evolution (LTE). It provides an overview of risk areas that should be studied more closely, and that decision makers should be aware of. The report is in addition intended as a framework for further discussions on security and vulnerability related to the use of LTE in the Armed Forces.

The armed forces need interoperability, bandwidth and cost effective solutions to fulfil their communication needs. Accordingly, it is natural to consider commercial solutions such as LTE for military use. This is discussed both in Norway and in other countries. The technology is readily available, the standards are open and maintained by telecommunications organizations and commercial actors, and the prevalence is great.

User devices are affordable. However, it requires a very large investment in infrastructure for the Norwegian Armed Forces to build its own nationwide network. Both base stations and access to frequencies represent a major cost. Consequently, it is natural to consider co-operation with commercial telecommunication providers and access to existing infrastructure. There are several possible business models – ranging from solutions fully delivered by the commercial operator to solutions where the Norwegian Armed Forces own the network themselves and act as a mobile network operator.

Different business models represent different degrees of vulnerability. The report first gives an overview of the LTE architecture and the security built into the standard. In order to be able to assess the vulnerability of the various business models, it is necessary to define the values that need protection. The report distinguishes between the values user data, information about the user, and network availability. The report seeks to illustrate generic security implications of different business models. A final assessment will also have to include the intended use of LTE in the Armed Forces. As a pure replacement for today's mobile telephony solution, some of the models could be less vulnerable than the current situation. However, if LTE is to be used in new areas, security cannot be evaluated without taking the specific requirements for these applications into consideration.

All business models have advantages and disadvantages. The review shows that control of base stations have a major impact on security. The vulnerability also increases when roaming is included.

Innhold

1 Innledning

LTE (Long Term Evolution) er en kommersiell 4G mobil bredbåndsteknologi som har blitt svært utbredt. På under 6 år har LTE vokst til å ha over 1 milliard abonnenter på verdensbasis, og det forventes at den sterke veksten vil fortsette slik at det i 2020 vil være nærmere 4 milliarder abonnenter [1].

Flere land vurderer å bruke LTE militært, deriblant Norge. Det er flere grunner til at LTE-teknologien kan være interessant å vurdere for Forsvaret. De viktigste er båndbredde, interoperabilitet og økonomi. Operative behov og aktuelle bruksområder for LTE-teknologi er fortsatt tema for diskusjon. Mulighetsrommet spenner fra «kontortelefon» hjemme i Norge i fredstid til anvendelse som bredbåndsradio i taktiske operasjoner på utenlandsoppdrag.

For å nå økt NbF-modenhet behøves blant annet mobil bredbåndskapasitet, og mange mener at LTE kan være et godt alternativ. Samtidig mangler NATO interoperabilitetsstandarder, da ulike leverandører tilbyr forskjellige proprietære bølgeformer. Interoperable systemer er avgjørende for en vellykket operasjon, og dagens løsning med blant annet å låne utstyr av hverandre skalerer dårlig. I en situasjon med et økende antall internasjonale operasjoner er behovet for interoperabilitet med andre nasjoner stort. Det er ønskelig at hver nasjon skal kunne bruke eget utstyr og være kompatible med dem de skal samhandle med.

Siden NATOs standardiseringsarbeid går sakte, er det interessant å vurdere kommersielle standarder som LTE. Standarden drives frem og vedlikeholdes av 3GPP (3rd Generation Partnership Project) der store teleaktører deltar. Ettersom utbredelsen er stor, gir dette rimelig utstyr. Det er også en fordel med et brukergrensesnitt som soldatene er vant til å bruke privat. Å benytte LTE kan derfor være et kostnadseffektivt alternativ.

Spørsmålet er hvordan Forsvaret eventuelt kan og bør benytte LTE. LTE er en infrastrukturbasert teknologi, og utbygging og vedlikehold av basestasjoner er kostnadskrevende. Det er ikke gitt at det er regningssvarende for Forsvaret å bygge ut og drifte egen infrastruktur. Ulike forretningsmodeller kan tenkes – alt fra en hvor Forsvaret eier og bygger ut alt selv, til at Forsvaret er kunde hos en eller flere kommersielle aktører. En mulighet er en kombinasjon hvor Forsvaret er en Mobil Virtuell Nettverksoperatør (MVNO) som eier og drifter deler av infrastrukturen.

Rapporten gir en oversikt over noen ulike forretningsmodeller og diskuterer sårbarheter knyttet til det å ikke ha kontroll på ulike deler av infrastrukturen. En annen hensikt er å gi et overordnet bilde over hva som må beskyttes og hvilke generiske sårbarheter som finnes. Rapporten tar ikke stilling til om Forsvaret bør eller ikke bør basere seg på LTE. Den påpeker bare risikoområder som bør studeres nærmere, og som beslutningstakere bør være kjent med. Forhåpentligvis kan også rapporten tjene som et rammeverk for videre diskusjoner rundt Forsvarets bruk av LTE og sikkerhetsutfordringer knyttet til dette.

Først i rapporten gis en introduksjon til arkitektur og sikkerhet i LTE, samt faktorer som kan påvirke valg av forretningsmodell. Videre diskuteres hvilke verdier som trenger beskyttelse, aktuelle trusler og mulige angrepsvektorer. Deretter følger en oversikt over sårbarheter ved ulike forretningsmodeller før avsluttende oppsummering og diskusjon.

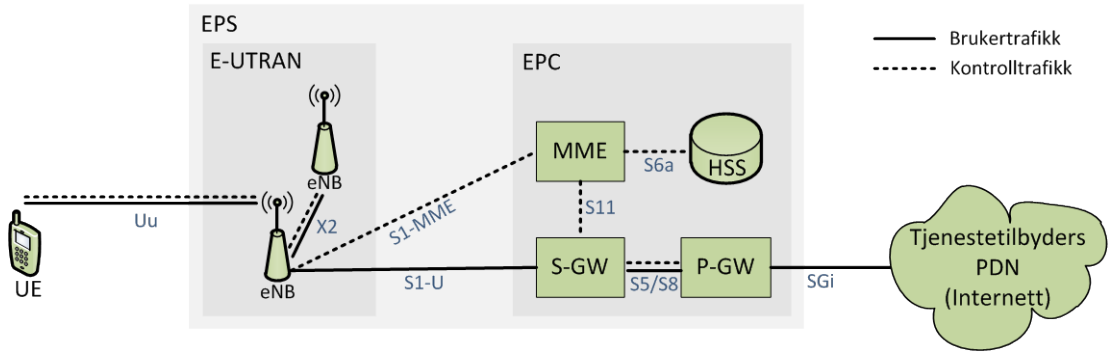
2 LTE-arkitektur

LTE-spesifikasjonene vedlikeholdes av 3GPP (3rd Generation Partnership Project) som er et samarbeid mellom telekommunikasjonsstandardiseringsorganisasjoner fra Asia, Europa og Nord-Amerika. Innholdet i dette kapittelet er for det meste basert på informasjon hentet fra hjemmesidene til 3GPP[4].

Figur 2.1 gir en oversikt over LTE-arkitekturen. Nettverket i LTE kalles EPS (Evolved Packet System). All kommunikasjon i EPS, både sanntidstjenester og andre tjenester, går over IP. EPS består av to deler:

- E-UTRAN (Evolved UMTS Terrestrial Radio Access Network) som er aksessnettverket bestående av basestasjonene.
- EPC (Evolved Packet Core) som betegner det bakenforliggende kjernenettverket.

I tillegg kommer selve brukerenhetene (UE, User Equipment). Hver komponent blir beskrevet nærmere i de følgende delkapitlene.



Figur 2.1 Oversikt over LTE-arkitekturen.

I taktiske operasjoner kan det være ønskelig å kunne kommunisere også uten fast infrastruktur. LTE Advanced [5] spesifiserer brukerenhet-til-brukerenhet kommunikasjon over korte

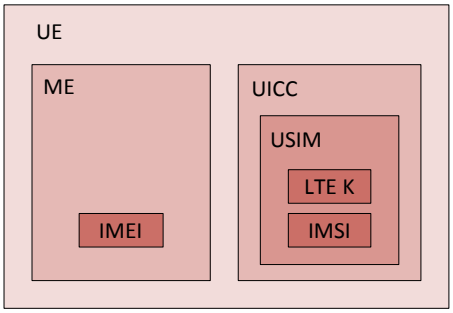
avstander. Forbindelsen kan enten initieres via fast infrastruktur, eller så kan brukerenhetene etablere forbindelser gjennom direkte forhandling seg imellom. Hovedfokus i denne rapporten er ordinær bruk av LTE hvor det kommuniseres ved hjelp av infrastrukturkomponenter.

2.1 Brukerenheten (UE)

UE (User Equipment) er brukerenheten som består av selve mobiltelefonen (ME, Mobile Equipment) og UICC (Universal Integrated Circuit Card) som vist i Figur 2.2. UICC er et smartkort som kjører applikasjonen USIM (Universal Subscriber Identity Module). USIM inneholder identifikatoren IMSI (International Mobile Subscriber Identity), som benyttes for å identifisere abonnenten.

En USIM kan kun inneholde én IMSI. I enkelte tilfeller kan UICC inneholde flere USIM med tilhørende IMSI [6]. USIM inneholder i tillegg til IMSI en unik sikkerhetsnøkkel, *LTE K*, som vil bli beskrevet i kapittel 3.

Mobiltelefonen (ME) identifiseres unikt ved hjelp av identifikatoren IMEI (International Mobile Equipment Identity). Denne identifikatoren er uløselig knyttet til utstyret, og byttes aldri. Den brukes blant annet til å sjekke om enheten er stjålet. IMSI kan derimot byttes, og dette gjøres for eksempel når man skifter abonnement fra en operatør til en annen.



Figur 2.2 Illustrasjon av hva brukerenheten (UE) består av.

2.2 Aksessnettverket (E-UTRAN)

Aksessnettverket i LTE kalles E-UTRAN, se Figur 2.1. Det består av basestasjoner som betegnes eNB (evolved-NodeB). Dette nettverket gir radiokommunikasjon mellom UE og EPC. Det er lagd med tanke på høy spektrumsutnyttelse, høy datarate, kort tidsforsinkelse og fleksibilitet i frekvens- og båndbreddebruk.

Hver eNB kontrollerer UE-er i en eller flere celler. De kommuniserer over følgende grensesnitt som er angitt i Figur 2.1:

- Uu: Grensesnitt mot UE for både brukertrafikk og kontrolltrafikk.

- S1: Grensesnitt mot EPC. S1-U overfører brukertrafikk fra/til S-GW og S1-MME overfører kontrolltrafikk fra/til MME. S-GW og MME beskrives i neste delkapittel.

- X2: Grensesnitt mot andre eNB. Overfører kontrolltrafikk samt brukertrafikk i forbindelse med bytte av basestasjon (handover).

I forhold til tidligere generasjoner mobilnettverk ligger det mer funksjonalitet i basestasjonene i LTE. Det finnes ingen sentral styringsenhet. Denne funksjonaliteten er lagt i basestasjonene for å redusere tiden det tar å sette opp en forbindelse og å foreta en handover.

Sentrale oppgaver for basestasjonene i LTE er dynamisk å tildele radioressurser til brukerenhetene basert på hvilke tjenester de benytter samt dynamisk å bestemme hvilken modulasjon og koding som skal benyttes i henhold til gitt radiomiljø. I tillegg utfører de handover.

Det finnes flere typer eNB. En "Home eNB" (HeNB) er en basestasjon som har blitt fremskaffet av en bruker for å tilby dekning innenfor en bygning eller et område. Den vil også avlaste operatørens nettverk. HeNB tilhører en lukket abonnementsgruppe og kan bare aksesseres av mobiler med et USIM som også tilhører denne gruppen. Slike små celler kalles også femtoceller.

2.3 Kjernenettverket (EPC)

Kjernenettverket i LTE kalles EPC. Det har en flat arkitektur med færre nivåer enn i GSM og UMTS. Hensikten er å få til en mer effektiv håndtering av datatrafikk ved at få nettverksnoder er involvert og konvertering mellom protokoller unngås. I tillegg er brukertrafikk og kontrolltrafikk separert i EPC, noe som gjør det enklere for operatørene å dimensjonere og tilpasse nettverkene til sine behov.

De mest sentrale elementene i EPC er:

- HSS (Home Subscriber Server) er operatørens sentrale database hvor informasjon om abonnentene er lagret. Den kontaktes av MME for autentisering av UE ved oppkobling.

- P-GW (Packet Data Network Gateway) håndterer brukertrafikk mellom LTE-nettverket og andre nettverk. Dette kan være nettverksoperatørens servere, Internett eller IMS (IP multimedia subsystem). Sentrale oppgaver er ruting av pakker, allokering av IP-adresser til brukerenhetene og å filtrere pakker for hver bruker.

- S-GW (Serving gateway) håndterer brukertrafikk. Dens viktigste oppgave er å transportere IP-pakker mellom eNB-er i et gitt ansvarsområde og P-GW, og den

fungerer i prinsippet som en ruter. Hver brukerenhet er tilknyttet en S-GW, men denne endres hvis brukerenheten flytter ut av ansvarsområdet.

- MME (Mobility Management Entity) håndterer kontrolltrafikk. Dens hovedoppgaver er signalering ved oppsetting av IP-forbindelser (kontakter S-GW og P-GW), sikkerhet og funksjoner relatert til hvilemodus (tracking og paging). En MME kontrollerer flere eNB i et gitt geografisk ansvarsområde.

EPC har følgende grensesnitt:

- SGi: Brukertrafikk mellom P-GW og andre pakkedatanettverk.
- S11: Kontrolltrafikk mellom MME og S-GW for EPS-management som blant annet handover støttet av MME og koordinering i forbindelse med paging. Mange-til-mange grensesnitt.
- S6a: Kontrolltrafikk mellom MME og HSS. Overfører abonnentinformasjon for autentisering og autorisasjon av brukere.
- S5/S8: Bruker- og kontrolltrafikk mellom S-GW og P-GW. Se avsnitt 4.3 for hvordan disse blir brukt ved roaming.

3 Sikkerhet i LTE

Trådløs kommunikasjon er generelt sårbar fordi det er vanskelig å begrense fysisk utbredelse av signalene. De fleste trådløse standarder har derfor sikkerhetstiltak for å beskytte informasjon som sendes over radio [18]. Sikkerhet i LTE omfatter sikkerhet over radiogrensesnittet, samt sikkerhet internt i EPS. Begge deler beskrives i det følgende.

Sikkerhet over radiogrensesnittet er skissert i Figur 3.1, og består av tre hoveddeler:

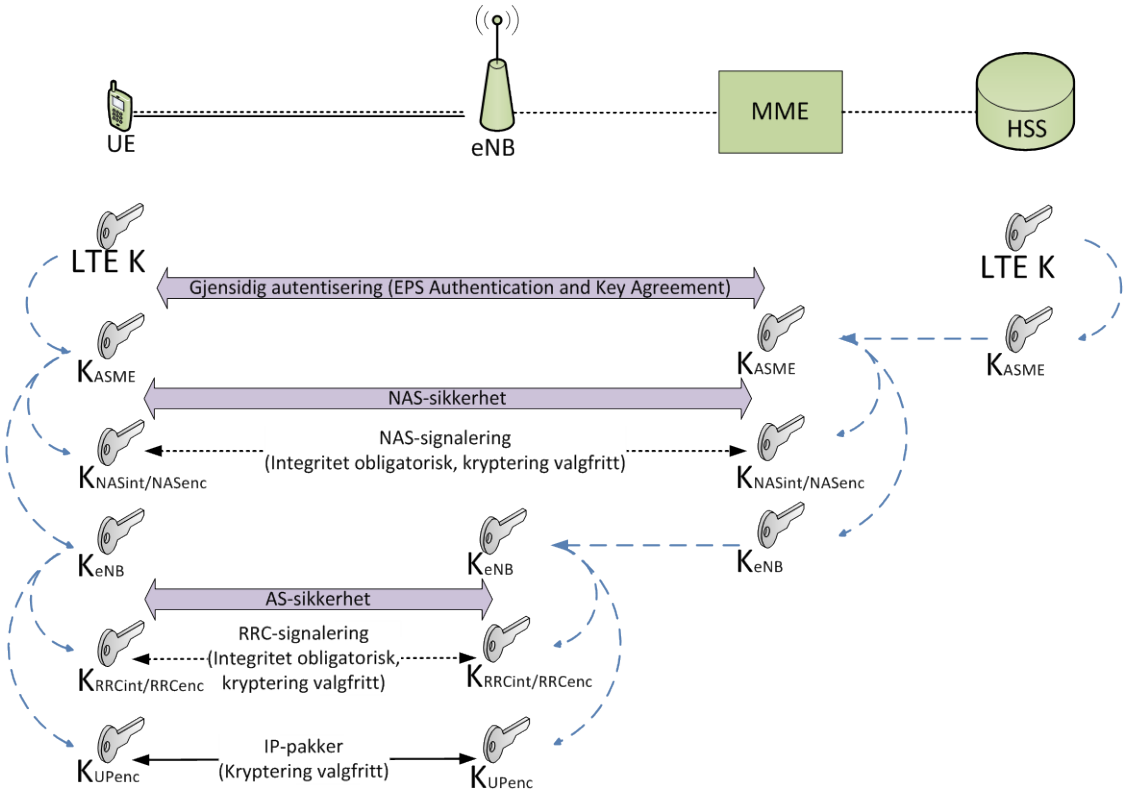
- LTE-autentisering: Gjensidig autentisering mellom UE (egentlig USIM) og nettverket.
- NAS-sikkerhet (Non-Access Stratum): Beskyttelse av kontrolltrafikk mellom UE og MME. Denne består av obligatorisk integritetsbeskyttelse og valgfri kryptering.
- AS-sikkerhet (Access Stratum): Beskyttelse av kontroll- og brukertrafikk mellom UE og eNB. Denne består av:

- Obligatorisk integritetsbeskyttelse og valgfri kryptering av RRC-signalering (Radio Resource Control).

- Valgfri kryptering av brukertrafikk (integritetsbeskyttelse tilbys ikke).

Det store bildet er altså at kontrolltrafikk mellom brukerenheten og LTE-nettverket blir integritetsbeskyttet, men ikke nødvendigvis kryptert. Brukertrafikk kan bli kryptert, men blir ikke integritetsbeskyttet. I kjernenettverket blir kontrolltrafikk integritetsbeskyttet mellom operatører, men innad i en operatørs nettverk er det ikke obligatorisk med hverken integritets- eller konfidensialitetsbeskytte. Det er ingen krav til beskyttelse av brukertrafikken i kjernenettet.

Dette blir nærmere beskrevet i det følgende. Lesere som ikke ønsker detaljene, kan hoppe over resten av dette kapittelet.



Figur 3.1 Oversikt over kryptonøkler og sikkerhet mellom brukerenheten (UE) og LTE-nettverket (EPS).

3.1 LTE-autentisering

LTE-autentiseringen er gjensidig mellom brukerenheten og nettverket. Prosedyren som blir brukt til dette kalles EPS AKA (Authentication and Key Agreement), og foregår mellom MME og USIM som sitter i UE. Sikkerheten er basert på en symmetrisk nøkkel, *LTE K*, som kun ligger i brukerens USIM og i HSS. Den blir ikke sendt mellom enhetene i LTE-infrastrukturen. MME er derfor avhengig av HSS for å autentisere USIM.

Fra *LTE K* avledes en ny nøkkel - K_{ASME} - som igjen benyttes til å utlede nye nøkler som beskytter brukerdata og kontrolltrafikk som forklart i det følgende. I motsetning til *LTE K* lagres K_{ASME} og de andre nøklene i ME, altså utenfor USIM.

Prosedyren starter med at UE sender en forespørsel til MME om å få registrere seg i nettverket. Her overføres blant annet IMSI (International Mobile Subscriber Identity) og hvilke sikkerhetsalgoritmer UE støtter i klartekst. Før MME kvitterer på denne forespørselen, sender den en autentiseringsforespørsel til HSS med blant annet brukerens IMSI. Denne brukes av HSS for å identifisere hvilken bruker det dreier seg om. HSS beregner så en eller flere autentiseringsvektorer med EPS AKA-algoritmen, og returnerer vektorene til MME. Vektorene inneholder blant annet:

- K_{ASME} - Aksessikkerhetsnøkkel (Access Security Management Entity Key)
- $AUTN_{HSS}$ - Autentiseringstoken
- Forventet respons

Til å beregne dette brukes blant annet nøkkelen *LTE K*.

Etter å ha lagret autentiseringsvektorene, velger MME ut én som den benytter til gjensidig autentisering med brukerenheten, og sender deretter blant annet autentiseringstokenet $AUTN_{HSS}$ til brukerenheten. Ved hjelp av sin kopi av *LTE K*, beregner USIM:

- K_{ASME} - Aksessikkerhetsnøkkel
- $AUTN_{UE}$ - Autentiseringstoken
- Respons

Hvis autentiseringstokenet ($AUTN_{UE}$) som UE beregner er lik autentiseringtokenet ($AUTN_{HSS}$) som er mottatt fra MME vil brukerenheten autentisere nettverket. Den returnerer så responsen til MME. Hvis responsen fra UE stemmer med forventet respons mottatt fra HSS, har MME/nettverket autentisert brukerenheten. MME og UE deler nå en felles aksessikkerhetsnøkkel K_{ASME}, som ikke har blitt sendt over radiogrensesnittet. Denne nøkkelen

brukes til å avlede nøkler for beskyttelse av kontrolltrafikk mellom UE og MME (NAS-sikkerhet) og kontroll- og brukertrafikk mellom UE og eNB (AS-sikkerhet).

3.2 Beskyttelse av kontrolltrafikk mellom UE og MME (NAS-sikkerhet)

NAS-sikkerhet skal beskytte kontrolltrafikk mellom UE og MME. Den baserer seg på aksessikkerhetsnøkkelen K_{ASME}, som de deler etter gjensidig autentisering. Først velger MME hvilke kryptoalgoritmer som skal benyttes. UE anga hvilke algoritmer den støttet i den første autentiseringsmeldingen til MME. Basert på aksessikkerhetsnøkkelen og valgte algoritmer utledes en NAS integritetsnøkkel, K_{NASint}, og en NAS-krypteringsnøkkel, K_{NASenc},.

Mulige algoritmer er SNOW 3G, AES (Advanced Encryption Standard) og ZUC (en kinesisk algoritme som er valgfri å støtte). Alle algoritmene bruker 128 bits nøkler og er flytchiffer eller kjøres i flytchiffer operasjonsmodus. Integritetsbeskyttelse er obligatorisk, men ikke kryptering. Det er valgfritt å kryptere NAS-signaleringsmeldingene.

Etter at MME har valgt NAS-nøkler og kryptoalgoritmer, sender den en melding til UE om hvilke sikkerhetsalgoritmer som er valgt. Meldingen blir integritetsbeskyttet med en kryptografisk sjekksum beregnet med integritetsnøkkelen K_{NASint}. UE utleder nøklene K_{NASint} og K_{NASenc} fra K_{ASME} og mottatte algoritmer og beregner den kryptografiske sjekksummen. Hvis denne stemmer overens med sjekksummen fått av MME, er meldingens integritet verifisert.

UE sender deretter en respons til MME om at meldingen er korrekt mottatt og at nøkler er utledet. Denne meldingen blir kryptert (hvis det er valgt å kryptere) og integritetsbeskyttet. Når MME har verifisert og dekryptert meldingen, er sikkerhetsoppsettet for NAS ferdig. Videre vil alle NAS-meldinger mellom MME og UE først bli kryptert, hvis dette er valgt, og deretter integritetsbeskyttet.

3.3 Beskyttelse av kontroll- og brukertrafikk mellom UE og eNB (AS-sikkerhet)

Hensikten med AS-sikkerhet er å beskytte kontroll- og brukertrafikk mellom UE og eNB. Det starter med at MME utleder en nøkkel, K_{eNB} fra K_{ASME}, og sender denne nøkkelen samt hvilke sikkerhetsalgoritmer UE støtter til basestasjonen. Basestasjonen velger deretter hvilke algoritmer som skal benyttes for å sikre kontroll- og brukertrafikk mellom basestasjon og brukerenhet. Basert på disse sikkerhetsalgoritmene og den mottatte nøkkelen K_{eNB} utleder basestasjonen en nøkkel for å integritetsbeskytte RRC-signaleringen (K_{RRCint}), en nøkkel for å kryptere RRC-signaleringen (K_{RRCenc}) og en for å kryptere brukertrafikken (K_{UPenc}).

Hvilke sikkerhetsalgoritmer som er valgt sender basestasjonen til brukerenheten. Denne meldingen blir integritetsbeskyttet med en kryptografisk sjekksum. Når brukerenheten mottar meldingen kan den på samme måte utlede sine nøkler, samt verifisere at meldingen er korrekt mottatt ved å verifisere sjekksummen.

UE sender deretter en respons til basestasjonen om at meldingen er korrekt mottatt og at nøkler er utledet. Denne meldingen blir integritetsbeskyttet med nøkkelen K_{RRCint}. Når basestasjonen

har verifisert meldingen, er AS-sikkerhetsoppsettet ferdig. Videre vil all RRC-signalering først bli integritetsbeskyttet og deretter eventuelt kryptert (omvendt av NAS-sikkerhet), samtidig vil all brukertrafikk bli kryptert om dette er bestemt. Integritetsbeskyttelse av RRC-signaleringen er obligatorisk, mens kryptering av både RRC-signalering og brukertrafikk er valgfritt for operatøren.

3.4 Sikkerhet i resten av aksessnettverket og kjernenettverket

I aksessnettverket og kjernenettverket er det obligatorisk å integritetsbeskytte kontrolltrafikk mellom sikkerhetsdomener, det vil blant annet si S8-grensesnittet (se Figur 2.1) ved roaming mellom operatører[10]. Konfidensialitetsbeskyttelse er anbefalt, men ikke obligatorisk. Internt i et sikkerhetsdomene er hverken beskyttelse av integritet eller konfidensialitet påkrevd. Et sikkerhetsdomene defineres som et nettverk administrert av samme autoritet, og som opererer på samme sikkerhetsnivå i de tilfeller hvor det finnes flere enn ett nivå. Et sikkerhetsdomene tilsvarer vanligvis en operatørs EPC, men i enkelte tilfeller kan en operatør ha flere sikkerhetsdomener. I aksessnettverket blir vanligvis X2- og S1-grensesnittene sikret.

Sikkerheten er basert på IPsec [7]. Trafikken beskyttes ved hjelp av IPsec ESP (Encapsulating Security Payload) [8] og nøkler som forhandles ved hjelp av IKEv2-protokollen (Internet Key Exchange) [9]. ESP kan kjøres i transport- eller tunnelmode. Primært benyttes ESP tunnelmode hvor hele det opprinnelige datagrammet blir beskyttet. I transportmode beholdes det opprinnelige IP-pakkehodet, og bare datadelen av datagrammet blir beskyttet. Det er valgfritt for operatøren å støtte transportmode.

Det er i utgangspunktet bare kontrolltrafikken som beskyttes i kjernenettet. Det er ingen obligatoriske beskyttelsestiltak for brukertrafikk.

4 Faktorer knyttet til valg av løsning

I dag benytter mobiloperatørene ulike forretningsmodeller. Det er ikke lenger slik at en operatør nødvendigvis eier og drifter hele nettverket sitt selv. De neste delkapitlene forklarer hva som menes med begrepene mobil nettverksoperatør (MNO) og mobil virtuell nettverksoperatør (MVNO).

Siden roaming også er en form for samarbeid mellom mobiloperatører har vi valgt å beskrive dette i et eget avsnitt. Brukerenheten omtales også ettersom den også kan ha sårbarheter. Ulike modeller knyttet til anskaffelse og bruk av brukerenheter er beskrevet til slutt i kapittelet.

4.1 Mobil nettverksoperatør (MNO)

En vanlig definisjon på en mobil nettverksoperatør (MNO) er at operatøren må ha lisens for bruk av aktuelle radiofrekvenser i tillegg til nødvendig infrastruktur for å tilby tjenester til sine abonnenter over disse frekvensene. Det er vanlig at en MNO også innehar de andre elementene som er nødvendig for å levere tjenester til sluttbruker, slik som kundebehandling, fakturering og markedsføring. I tillegg kan en MNO også selge aksess til nettverkstjenester til grossistpriser til mobile virtuelle nettverksoperatører (MVNO). Det er en regulert plikt i Norge at mobile nettverksoperatører må gi adgang til virtuelle operatører i sine nett. De mobile nettverksoperatørene i Norge er Telenor, Telia (tidligere NetCom) og ICE.

Som egen mobil nettverksoperatør vil Forsvaret kunne ha egne basestasjoner for å bygge ut eller forbedre dekning i enkelte områder. Dette kan gjelde både mobile noder for taktisk bruk og som deler av fast infrastruktur.

4.2 Mobil virtuell nettverksoperatør (MVNO)

En mobil virtuell nettverksoperatør (MVNO) er en tjenestetilbyder som ikke har lisens på aktuelle radiofrekvenser og heller ikke har sin egen basestasjonsinfrastruktur.

Det er mange ulike mobile virtuelle nettverksoperatører. De enkleste tilbyr egentlig bare merkenavnet sitt og i enkelte tilfeller sine distribusjonskanaler. Disse selskapene har lave investeringskostnader og vil på kort tid kunne være i drift. De mest avanserte virtuelle nettverksoperatørene innehar alle funksjoner som er nødvendige for å levere tjenester i mobilnettet bortsett fra den fysiske nettverksinfrastrukturen og lisens på radiofrekvensene. Mange virtuelle nettverksoperatører produserer sine egne UICC.

I Norge fantes det pr januar 2015 følgende mobile virtuelle nettverksoperatører som brukte henholdsvis Telenor og NetCom (nå Telia) sine nett [3]:

- Telenor: Telenor, Djuice, Talkmore, Hello, Xito, Telipol, Phonero, Chilimobil.
- NetCom: NetCom, OneCall, MyCall, Chess, Banzai, Telio, NextGenTel, Tele2.

Forsvaret som egen MVNO vil kunne inngå egne roamingavtaler. Som ikke-kommersiell aktør vil de dermed trolig kunne få økt dekning og robusthet ved å inngå avtale med alle norske MNO-er.

4.3 Roaming

Roaming er når en bruker med kundeforhold tilknyttet et spesifikt mobilnett benytter et mobilnett tilknyttet en annen operatør, vanligvis fordi han oppholder seg utenfor sin operatørs

geografiske dekningsområde. Denne muligheten kan være kommersielt fremforhandlet eller pålagt av myndighetene. I Norge er det Nasjonal kommunikasjonsmyndighet som gir slike retningslinjer. Man kan ha både nasjonal og internasjonal roaming.

Når en brukerenhet roamer vil den alltid benytte HSS i hjemmenettverket, mens E-UTRAN, MME og S-GW alltid vil være i det besøkte/lokale nettverket. P-GW kan derimot være både i hjemmenettverket og det besøkte nettverket. Kommunikasjon med Internett bruker vanligvis P-GW i hjemmenettverket og dette skjer over S8-grensesnittet (se Figur 2.1). Talekommunikasjon vil for eksempel vanligvis gå via P-GW i det besøkte nettverket, og dette skjer da over S5-grensesnittet. Fordelene med dette er at ved talekommunikasjon kan brukeren ta en lokal telefon uten at det må gå via hjemmenettverket og nødsamtaler vil bli håndtert av lokal nødetat. HSS vil indikere om hjemmenettverket vil tillate bruk av lokal P-GW for hver kombinasjon av bruker og pakkedatanettverk.

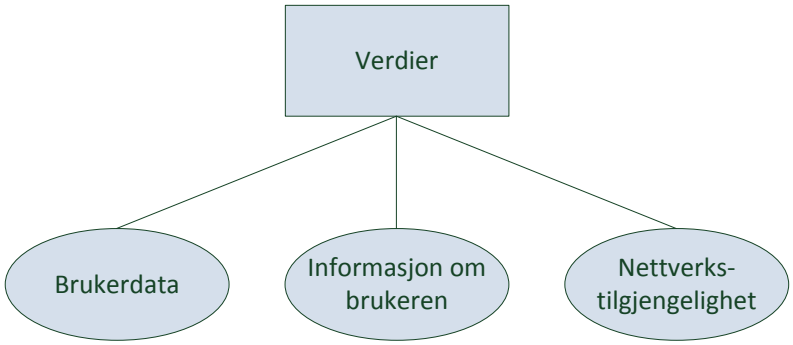
4.4 Brukerenheten

I februar 2016 var det i følge GSA (Global mobile Suppliers Association) 4416 forskjellige LTE brukerenheter på markedet fra 369 leverandører, og av disse var 2706 smarttelefoner [2]. Det er vanskelig å ha tillit til alle disse terminalene, og en mulighet for Forsvaret er å velge ut en eller noen få brukerenheter som tillates brukt.

Brukerenheten kan derfor være en dedikert enhet eid av Forsvaret delt ut til den enkelte, og som ikke brukes privat. Det kan også være restriksjoner knyttet til hvilke applikasjoner det er lov å laste ned. På denne måten vil det være mulig å ha en viss kontroll med brukerenheten. Et annet alternativ er en bring-your-own-device-løsning hvor brukernes egne enheter brukes både privat og militært. Her vil det være vanskeligere å ha samme tillit til brukerenheten. Det går også an å velge en mellomløsning hvor det deles ut en dedikert telefon som også kan brukes privat. Mer informasjon om sårbarheter i brukerenheten finnes i [19].

5 Verdier

For å vurdere LTE for bruk i Forsvaret og hvilke sårbarheter dette innebærer, er det viktig å vite hvilke verdier man ønsker å beskytte. Uavhengig av forretningsmodell, er det behov for å beskytte følgende verdier*: brukerdata, informasjon om brukeren* og *nettverkstilgjengelighet*, som vist i Figur 5.1.



Figur 5.1 Kategorier av verdier som må beskyttes.

5.1 Brukerdata

Data som endebrukeren genererer eller konsumerer kaller vi brukerdata. Dette inkluderer også tale. Brukerdata må beskyttes mot uautorisert innsyn og endring. Det vil si at det er viktig med konfidensialitets- og integritetsbeskyttelse av brukerdataene. Når det gjelder tilgjengelighet til brukerdata håndteres det av nettverkstilgjengeligheten som beskrevet under.

5.2 Informasjon om brukeren

Informasjon om brukeren definerer vi som informasjon om blant annet hvor brukeren er, hvem han er, hvem vedkommende snakker med samt kommunikasjonsmønstre. Dette er informasjon som det kan være ønskelig å dele med sine egne, for eksempel for å få tilgang til lokale tjenester, men som ikke ønskes avslørt overfor fienden eller annen uautorisert tredjepart.

5.3 Nettverkstilgjengelighet

Nettverkstilgjengelighet omfatter tilgjengelighet av nettverkskomponenter og administrativ informasjon som utveksles for å holde nettverkstjenesten operativ. Dette innebærer høy oppetid og beskyttelse mot uautoriserte endringer av nettverket.

Nettverkstilgjengelighet er her kategorisert som en verdi med eget beskyttelsesbehov. Det kan diskuteres hvorvidt beskyttelse av nettverket snarere er en konsekvens av behovet for å beskytte tilgjengelighet av brukertrafikk enn å beskytte nettverket som en egen ressurs. Årsaken til at det her er valgt å skille nettverket ut som en egen ressurs er at det ansees som ønskelig å opprettholde tilgjengeligheten til nettverkstjenesten uavhengig av pågående brukertrafikk, og fordi beskyttelsesbehovet for nettverket er noe annerledes enn for brukerdataene.

6 Trusler og angrepsvektorer

Det finnes mange ulike trusler mot de definerte verdiene. Disse kan rette seg mot brukerenheten, radiogrensesnittet mellom brukerenheten og basestasjonen, LTE-infrastrukturen og i andre tilkoblede nett. I dette kapittelet gis eksempler på trusler, kategorisert etter hvor i nettverksarkitekturen de angriper (angrepsvektor).

6.1 Brukerenheten

Ondsinnet programvare kan installeres på brukerenheten for eksempel under produksjon, ved at noen får fysisk tilgang til brukerenheten eller ved at programvaren overføres via nettet i form av et vedlegg, en nedlastbar applikasjon eller lignende. Dette er det vanskelig å kontrollere, og mulighetene er mange siden brukerenhetene kommer med stadig raskere CPU og større minne. I tillegg kan USIM være kompromittert.

Disse truslene kan potensielt true alle de tre verdiene definert i kapittel 5. Den ondsinnede programvaren kan for eksempel blokkere brukerenheten eller bidra til DOS-angrep (Denial of Service) på infrastrukturkomponenter slik at også nettverkstilgjengeligheten trues. Den kan også true konfidensialitet og integritet av både brukerdata og informasjon om brukeren.

6.2 Radiogrensesnittet

Radiogrensesnittet kan utsettes for både intelligent og uintelligent jamming. Flere artikler trekker frem hvor enkelt det er å jamme LTE [13][14][15], og jammeutstyr kan kjøpes rimelig på nett [16]. Blant annet foretar brukerenheten og basestasjonen en kontinuerlig synkronisering, og ved å forstyrre denne vil det være umulig å sende data. Kommunikasjonen kan også blokkeres på grunn av utilsiktet interferens med andre systemer som Digital TV og S-bånd radar brukt i flytrafikkontroll [13]. Jamming og interferens truer først og fremst nettverkstilgjengeligheten.

Operatøren kan velge å ikke kryptere over radiogrensesnittet, noe som vil kunne true både konfidensialitet og integritet av trafikken.

En annen trussel som potensielt kan true alle verdiene er at det introduseres en falsk basestasjon som brukerne feilaktig kobler seg opp mot. Dette er vanskeligere med LTE enn ved tidligere generasjoner mobiltelefoni, siden LTE har autentisering av basestasjonen. Enklere er det antakelig å benytte en enkel form for IMSI-catcher for å få tilgang til IMSI-ene til brukerne i området. Forespørsel og respons angående IMSI foregår ukryptert.

6.3 Aksessnettverket og kjernenettverket.

Både eNB, MME, S-GW og P-GW er sentrale noder i nettverket. Ved å slå ut disse enten logisk eller fysisk – tilsiktet eller utilsiktet – vil tilgjengeligheten til nettverket være truet. I MME er det i tillegg tilgang til mye informasjon om brukeren i form av IMSI, IMEI, geografisk posisjon,

krypteringsnøkler etc. På tilsvarende måte er det tilgang til brukertrafikk i eNB, S-GW og P-GW. Ved å ha fysisk eller logisk tilgang til infrastrukturkomponentene kan man derfor true alle de tre verdiene vi har definert.

HeNB og WiFi-nettverk er billige og enkle å få tak i og kan brukes for å avlaste LTE-nettverket. De kan dermed fungere som en inngangsport til LTE-nettverket også for angripere. Det vil si at det er langt flere angrepspunkter til LTE-nettverket enn ved tidligere generasjoner av mobiltelefoni, og mange av dem har begrenset fysisk sikring.

6.4 Andre nettverk

Mobiltelefonsystemer baserte seg tidligere på linjesvitsjede nettverk som etter hvert fikk en begrenset datakapasitet. Disse var enklere å kontrollere for operatørene, fordi de hadde enklere signalering og færre forbindelser til omverdenen. I LTE-nettverk er det IP ende-til-ende, hvor brukerenheten har sømløs roaming. Dette medfører at operatørene deler de samme truslene siden deres respektive infrastrukturer og tjenester er sammenkoblet til ett aggregert tjenestenettverk. Slike distribuerte nettverk og åpne arkitekturer medfører at sårbarheter på en enhet eller ett grensesnitt kan være en inngangsport for angripere som ønsker å kompromittere LTE-nettverket. Trusler her kan potensielt true alle de tre verdiene.

I februar 2016 var Telenor sitt nett nede i over 3 timer. Først og fremst var det taletrafikken som ble rammet, men også noe av SMS-trafikken. Det viste seg at feilen skyldtes uvanlig signaleringstrafikk inn i Telenor sitt nett fra en annen internasjonal operatør og inneholdt meldingstyper som forekommer svært sjelden [17]. Dette gjaldt antakelig linjesvitsjet tale (2G/3G-trafikk) men viser allikevel at sårbarheten øker når nett knyttes sammen.

7 Sårbarheter ved ulike forretningsmodeller

Forretningsmodellene gir ulike sårbarheter. Vi har i det følgende sett på sårbarheter knyttet til hvilke komponenter i LTE-nettverket Forsvaret har kontroll på ved ulike forretningsmodeller. Med kontroll menes at komponenten anskaffes, brukes og driftes av Forsvaret eller andre med tilsvarende tillit.

Ideelt sett burde man også ha kontroll på produksjonen. Vi har valgt å ikke ta hensyn til dette, siden noe av hensikten ved å bruke LTE i Forsvaret nettopp er å kunne bruke kommersiell hyllevare. Man bør likevel være klar over at kommersiell hyllevare kan inneholde innlagte sårbarheter som vil kunne utgjøre en trussel.

Vurderingene er basert på en tillitsmodell som i prinsippet skiller mellom to hovedkategorier aktører: «Egne med høy tillit» og «Eksterne med lavere tillit». Den første gruppen omfatter

typisk både Forsvarets eget personell, samt andre aktører med nasjonal sikkerhetsklarering og nødvendig autorisasjon. Den inkluderer både legitime brukere og administratorer av systemet. Den andre gruppen omfatter eksterne aktører som ikke nødvendigvis er eller kan bli klarert og autorisert. Antakelsen er at det i denne siste gruppen kan finnes aktører som ikke opptrer vennligsinnet i enhver situasjon, og dermed kan true en eller flere av verdiene. Innenfor hver hovedkategori er det mulig å definere flere undergrupper med ulik grad av tillit, men vurderingen har vært at denne forenklede tillitsmodellen er tilstrekkelig for en overordet forståelse av de generiske sårbarhetene i LTE.

Vi har valgt fire ulike forretningsmodeller i et forsøk på å spenne ut rommet av løsninger for Forsvaret. Disse er:

- Forsvaret som egen MNO
- Forsvaret som egen MVNO – kontroll på USIM og hele EPC
- Forsvaret som egen MVNO – kontroll på USIM og HSS
- Forsvaret som kunde hos en MNO

Dette kapitlet søker å gi en overordnet oversikt over hvilke verdier som er truet ved disse ulike forretningsmodellene. Dette visualiseres ved hjelp av figurer hvor de ulike komponentene i infrastrukturen fargekodes utfra om Forsvaret har kontroll med komponenten eller ikke. Grønn indikerer kontroll over komponenten både under anskaffelse og drift. Gul indikerer delvis kontroll, mens rødt betyr at denne komponenten er utenfor Forsvarets kontroll ved anskaffelse og/eller drift.

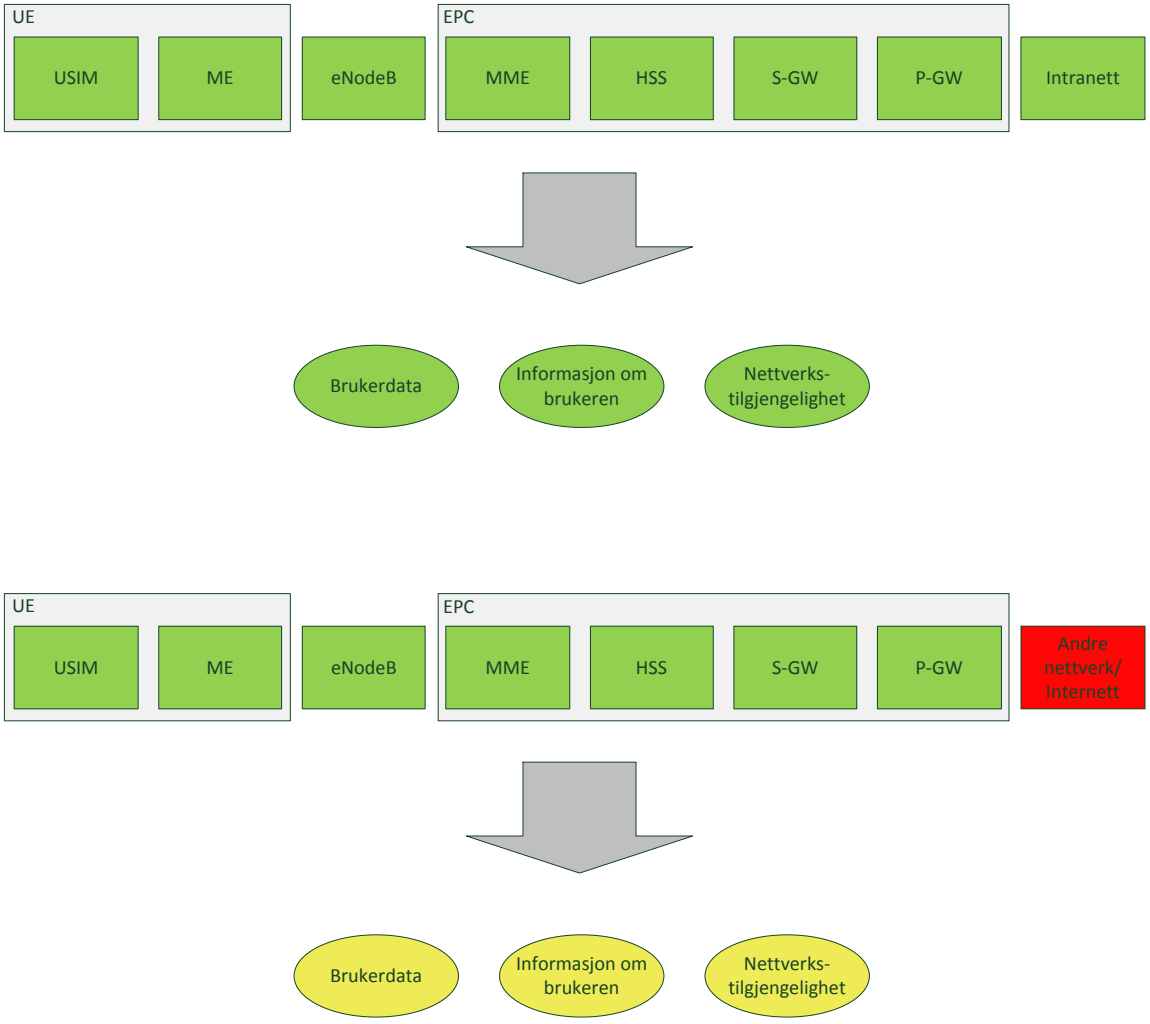
Verdiene, for eksempel brukerdataene, blir også fargesatt med de samme fargene. Her betyr grønn at verdien er beskyttet ved at Forsvaret har kontroll på de komponentene som verdien er avhengig av. Gul farge indikerer delvis beskyttet, mens rødt betyr at verdien er truet.

7.1 Forsvaret som egen MNO

I denne forretningsmodellen er Forsvaret egen operatør med god kontroll på alle deler av infrastrukturen, også under anskaffelse. Det er heller ikke noen andre virtuelle operatører i Forsvarets nett. Dette er illustrert i Figur 7.1. Alle komponentene i E-UTRAN og EPC er under kontroll av Forsvaret eller annet personell med tilsvarende tillit og dermed grønne. Det er forutsatt at ME er en dedikert enhet utdelt av Forsvaret, og kun til militært bruk. Denne er dermed også grønn. Det samme er USIM som blir utstedt av Forsvaret.

I denne forretningsmodellen har vi tatt med to tilfeller når det gjelder kobling til andre nett. I det første tilfellet har vi ingen kobling mot Internett eller roamingavtaler med andre operatører, kun et Intranett kontrollert av Forsvaret. I det andre tilfellet har Forsvaret roamingavtaler med andre operatører og er tilkoblet Internett.

I det første tilfellet vil man stå igjen med LTE sine generelle sårbarheter som dårlig jammeresistens og sårbarheter knyttet til det å benytte en infrastrukturbasert kommunikasjonsteknologi. Gitt at Forsvaret bruker LTE-teknologi, kan vi si at denne modellen gir god kontroll på brukerdata og god kontroll på informasjon om brukeren. Siden nettverkstilgjengeligheten er så god som den kan bli med kommersiell LTE-teknologi er den farget grønn øverst i Figur 7.1.



Figur 7.1 Illustrasjon som viser hvilke deler av infrastrukturen Forsvaret har kontroll med og hvilke verdier som er beskyttet i forretningsmodellen hvor Forsvaret er en egen MNO. Den øverste figuren viser tilfellet uten roamingavtaler eller kobling til Internett, mens den nederste figuren viser tilfellet med dette.

Med roamingavtaler og kobling til Internett vil man introdusere sårbarheter. Så lenge man kommuniserer innenfor Forsvarets nett vil vi likevel si at Forsvaret har god kontroll, selv om den ikke er like god som i det første tilfellet. Hvis en bruker derimot benytter roaming, vil kontroll med alle verdiene mistes fordi det benyttes infrastrukturkomponenter i det besøkte nettverket. Dette kan sammenlignes med forretningsmodellen hvor man hverken har kontroll med eNB eller EPC. Derfor blir verdiene nederst i Figur 7.1 gule i dette tilfellet.

I utlandet vil Forsvaret selvfølgelig ikke ha noen fordeler av å ha egne basestasjoner i Norge. I internasjonale operasjoner må Forsvaret enten ha med seg egne mobile basestasjonsnoder, eller leie dette av lokale operatører eller andre med tilgang til basestasjoner i operasjonsområdet. I prinsippet kan Forsvaret fremdeles bruke sin egen EPC. Ved reiser i utlandet kan Forsvarets ansatte enten bruke andre USIM, eller Forsvaret kan inngå roamingavtaler med operatører i utlandet på samme måte som andre kommersielle operatører gjør. Dette går også an å gjøre ved internasjonale operasjoner, men sårbarhetene blir da omtrent som i forretningsmodellen beskrevet i delkapittel 7.3.

En viktig kommentar til denne forretningsmodellen er at det er svært dyrt å bygge ut basestasjonsinfrastruktur i hele landet. Det er også usikkert om Forsvaret får tilgang til LTE-frekvenser. Hvis Forsvaret må bruke frekvenser som ikke ligger i LTE-standarden, må både basestasjoner og brukerenheter tilpasses disse frekvensene, og noe av den økonomiske gevinsten av å bruke kommersiell teknologi forsvinner.

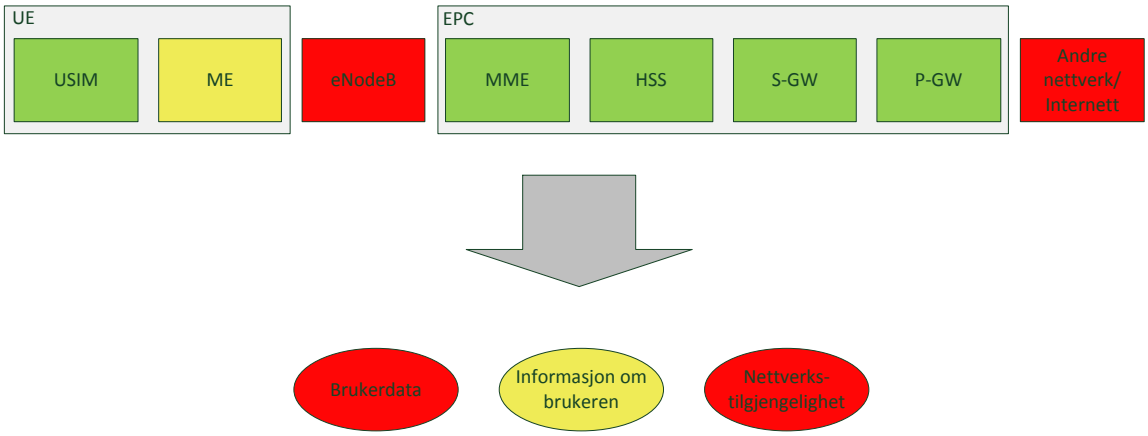
7.2 Forsvaret som egen MVNO – kontroll på USIM og hele EPC

Med denne forretningsmodellen vil Forsvaret ikke ha egne frekvenser og egne basestasjoner, men leie dette av en mobiloperatør. Resten av infrastrukturen vil Forsvaret eie og drifte selv. Dette er illustrert i Figur 7.2, og her er derfor eNB rød. Vi har også forutsatt at det er roaming og kobling til Internett. Brukerenheten er her gul, fordi vi har forutsatt at det blir levert dedikerte brukerenheter, men som også kan brukes privat. Forsvaret har derfor bare delvis kontroll på enhetene.

I tillegg til sårbarhetene diskutert i forretningsmodellen over, er det sårbarheter knyttet til det å ikke ha kontroll over basestasjonene, noe som blant annet gjør det vanskelig å beskytte nettverkstilgjengeligheten. I tillegg termineres krypteringen av brukertrafikken i basestasjonene som beskrevet i kapittel 3. Brukerdataene vil derfor både kunne avleses i basestasjonen, samt at den kan endres, stoppes eller det kan bli sendt falske data. Samtidig vil en del av informasjonen om brukeren som for eksempel omtrent hvor han befinner seg være tilgjengelig for basestasjonen. At brukerenheten er gul og vi ikke har kontroll på denne, medfører at alle verdiene potensielt kan være truet som beskrevet i avsnitt 6.1.

Basert på disse sårbarhetene er både brukerdata og nettverkstilgjengeligheten rød med denne forretningsmodellen. Videre er informasjon om brukeren gul ut fra diskusjonen over, samt at mye av kontrolltrafikken kan gå kryptert mellom basestasjonen og MME (se avsnitt 3.2).

Ved internasjonale operasjoner kan det være mulig å gjøre en MVNO-avtale for å kunne bruke andre operatørers eNB, men egen EPC. Ved enkeltpersoner som er på reise er det mest hensiktsmessig med vanlig roaming, eventuelt å bruke et annet eventuelt lokalt USIM.



Figur 7.2 Illustrasjon som viser hvilke deler av infrastrukturen Forsvaret har kontroll med og hvilke verdier som er beskyttet i forretningsmodellen hvor Forsvaret er en egen MVNO som leier basestasjoner av en kommersiell operatør. Resten av infratrukturen har Forsvaret kontroll på.

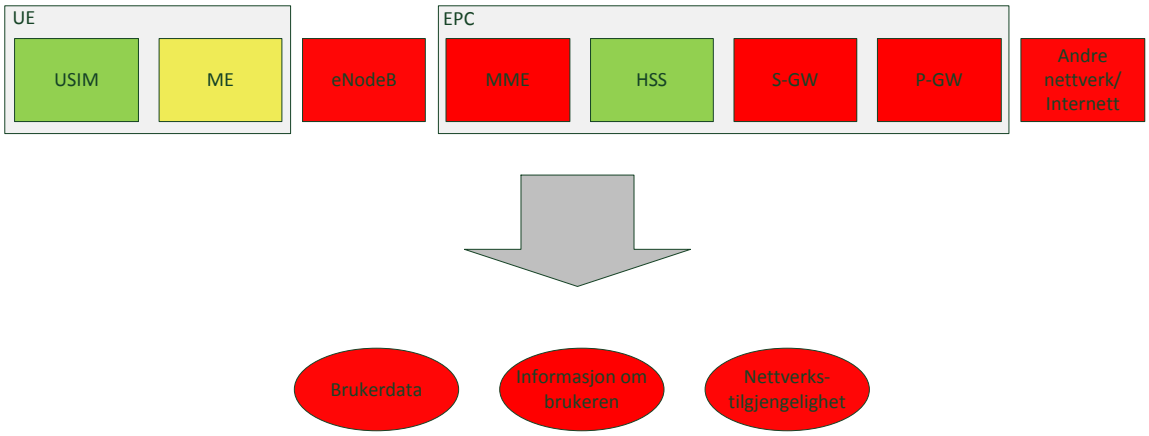
7.3 Forsvaret som egen MVNO – kontroll på USIM og HSS

Ved denne forretningsmodellen er Forsvaret en MVNO som leier hele infrastrukturen bortsett fra HSS og USIM. På denne måten har Forsvaret dermed kontroll på alle *LTE K* nøklene, selv om det meste av infrastrukturen leies. Denne forretningsmodellen er vist i Figur 7.3, der bare USIM og HSS er grønne. På samme måte som i forrige forretningsmodell er brukerenheten en dedikert enhet utdelt av Forsvaret, men som også brukes privat. Den er derfor gul.

Denne forretningsmodellen har alle sårbarhetene fra forrige modell. I tillegg vil Forsvaret miste kontrollen på informasjonen om brukeren, da krypteringen av brukertrafikken termineres i MME som i denne modellen er en komponent utenfor Forsvarets kontroll. Selv om Forsvaret har kontroll på nøkkelen *LTE K*, vil de ikke ha kontroll på de utledede nøklene brukt for å beskytte brukertrafikken og kontrolltrafikken. De vil også miste kontrollen på infrastrukturkomponenter hvor denne trafikken går åpen. På bakgrunn av dette har brukertrafikken og informasjon om brukeren blitt farget rød.

Ved å leie all infrastruktur bortsett fra HSS, øker sårbarheten knyttet til nettverkstilgjengeligheten. Man har ikke kontroll på mange av de kritiske nodene i nettverket, og tilgjengeligheten blir mer sårbar enn de tidligere forretningsmodellene. Nettverkstilgjengeligheten er derfor også i denne modellen rød.

Ved denne forretningsmodellen vil det ikke være noen nevneverdig forskjell i sårbarhet med og uten roaming, verken på reise eller i internasjonale operasjoner.



Figur 7.3 Illustrasjon som viser hvilke deler av infrastrukturen Forsvaret har kontroll med og hvilke verdier som er beskyttet i forretningsmodellen hvor Forsvaret er en egen MVNO som leier basestasjoner og store deler av EPC fra en MNO. Forsvaret har kontroll på USIM og HSS.

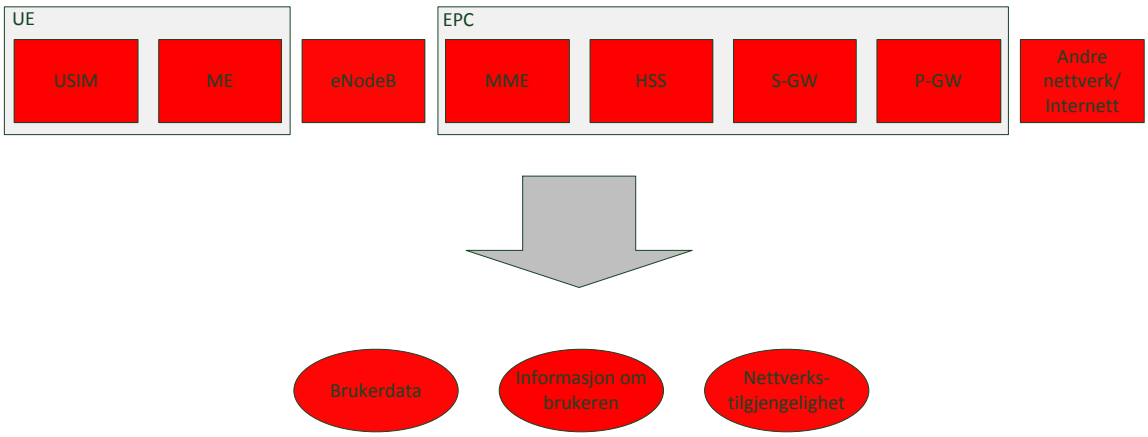
7.4 Forsvaret er kunde hos en MNO

Ved denne forretningsmodellen er Forsvaret kunde hos en kommersiell mobiloperatør.

Alle sårbarhetene diskutert i forrige forretningsmodell gjelder også her, i tillegg til at Forsvaret ikke har kontroll med nøkkelen *LTE K*. En utro tjener i selskapet kan for eksempel hente ut en eller flere nøkler, som kan «selges» og brukes til passiv avlytting også av andre.

Denne forretningsmodellen er illustrert i Figur 7.4. I denne modellen har vi forutsatt en bring-your-own-device-løsning når det gjelder brukerenheten. Det ville ikke gjort noen vesentlig forskjell for vurderingen om man i stedet hadde hatt en dedikert brukerenhet. Ved denne løsningen er alle de sentrale komponentene i nettverket røde.

I forrige forretningsmodell var nettverket så sårbart at vi vurderte alle verdiene til å være røde. Sikkerheten har her blitt enda dårligere, og verdiene er derfor røde også i denne modellen.



Figur 7.4 Illustrasjon som viser hvilke deler av infrastrukturen Forsvaret har kontroll med og hvilke verdier som er beskyttet i forretningsmodellen hvor Forsvaret er kunde hos en MNO.

Denne forretningsmodellen likner mest på den Forsvaret bruker i dag. Forskjellen er at Forvaret i dag er kunde hos en MVNO som leier infrastruktur. Figur 7.4 gjelder også for dagens løsning.

8 Diskusjon og oppsummering

Gjennomgangen av sårbarhetene i de ulike forretningsmodellene for bruk av LTE i Forsvaret viser ikke uventet at Forsvaret som egen mobil nettverksoperatør uten roaming eller tilknytning til andre nett gir lavest sårbarhet. Antakelig er dette en urealistisk modell fordi det er kostnadskrevende å bygge et landsdekkende LTE-nettverk med basestasjoner. Forsvaret vil med denne modellen ha behov for egne frekvenser som alternativt kunne ha blitt solgt til kommersielle operatører og gitt statlige inntekter. Uten roamingavtaler eller kobling til Internett vil også tjenestetilbudet bli svekket. Det er imidlertid mer realistisk at Forsvaret kan benytte mobile eNB-er og en tilsvarende forretningsmodell for å gi områdedekning i en taktisk operasjon. Utfordringen her vil trolig være tilgang til frekvenser, eller snarere mulig interferens med andre aktører som opererer i samme frekvensområde.

Gjennomgangen viser også at det å ikke ha kontroll på eNB gir store konsekvenser. Ved en forretningsmodell hvor Forsvaret leier basestasjoner, men har kontroll på resten av infrastrukturen, vil først og fremst nettverkstilgjengeligheten være truet. Å ha tilgang til basestasjoner er helt essensielt, og det er viktig å kunne ha tillit til at man har denne tilgangen også i en mer spent sikkerhetspolitisk situasjon. Konfidensialitet og integritet til brukertrafikk

vil også være truet, siden krypteringen termineres i basestasjonen. Integritet er trolig ikke et stort problem for tale, men for data kan dette være kritisk. Det er viktig å kunne stole på at de data man mottar er korrekt. Noe informasjon om brukerene vil også være tilgjengelig, som omtrentlig geografisk posisjon og hvem som kommuniserer med hverandre.

Forskjellene på de to siste forretningsmodellene hvor Forsvaret er en virtuell mobiloperatør med kontroll på USIM og HSS eller er en ordinær bedriftskunde hos en kommersiell operatør, er derimot ikke så stor. Andre har uansett tilgang til både kontroll- og brukertrafikken siden de har tilgang til infrastrukturkomponentene. En viktig observasjon er at samme situasjon gjelder ved roaming i alle de fire forretningsmodellene. Brukeren som roamer benytter da infrastrukturkomponenter som Forsvaret ikke har kontroll på.

Ingen av forretningsmodellene diskutert her representerer høyere sårbarhet enn hva man allerede finner i dagens mobilkommunikasjonsløsing hvor Forsvaret er kunde hos en MVNO. Rapporten tar ikke stilling til om sikkerheten i dagens mobiltelefonibruk i Forsvaret er tilfredsstillende. Som en ren erstatter av dagens mobiltelefoniløsning vil forretningsmodellene diskutert her kunne gi lavere sårbarhet, men også forventet framtidig bruksområde bør tas med i betraktningen. Anvendelsesområder for LTE i Forsvaret er tema for diskusjon, men det blir beskrevet intensjoner om operativ anvendelse utover dagens bruk av mobiltelefoni. Når anvendelsesområdet utvides, vil det kreves en nærmere analyse for å kunne avgjøre hvordan sårbarheten totalt sett påvirkes i forhold til nåsituasjonen. Det vil avhenge av blant annet scenario og hvilket kommunikasjonsmiddel LTE eventuelt erstatter.

De generiske sårbarhetene til LTE, som lav jammeresistens og avhengigheten av infrastruktur, gjelder uavhengig av forretningsmodell. Eksempelvis er LTE-nettverket sårbart for angrep som rammer strømforsyningen.

Rapporten forutsetter bruk av kommersielt utstyr, og vurderingen av sårbarhet tar utgangspunkt i at man kan stole på slikt utstyr. Dette er antakelig en sterk forenkling da det er vanskelig å ha full tillit til kommersielt utstyr. Uten tillit til infrastrukturkomponentene og brukerenhetene, vil alle verdiene i samtlige forretningsmodeller være truet, og det ville vært vanskelig å få frem forskjellene på de ulike forretningsmodellene.

I rapporten gjøres videre forenklinger ved å bruke tre farger for å indikere sårbarhetsnivå. Dette er gjort for å få frem det store bildet og å gi en overordnet oversikt over forskjellene og likhetene mellom forretningsmodellene. Ulempen er at enkelte nyanser blir maskert bort.

Rapporten har avdekket flere områder som bør studeres nærmere. Ett naturlig tema er anvendelsesområder for LTE i militær sammenheng. Infrastrukturbaserte systemer som LTE er mer sårbare enn tradisjonelle autonome militære radiosystemer. Dette kan ha betydning for hvor og hvordan Forsvaret bør benytte LTE. Innenfor anvendelsesområdet for LTE er det videre naturlig å studere hvordan de ulike verdiene kan sikres bedre.

3GPPs standardisering av device-to-device-funksjonalitet gjør LTE mindre avhengig av infrastrukturkomponenter over korte avstander. Det har også kommet militært tilpassede LTE-infrastrukturkomponenter, og kanskje vil noe av dette ha bedre innebygget sikkerhet. Ulempen er at dette kan være dyrere enn rent sivilt utstyr. For sikring av brukerdata kan det være aktuelt å benytte ende-til-ende applikasjonslagskryptering for eksempel med SCIP (Secure Communication Interoperabiltiy Protocol). For gradert bruk vil det også være behov for å studere hvordan kommersielle brukerterminaler kan sertifiseres og sikres. Dette gjelder uavhengig av hvilken forretningsmodell som velges.

I hvilken grad informasjon om brukere kan skjules for uautoriserte vil i stor grad avhenge av valgt forretningsmodell. En mulighet kan være å benytte mange IMSIer for hver bruker. Hvor effektivt dette er, avhenger blant annet av hvilke komponenter i infrastrukturen Forsvaret har kontroll over.

Det er mange måter å sikre nettverkstilgjengeligheten bedre på innenfor hver forretningsmodell. Noen aktuelle løsninger kan være å ha avtaler med flere uavhengige operatører, sterkere sikkerhetskrav til infrastrukturkomponenter og programvare i kjernenettet, egne mobile basestasjoner – med eller uten egen innebygd EPC, mer avansert nettovervåkning, bedre beskyttelse av strømnettet med mer. Det er også viktig å skaffe en god oversikt over sårbarheter og angrepsvektorer innen aksess- og kjernenettverket for å finne måter å sikre tilgjengeligheten bedre.

Effekten av disse tiltakene må analyseres nærmere, og kostnadene må vurderes mot nytte. For eksempel vil mobile basestasjoner bare hjelpe på tilgjengeligheten i et begrenset geografisk område, mens ende-til-ende kryptering fremdeles vil gi muligheter for trafikkanalyse siden adresseinformasjon ikke vil være skjult.

Kort oppsummert har alle forretningsmodellene sine styrker og svakheter. I hvilken grad Forsvaret har kontroll over eNB har stor innvirkning på grad av sårbarhet. Det er flere punkter som bør avklares før Forsvaret eventuelt velger sin forretningsmodell. Ikke minst hvem i Forsvaret som skal bruke LTE og hvordan det skal brukes. Forhåpentligvis kan denne rapporten tjene som et rammeverk for videre diskusjoner knyttet til sikkerhet og sårbarhet ved bruk av LTE i Forsvaret.

Forkortelser

AES	Advanced Encryption Standard
AKA	Authentication and Key Agreement
AS	Access Stratum
ASME	Access Security Management Entity
CPU	Central Processing Unit
DOS	Denial of Service
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
eNB	Evolved Node B
EPC	Evolved Packet Core
EPS	Evolved Packet System
ESP	Encapsulating Security Payload
HSS	Home Subscriber Server
IKE	Internet Key Exchange
IMEI	International Mobile Equipment Identity
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
LTE	Long Term Evolution
ME	Mobile Equipment
MME	Mobility Management Entity
MNO	Mobil Nettverksoperatør
MVNO	Mobil Virtuell Nettverksoperatør

NAS	Non Access Stratum
PDN	Packet Data Network
P-GW	PDN Gateway
RRC	Radio Resource Control
SCIP	Secure Communication Interoperability Protocol
S-GW	Serving Gateway
SMS	Short Message Service
UE	User Equipment
UICC	Universal Integrated Circuit Card
UMTS	Universal Mobile Telecommunications System
USIM	Universal Subscriber Identity Module

Referanser

[1] http://www.ovum.com/press_releases/global-lte-subscriptions-pass-1-billion/

[2] REPORT: Status of the LTE Ecosystem, GSA, February 11, 2016.

[3] http://www.dinside.no/932319/hvilke-operatorer-bruker-telenors-og-netcoms-nett

[4] www.3gpp.org/technologies

[5] Universal Mobile Telecommunications System (UMTS); LTE; Proximity-based Services (ProSe); Security aspects, 3GPP TS 33.303 version 13.2.0 Release 13, ETSI TS 133 303, Jan, 2016.

[6] Response to Questions and issues as a basis for discussion on Multi-mode UEs, T3-000298, TSG T3, 3GPP TSG-T3 (USIM) Meeting #14, Visby Sweden, May, 2000.

[7] S. Kent and K. Seo, Security Architecture for the Internet Protocol, RFC 4301, IETF, Desember 2005.

[8] S. Kent, IP Encapsulating Security Payload (ESP), RFC 4303, IETF, Desember 2005.

[9] C. Kaufman (Ed.), Internet Key Exchange (IKEv2) Protocol, RFC 4306, Desember 2005.

[10] Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; 3G security; Network Domain Security (NDS)M IP network layer security, 3GPP TD 33.210 version 12.2.0 Release 12, ETSI TS 133 210 V12.2.0 (214-10)

[11] Huawei LTE Security Solution, Whitepaper, Draft B, Huawei Technologies Co. Ltd, 2016-03-07.

[12] Security of Home Node B (HNB) / Home evolved Node B (HeNB), 3GPP TS 33.320 version 13.0.0, Release 13, Jan, 2016.

[13] N. Mahmud, Vulnerabilities of LTE and LTE-Advanced Communication, White Paper, Rohde & Schwarz, 2014.

[14] M. Lichtman, J. H. Reed, T.C. Clancy, and M. Norton, Vulnerability of LTE to Hostile Interference, IEEE Global Conference on Signals and Information Processing (GlobalSIP), 2013.

[15] R. P. Jover, J. Lackey, and A. Raghavan, Enhancing the security of LTE networks against jamming attacks, EURASIP Journal on Information Security, Springer, 2014.

[16] http://www.jammerfromchina.com/categories/4G%7B47%7DLoJack%7B47%7DXM_Jammers/

[17] https://www.telenor.no/om/pressesenter

[18] C. Cox, An Introduction to LTE, LTE, LTE-Advanced, SAE, VoLTE and 4G Mobile Communications, Second Edition, John Wiley & Sons Ltd, 2014.

[19] F. Mancini, Modern mobile platforms from a security perspective, FFI-rapport 16/00319, 2016.

About FFI

The Norwegian Defence Research Establishment (FFI) was founded 11th of April 1946. It is organised as an administrative agency subordinate to the Ministry of Defence.

FFI's MISSION

FFI is the prime institution responsible for defence related research in Norway. Its principal mission is to carry out research and development to meet the requirements of the Armed Forces. FFI has the role of chief adviser to the political and military leadership. In particular, the institute shall focus on aspects of the development in science and technology that can influence our security policy or defence planning.

FFI's VISION

FFI turns knowledge and ideas into an efficient defence.

FFI's CHARACTERISTICS

Creative, daring, broad-minded and responsible.

Om FFI

Forsvarets forskningsinstitutt ble etablert 11. april 1946. Instituttet er organisert som et forvaltningsorgan med særskilte fullmakter underlagt Forsvarsdepartementet.

FFIs FORMÅL

Forsvarets forskningsinstitutt er Forsvarets sentrale forskningsinstitusjon og har som formål å drive forskning og utvikling for Forsvarets behov. Videre er FFI rådgiver overfor Forsvarets strategiske ledelse. Spesielt skal instituttet følge opp trekk ved vitenskapelig og militærteknisk utvikling som kan påvirke forutsetningene for sikkerhetspolitikken eller forsvarsplanleggingen.

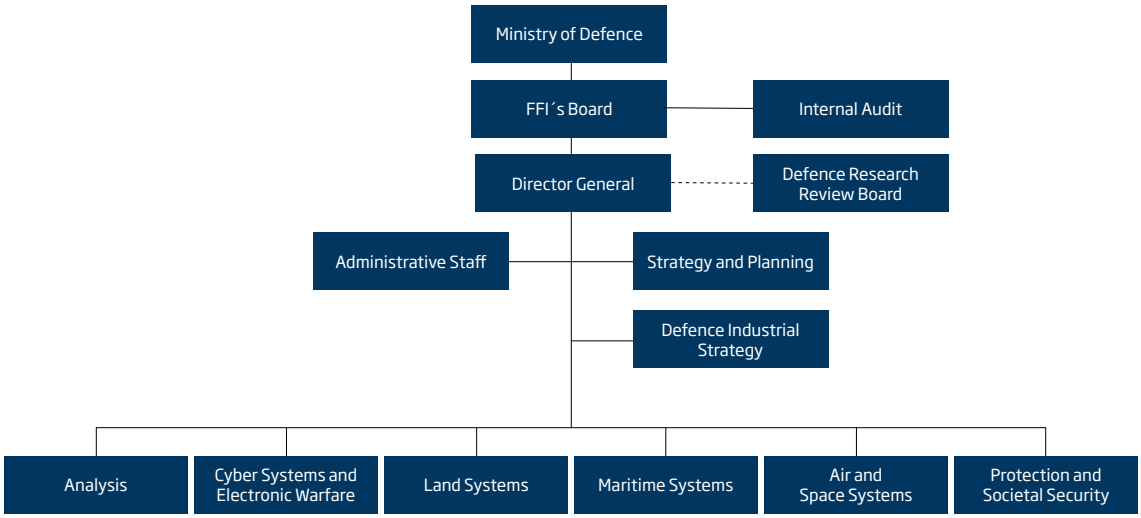
FFIs VISJON

FFI gjør kunnskap og ideer til et effektivt forsvar.

FFIs VERDIER

Skapende, drivende, vidsynt og ansvarlig.

FFI's organisation



Forsvarets forskningsinstitutt
Postboks 25
2027 Kjeller

Besøksadresse:
Instituttveien 20
2007 Kjeller

Telefon: 63 80 70 00
Telefaks: 63 80 71 15
Epost: ffi@ffi.no

Norwegian Defence Research Establishment (FFI)
P.O. Box 25
NO-2027 Kjeller

Office address:
Instituttveien 20
N-2007 Kjeller

Telephone: +47 63 80 70 00
Telefax: +47 63 80 71 15
Email: ffi@ffi.no

FFI Forsvarets forskningsinstitutt
Norwegian Defence Research Establishment