NTNU
Det skapende universitet

Prinsipper for bruk av krypteringsnøkler for ERTMS i Norge

Henning Andenæs

Master i veg og jernbane
Innlevert: mai 2015
Hovedveileder: Tor Engebret Onshus, ITK

Norges teknisk-naturvitenskapelige universitet
Institutt for teknisk kybernetikk

Forord

Denne masteroppgaven er skrevet som en del av Erfarings basert master som er et samarbeid mellom Jernbaneverket og NTNU høsten 2014 og våren 2015. Under arbeidet med oppgaven fant jeg ut at det ikke var enkelt å få fagpersoner eller fagmiljøer i tale når det gjelder kryptering og sikkerhet i forbindelse med innføringen av ERTMS. Dette har ført til at jeg har brukt mange timer på å lese relevant og irrelevant litteratur, samtidig som jeg iherdig har prøvd å komme i kontakt med nøkkelpersoner innen dette fagområdet. Noe jeg til slutt lykkes med, og dermed kunne faglig forsvare min trusselvurdering og analyser. Jeg håper denne oppgaven vil kunne hjelpe Jernbaneverket med sitt viktige arbeide med implementering av ERTMS i Norge. Slik at Jernbaneverket kan innføre ERTMS riktig med hensyn til organisering internt og sikre ERTMS installasjonene på en riktig måte for å unngå «hacking» av systemene. Oppgaven beskriver hva en slik innføring kan ha å si for sikkerheten ved togframføring, hvem som kan tenkes å angripe ERTMS og hvilke mekanismer en kan benytte for å sikre systemet mot angripere eller farer. Jeg vil takke følgende personer:

- Min ektefelle som har støtte meg, oppmuntret, lest korrektur oppgaven og har hatt troen på meg.
- Hovedveileder Professor Tor Onshus ved NTNU, for din hjelp som du utfører med veldig god faglig tyngde.
- Lokaleveileder ved Jernbaneverket Senioringeniør John Price, for svært god ERTMS faglig rettledning og at jeg fikk bruke disponere noe av din tid i en hektisk hverdag ved Jernbaneverket.
- Lederen av KMC i Jernbaneverket Senioringeniør Roy Seland for din tid og at du satte meg i kontakt med fagpersoner i Danmark og Sverige.
- Leder ved Signaltjenester i Jernbaneverket Sjefingeniør Øystein Larsen, tusen takk for muligheten du ga meg til å fordype meg i en oppgave og et aktuelt fagfelt innen signal.
- Alle mine medstudenter fra Jernbaneverket for tre hyggelige og morsomme år. Uten dere med faglig utveksling på tvers av fag og samarbeid hadde dette ikke vært mulig

Tusen takk til alle dere som har vært med og bidratt på en eller annen måte.

Oslo, 14 mai 2015, Henning Andenæs

Oppgavetekst

Prinsipper for bruk av krypteringsnøkler for ERTMS i Norge

ERTMS (European Rail Traffic Management System) er det nye felles signalanlegget for EU og Europa. ERTMS består av to deler: ETCS (European Train Control System- europeisk tog styringssystem og GSM-R (Mobiltelefoni spesielt for jernbane). ERTMS innføres for å forenkle tog trafikk mellom landegrenser og fornye det 50 år gamle eksisterende signalanlegget. Hovedårsaken for at Norge innfører ERTMS, er å fornye signalanlegg til noe mer moderne enn gammel rele teknologi. I dag er det over 24 forskjellige signalsystemer i Europa.

I forbindelse med at Jernbaneverket skal starte en pilot med ERTMS på Østrelinje fra 2015, trenger de et rammeverk for krypteringsnøkkel håndtering. Prosjektet har ikke kommet fram til en nøkkel håndterings system/prinsipper for krypteringsnøkkel for kommunikasjonen mellom tog (Ombordutrustning) og togradioblokksenter (RBC). Denne kommunikasjon går via GSM-R som tidligere nevnt er en del av ERTMS.

.

Oppgaven skal omhandle følgende temaer: Generelt trusselbilde for jernbanen i Norge, Faktorer som påvirker nøkkelhåndtering Risiko ved at nøkkel blir kompromittert eller falsk kjør signal og prosedyrer, risiko ved feil nøkkelhåndtering, risiko for kryptografiske angrep, antall nøkler og hvor ofte de må byttes og erfaringer og praksis fra andre land.

Oppgaven skal gi en anbefaling for nøkkelhåndtering og bruk i forbindelse med ERTMS i Norge og hvordan dette kan implementeres.

Oppgaven gitt: September 2014

Hovedveileder: Tor Onshus, Institutt for Teknisk kybernetikk, NTNU

Lokalveileder: John Price, Hastighetsovervåkning infrastruktur/prosjekter, Jernbaneverket

Sammendrag og konklusjon

I forbindelse med innføring av det nye signalsystemet ERTMS (European Rail Traffic Management System) i Norge, må det etableres en organisasjon for kryptering og krypteringsnøkkelhåndtering i Jernbaneverket. I ERTMS standarden er nøkkelhåndtering kun mulig ved offline distribusjon av nøkler i dag. Dette medfører at mye av arbeidet ved nøkkelhåndtering gjøres manuelt. For å vite mere om hvordan dette bør gjennomføres har jeg sett på trusselbilde mot jernbanen i Norge. Utfra de funn som er oppdaget er det videre arbeidet med faktorer som kan påvirke nøkkelhåndteringen. Faktorene er delt opp i ytre og indre faktorer, der ytre er faktorer som ikke Jernbaneverket kan påvirke. De indrefaktorene er faktorer som Jernbaneverket kan gjøre noe med ved fysisk sikring og organisering av KMC (Key Management Center). I samarbeidet med ERTMS prosjektet er det gjennomført en analyse som er et vedlegg. I tillegg til dette er det gjennomført en mer utfyllende analyse av hvilke farer eller trusler Jernbaneverket står ovenfor. Den største utfordringen med arbeidet har vært å komme i kontakt med personer med kompetanse på dette, å få uttalelser eller informasjon fra fagmiljøer som for eksempel PST(Politiets Sikkerhets Tjeneste) og NSM (Nasjonal Sikkerhets Myndighet). Denne oppgaven ser også på hvordan nøkkelhåndtering er planlagt gjennomført i Sverige og Danmark.

På bakgrunn av innsamlet materiale foreslås flere tiltak og anbefalinger til Jernbaneverket. Det viktigste tiltaket er å etablere en god kultur for sikkerhet som et mål for hele organisasjonen, inkludert ledelsen. Funnene som er gjort gjennom arbeidet med oppgaven tyder på at dette er en oppgave som Jernbaneverket ikke har vært villig til å ta, resultatet blir da at det ikke blir tatt grep i organisering og fysisk sikring av kritiske systemer eller personell. Jernbaneverket anbefales å starte arbeidet med fysisk sikring og etablering av en god sikkerhetskultur i sin organisasjon. Jernbaneverket bør sikkerhetsklarer ansatte som arbeider i KMC eller på annen måte jobber med nøkkelhåndtering med klarering «HEMMELIG» med påfølgende kurs. Det bør også utnevnes en sikkerhetsleder for KMC. Sikkerhetsleder gjennomfører en årlig sikkerhetssamtale med alle ansatte ved KMC engang i året. Jernbaneverket anbefalelses videre å følge de krav NSM setter for krypteringsalgoritmer. Jernbaneverket bør også være en pådriver overfor ERA (European Railway Agency) for å få implementert AES og en standard for online nøkkelhåndtering i ERTMS. Dette i tett samarbeid med Danmark som planlegger online nøkkelhåndtering. Det anbefalelses å ivareta sikkerhetsarbeidet i kontrakten med leverandør. Der ansvarsområde angående sikkerhet og

ansvar for sikkerheten til enkelte komponenter tydelig gjøres, dette anses som den viktigste delen i forbindelse med nøkkelhåndtering der leverandør også er involvert.

Når det gjelder levetid for de ulike krypteringsnøklene tar jeg utgangspunkt i OBU (Ombord Utrustningen) til togene, da denne delen er dårligst sikret å fare for nøkkel kompromittering er størst. GCD (Generic Crypto Device) som er en del av OBU'en har en levetid på maksimalt fem år på grunn av backup batterienes levetid.

Det anbefales at nøkkel for OBU har en levetid på maksimalt tre år. For RBC (Radio Block Center) som anses som bedre sikret, anbefales en levetid på maksimalt fem år. Inntil videre anbefales det å arbeide med de tiltak som er beskrevet. Jernbaneverket må samarbeide med Danmark og ERA, for å ta nøkkelhåndterings standard i ERTMS teknologisk videre og for å forbedre sikkerheten i ERTMS kontinuerlig.

Abstract and conclusion

Jernbaneverket is establishing an organization to oversee the use of encryption and administer an encryption key handling program in connection with the establishment of a new signaling system in Norway called ERTMS (European Rail Traffic Management System). The current ERTMS standard specifies that key management shall be performed by offline distribution of key files, which requires manual routines for key handling.

This paper presents my research into the threat environment surrounding the railway in Norway. The findings are analyzed to identify factors that can affect key handling. These factors are categorized into external and internal factors, where external factors are those that Jernbaneverket cannot directly affect. The internal factors can be addressed with countermeasures such as physical security and the structure of the key management center.

A security analysis was performed in cooperation with Jernbaneverket's ERTMS pilot line project; the report is included as an attachment. A more thorough analysis of the threats Jernbaneverket faces regarding key management is also presented. The most significant challenge encountered in the course of the research was to gain access to security experts in from PST (Politiets Sikkerhets Tjeneste, the Norwegian police security service) and NSM (Nasjonal Sikkerhets Myndighet, the Norwegian national security administration). The paper also presents research into current and planned ERTMS key handling practices in Sweden and Denmark.

Based on this research, I make several recommendations to Jernbaneverket. The most important measure is to establish a good security culture in the entire organization, including the leadership. My findings indicate room for improvement in this area, with not enough attention paid to establishing a security organization and physical security of critical systems and personnel.

I recommend that Jernbaneverket improve physical security and establish a good security culture within the organization. Jernbaneverket should require security clearances at the "SECRET" (HEMMELIG) level for personnel employed in the key management organization, supported by an appropriate course of instruction. The key management organization should have a security manager. The security manager should conduct annual security interviews with all personnel involved in key management.

Jernbaneverket should also adhere to the NSM requirements for encryption algorithms. ERA (the European Railway Agency) should be urged to implement the AES algorithm and produce a standard for online key management in ERTMS. Establish cooperation with Denmark, where planning for online key management is already underway.

It is recommended to have clear security requirements in contracts with suppliers, where responsibilities for security are defined down to the component level. This is considered the most important aspect of key management where contractors are involved.

The lifetime of encryption keys is driven by the OBU (Onboard Unit), since this subsystem is the most exposed and the threat of encryption key compromise is highest. The GCD (Generic Crypto Device) which is a part of the OBU has a maximum lifetime of five years, driven by the lifetime of the backup battery.

I recommend that lifetime of encryption keys for OBU is maximum three years. For RBC (Radio Block Center) that is considered more secure than OBU. I recommend an encryption keys has a maximum lifetime of five years. Until further notice it is recommendations to work with the described actions. Jernbaneverket must cooperate with Denmark and ERA, to take key management standard in ERTMS technology further and to enhance the security of ERTMS continuously.

Innholdsfortegnelse

Figurer

Tabeller

Begreper og definisjoner

AES	Advanced Encryption Standard
ATC	Automtaic Train Controll
CENELEC	European Standards Organizations
DES	Data Encryption Standard
DMZ	Demilitarized Zone for server
EOA	End Of Authority
ERA	European Railway Agency
ERTMS	European Rail Traffic Management System
ETCS	European Train Control System
EU	European Union
EURO-BALISE	Standing alone fixed data Balises, or controlled data Balises linked to the wayside signalling system.
EVC	European Vital Computer
FATC	Fullstendig hastighetsovervåking
FS	Full Supervision
GCD	Generic Crypto Device
GSM-R	Globalt System for Mobilkommunikasjon for Rail
KMAC	Key Message Authentication Code
KMC	Key Management Center
KSMAC	Session Key
KTRANS	Key for Transfering KMAC keys to OBU/RBC
MA	Movement
MAC	Message Authentication Code
MDT	Mean Down Time
MLD	Mean Logistic Time
MRT	Mean Repair Time
MTBF	Mean Time Between failure
MTTF	Mean Time To Failure
NL	Non Leading
NSM	Nasjonal Sikkerhets Myndighet
NTP	Nasjonal Transport Plan

OBU	Onboard Unit
OS	On Sight
PST	Politiets Sikkerhets Tjeneste
RAMS	Reliability Availability Maintainability Safety
RBC	Radio Block Center
RV	Reversing
SB	Stand By
SH	Shunting
SIL	Safety Integrity Level
SN	STM National
SR	Staff Responsible
STM	Specific Transmission Module
TLS	Transport Layer Security
TR	Trip: Modus for passert sluttpunkt
UN	Unfitted: Modus med linjer uten ERTMS

1. Introduksjon

1.1 Bakgrunn

Som en siste del av studie erfaringsbasert master i Jernbaneteknikk skal det skrives en masteroppgave. I den forbindelse ble det i samarbeid med ERTMS (European Rail Traffic Management System) prosjektet i Jernbaneverket, laget en oppgavetekst som tar utgangspunkt i kommunikasjonen mellom tog og RBC (Radio Block Center) som går på GSM-R og er en kryptert forbindelse. Det er ønskelig å finne ut mere om sårbarheter og robustheten til den krypteringslogaritmen som allerede er implementert i ERTMS systemet. Oppgaven ble laget i samarbeid med John Price i Jernbaneverket.
Jernbaneverket skal i løpet av 2015 etablere en erfaringsstrekning mellom Ski og Mysen basert på signalsystemet ERTMS. Kryptonøkkelhåndtering på denne strekningen er foreløpig besluttet å gjennomføres offline. Det vil si at en fysisk må bytte krypteringsnøkler manuelt i RBC og i hvert enkelt togsett ved nøkkel skifte. På erfaringsstrekningen vil det kun bli brukt en RBC og kun utvalgte togsett som får installert utrustning ombord vil kunne trafikkere strekningen. Kommunikasjonen mellom tog og RBC går på GSM-R (GSM-Rail) kommunikasjon. Det er denne kommunikasjonen som krypteres. De anbefalinger oppgaven vil gi til Jernbaneverket er derfor kun rådgivende.

1.2 Målet for oppgaven

Denne oppgaven skal finne svar på hva er trusselen til jernbanen i Norge med tanke på villede eller uønskede hendelser som har til hensikt å skape ulykker eller skade, hvor ofte må en krypteringsnøkkel byttes får å unngå kompromittering av denne, hvordan på best mulig måte skal Jernbaneverket organisere og gjennomføre nøkkelhåndtering. Erfaringer fra andre landet skal også innhentes og sammenlignes med hvordan dette er tenkt gjennomført i Norge. Til slutt vil rapporten komme med en anbefaling og hvordan en bør arbeide videre i Jernbaneverket med dette området. Det er ikke kjent at en slik vurdering er gjort tidligere i Norge.

1.3 Organisering av rapporten

Første del vil prøve å gi en innføring i ERTMS og hvilken del av ERTMS denne oppgaven skal fokusere på og omhandle. Herunder også hvordan ERTMS og krypteringsmetoden teknisk fungerer. Den andre delen skal omhandle trusselen mot jernbanen i Norge. Den delen vil ha fokus på villede hendelser som har til hensikt til å

skade eller skape ulykker. Kapittel 1 og 2 er teorier som vil danne grunnlaget for resten av rapporten. Kapittel 3 vil fokusere på faktorer som er med på å påvirke nøkkelhåndtering, dette med bakgrunn i de to første delene av rapporten. Kapittel 5 vil omhandle hvordan dette gjøres i Sverige og Danmark, for å kunne sammenligne med det som er planlagt gjort i Norge og som en referanse som underbygger denne rapporten sitt resultat. I den sjettedelen av rapporten gjennomføres en risikoanalyse som underbygger den anbefaling denne rapporten vil gi til krypteringshåndteringen i Norge. Den vil bygge på alt foregående arbeide og informasjon som er kommet inn fra ulike faglige instanser, -kilder og litteratur. Kapittel 7 er et forslag til hvordan Jernbaneverket videre bør arbeide på dette området, spesielt med tanke på videre arbeide etter erfaringstrekningen, da det skal gjennomføres en videre utrulling av ERTMS i Norge.

2. Grunnleggende innføring i ERTMS og kryptert GSM-R kommunikasjonen mellom tog og RBC

Man er gammel når man har større glede av fortiden enn av fremtiden

- *John Knittel*

2.1 Innledning

ERTMS står for European Railway Traffic Management System, som heretter kalles ERTMS. ERTMS er et felles europeisk signalanlegg for jernbanen. Systemets hovedprinsipp går ut på at optiske signaler (lyssignaler) erstattes av informasjon om kjøretillatelse og hastighet som trådløst sendes direkte til togets førerrom og vises til fører via et panel ombord. ERTMS er et databasert system som *kan* reduserer sannsynligheten for menneskelige feil.

I dette kapittelet skal en få grunnleggende innføring i ERTMS, slik at en lett kan forstå ERTMS sin virkemåte og hvordan dette enkelt teknisk fungere. Om en ønsker dypere innsikt i ERTMS sin virkemåte henvises det til andre kilder som for eksempel ETCS for Engineers av Peter Stanley.

2.2 Grunnleggende Innføring i ERTMS

ERTMS består av tre hoveddeler.

1. ETCS som står for Train Control System-hastighetsovervåkning og signalering.
2. GSM-R som er GSM kommunikasjonen mellom tog og signalanlegg.
3. Felles europeiske trafikkregler kombinert med egne nasjonale regler.[1]

European Union heretter kalt EU har siden tidlig 1990 tallet arbeidet for å utvikle teknologi og spesifikasjoner for et felles europeisk tog trafikk styringssystem. Dette for å gjøre det enklere å trafikkere med tog over landegrenser, og på infrastruktur systemer som er levert av ulike leverandører. ERTMS er en ny generasjon av togkontroll og signalering, inkludert avansert tog beskyttelses med hastighets- og bremseovervåkning. Grunnene til å implementere ERTMS er av og til mange men de viktigste er:

1. Hovedgrunnen for fleste EU-land er å implementere regler som vil harmonisere signalsystemene i EU-landene. Dette vil gjøre internasjonal togtrafikk enklere. I dag er det over 20 forskjellige systemer. Enkelte med lokale varianter.
2. Eksisterende signalanlegg begynner å bli gammelt eller er allerede foreldet. ERTMS vil da redusere kostnader og kan redusere tekniske feil.
3. ERTMS vil redusere økonomiske risiko sammenlignet med flere ulike systemer ombord og infrastruktur langs sporet. Dette vil bidra til et felles system og ikke et enkelt system for togtrafikk. [2]

For Norge er den viktigste grunnen for å gå over til ERTMS, at dagens signalanlegg har høy alder og er basert på teknologi som er i ferd med å fases ut. Jernbaneverket har derfor stort behov for utskifting av disse anleggene i de kommende årene. Dette utgjør grunnlaget for Jernbaneverkets signalstrategi. Jernbaneverket har lagt til grunn følgende utvalgskriterier for innføring av ERTMS:

- Alder for signalanlegg og ATC (Automatic Train Control)
- Konkurranseutsetting av trafikk
- Grenseoverskridende trafikk
- Samfunnsnytten
- Større foreliggende utbyggingsplaner
- Strekningen bør fjernstyres eller innehar en rekke betjente stasjoner
- Strekningen har ikke FATC[3]

I senere tid er dette også politisk vedtatt at det skal innføres ERTMS som det nye signalsystemet i Norge. Alle nyere signalsystemer skal kunne bygges om til ERTMS som signalsystemet Signan levert av Thales. Om en større ombygging av dagens signalanlegg må gjennomføres, skal det vurderes å bruke Signan fra Thales.

ERTMS som system er definert i tre nivåer (Level 1, 2, og 3). Der nivå 1 er i funksjon tilsvarende dagens ATC. De ulike ETCS nivåene er som følger:

ERTMS Nivå 1:
Dette er et system hvor signaler langs sporet beholdes, men hvor togfører i tillegg får informasjon om kjøretillatelse, hastighet og strekningsinformasjon direkte i togets

førerpanel. Med bakgrunn i systemets punktformige dataoverføring, må toget passere baliser plassert i sporet for å kunne motta kjøretillatelse. Systemet overvåker hvor langt kjøretillatelsen gjelder og maksimalt tillatt hastighet.

ERTMS Nivå 2:
Dette er et digitalt radiobasert signalsystem hvor lokfører mottar informasjon om kjøretillatelse og hastighet direkte i togets førerpanel. Med dette kan signaler og hastighetsmerker langs sporet fjernes. Systemet overvåker hvor langt kjøretillatelsen gjelder og maksimalt tillatt hastighet. Deteksjon av hvor tog befinner seg gjøres med akseltellere eller sporfelt, og tog melder i tillegg regelmessig inn sin egen posisjon og kjøreretning til signalanlegget (RBC). Signalanlegget overvåker togets bevegelse og sender toget kontinuerlig endringer i kjøretillatelse og tillatt hastighet via GSM-R. Baliser plassert i sporet benyttes som kilometermerker for å fastslå/korrigere togets posisjon.

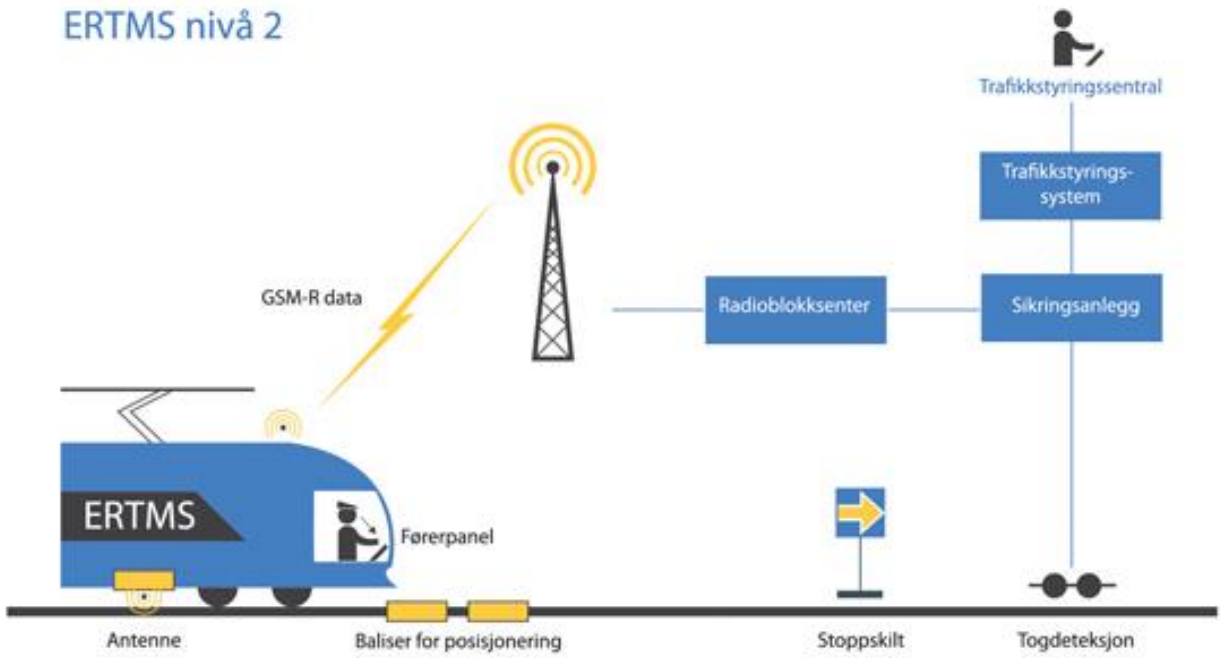
ERTMS Nivå 3
Systemet fungerer tilsvarende som ETCS Nivå 2, men med et viktig unntak. Avstand mellom togene ivaretas uten bruk av systemer for deteksjon av tog (sporfelt/akseltellere). Tog melder regelmessig inn sin posisjon og kjøreretning til signalanlegget (RBC), men i tillegg må togene ha et system for å sikre at det ikke har mistet en vogn, når tog deteksjon ikke lenger benyttes. Dette systemet benevnes tog integritet. [1]

I Norge er det valgt å starte opp med ERTMS Nivå 2 på erfaringsstrekningen mellom Ski og Mysen. Det er også en stor sannsynlighet for at videre utrulling også vil være nivå 2.

Figur 2.1 viser hvordan dette prinsipielt fungerer for ERTMS Nivå 2. Under toget er det en antenne for å kunne dedikere balisene som er Euro-baliser. Det er også antenne på taket for GSM-R kommunikasjon mellom radioblokksenter og toget. Det er denne kommunikasjonen denne oppgaven videre skal omhandle. Denne er kryptert og må være sikker i forhold til hacking og kompromittering, slik at ikke en villed uønsket hendelse kan forekomme av fremmede personer, organisasjoner eller makter. Om toget mister GSM-R forbindelsen vil toget stanse etter 90 sekund.

Radioblokksenteret kommuniserer videre med sikringsanlegget som igjen kan styres av en togleder med trafikkstyringssentralen. Dette til sammen ivaretar forriglingen til signalanlegget.

Markutstyret ute i sporet er det plassert ut to og to Euro- baliser i mellom skinnene på sviller, dette for å kunne dedikere hvilken retning toget har, posisjon og hastighet. Stoppskilt eller Marker Board viser eventuelt hvor langt toget har autorisasjon til å kjøre. Har ikke toget tillatelse å kjøre videre enn nærmeste stoppskilt/Marker Board skal toget stanse ved dette stoppskiltet.



Figur 2.1 *Prinsippskisse for ERMS Nivå 2 kommunikasjonen [jbv.no]*

Også togene må utrustes med ETCS, On-bord unit (OBU). Dette utstyret består av en datamaskin EVC (European Vital Computer) som kontinuerlig overvåker togets hastighet. For å kunne motta kjøretillatelse fra RBC, i Nivå 2 og 3 er togene også utstyrt med radiomodem for kommunikasjon mot GSM-R (R for railway). Det er også en egen enhet for kryptering GCD (General Crypto Device). Videre benyttes hjulomdreiningssensor og radar for å fastslå togets posisjon i forhold til siste passerte Euro-balise. Dersom et tog med ETCS også skal kunne kjøre på strekninger med ATC må det utrustes med en STM

(Specific Transmission Module). Denne oversetter informasjon fra ATC systemet til et "språk" ETCS forstår. Det er ETCS som overvåker og eventuelt bremser toget.[1]

Figur 2.2 viser førerpanelt i toget som lokfører forholder seg til i forhold til hastighet og autorisasjon for fremføring av toget.

Figur 2.2 *Førerpanelet ombord i toget med forklaring*

Lokfører kan fremføre toget når det er gitt en Movement Autority (MA) på displayet. Toget må stoppe ved End Of Autority (EOA) som vises med et Marker Board ved sporet. Hvor langt toget har MA vises på søylen til høyre på panelt. Der vises også, hastighet, anbefalt bremsing og EOA. Lokfører må også ta hensyn til hvilken modus toget har fra ERTMS. ERTMS har ulike moduser for toget, de viktigste modusene er:

1. FS - Full Supervision: Full overvåkning (full kjør)
2. OS - On Sight: Kjøring på belagt spor
3. SR – Staff Responsible: Kjøring uten signalering
4. SH - Shunting: Skiftemodus
5. SB - Stand By: Oppvåkningsmodus

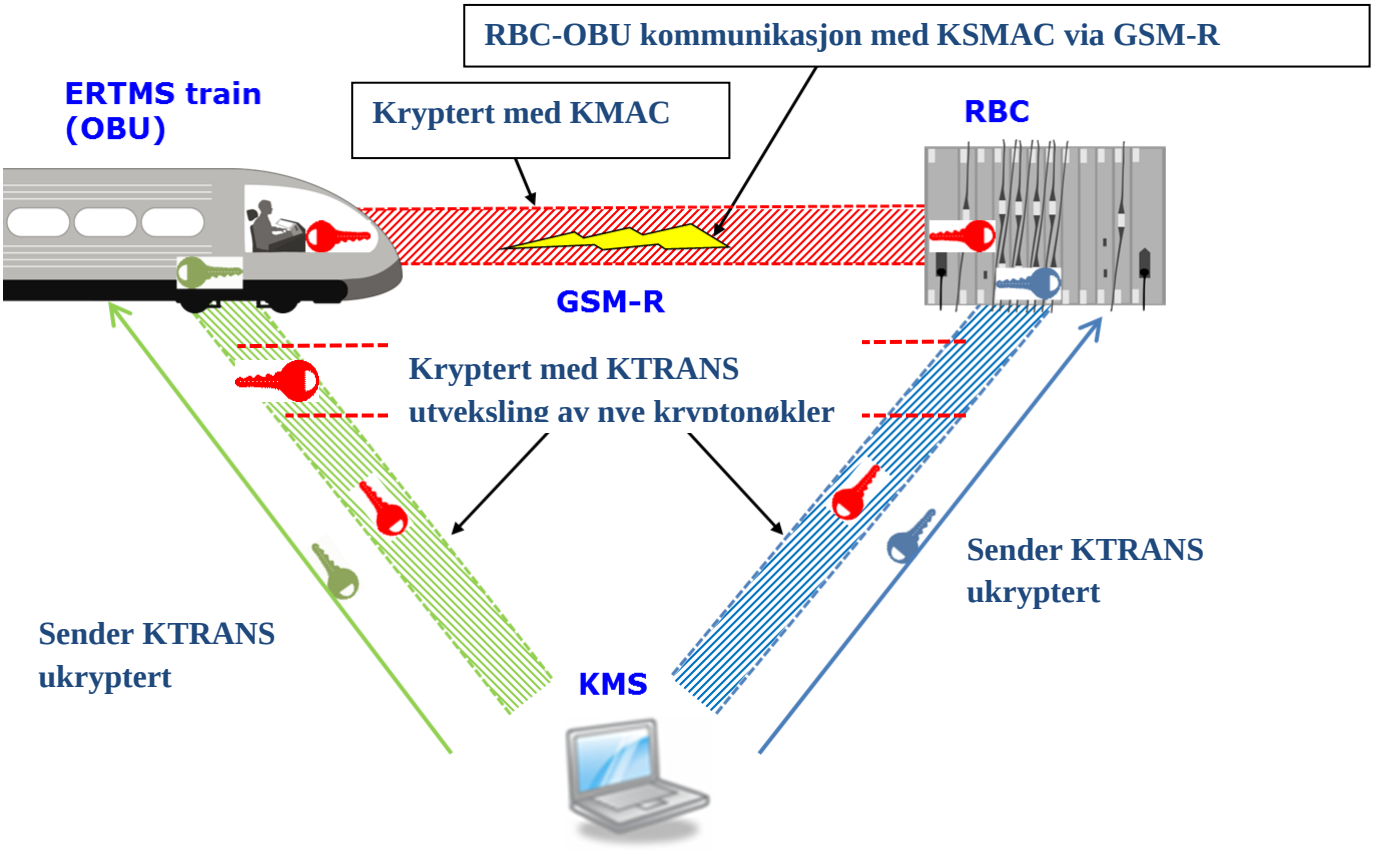
6. SN - STM National: Modus for linjer med ATP
7. UN - Unfitted: Modus med linjer uten ERTMS
8. RV - Reversing: Bakking/Rygge
9. TR - Trip: Modus for passert sluttpunkt (EOA)
10. NL - Non Leading: Ikke førende

Dette er kort om hva er ERTMS er. Norge har valgt å implementere ERTMS nivå 2 Baseline 2 for teststrekningen. For videre utrulling etter test vil de bli implementert ERTMS nivå 2 baseline 3.

2.3 Kryptert GSM-R kommunikasjonen mellom tog og RBC

Kommunikasjonen mellom tog og RBC er en kryptert GMS-R forbindelse. GMS-R i kryptosammenheng anses som å være en usikret kommunikasjonsbærer. RBC og tog får krypteringsnøkkel fra KMC (Key Management Center). Organisering hvordan krypteringsnøkkelhåndteringen administrativt kan gjennomføres i Norge og levetid til nøkler, kommer det mere om i kapittel 4 og 6. Kryptering i ERTMS er en symmetrisk krypterings metode som kalles triple-DES kryptering. . Den er på 64 bit der av 8 bit brukes til paraity og 56 bit til kryptering.

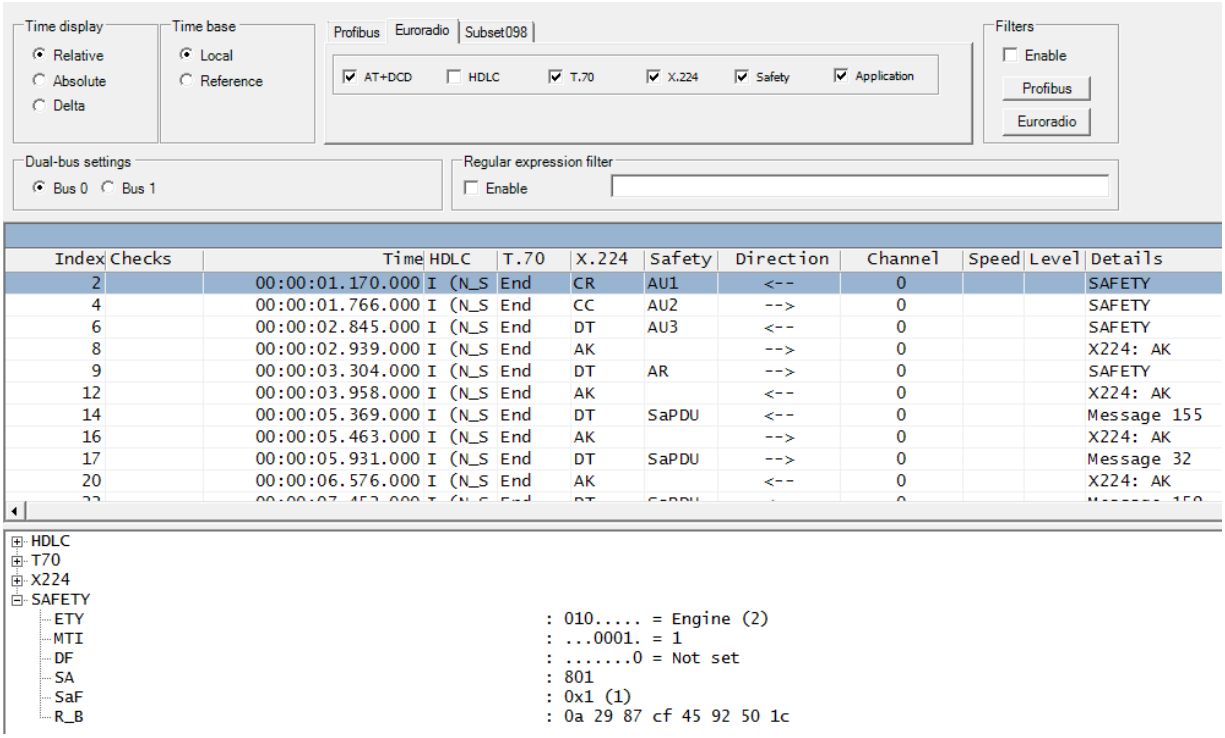
Ved symmetrisk kryptering deler både tog og RBC en krypteringsnøkkel. Togets og RBC har en helt lik nøkkel. Men ulike OBU'er (OmBord Utrustning) kan ha ulike nøkler. RBC'en vil da ha en database med de ulike nøklene til OBU'ene.Denne nøkkelen brukes for både kryptering og de kryptering av informasjon som sendes mellom tog og RBC. Nøklene utveksles via en sikker kanal denne kalles KTRANS (Key for Transfering KMAC keys to OBU/RBC) slik at nøkkel er beskyttet. Figur 2.3 er en illustrasjon på kryptert kommunikasjonen mellom RBC og toget over GMS-R som sambandsbærer og illustrasjon på hvordan nøkkelhåndtering gjennomføres mellom RBC og KMC. Ved offline nøkkelhåndtering vil dette være en manuell prosess. Men under den manuelle operasjonen ved bytte av nøkler i OBU og RBC vil en KTRANS beskytte nøklene til de er installert. I RBC skjer nøkkelbytte ved å installere en fil som inneholder en database med ulike kryptonøkler for ulike tog typer og hvilket tog nummer denne tilhører. Dette vil si en RBC på forhånd må vite hvilke tog som skal trafikkere strekningen. I OBU kan nøkkel lastes opp via en minnepinne, men da helst en kryptert og sikra minnepinne.



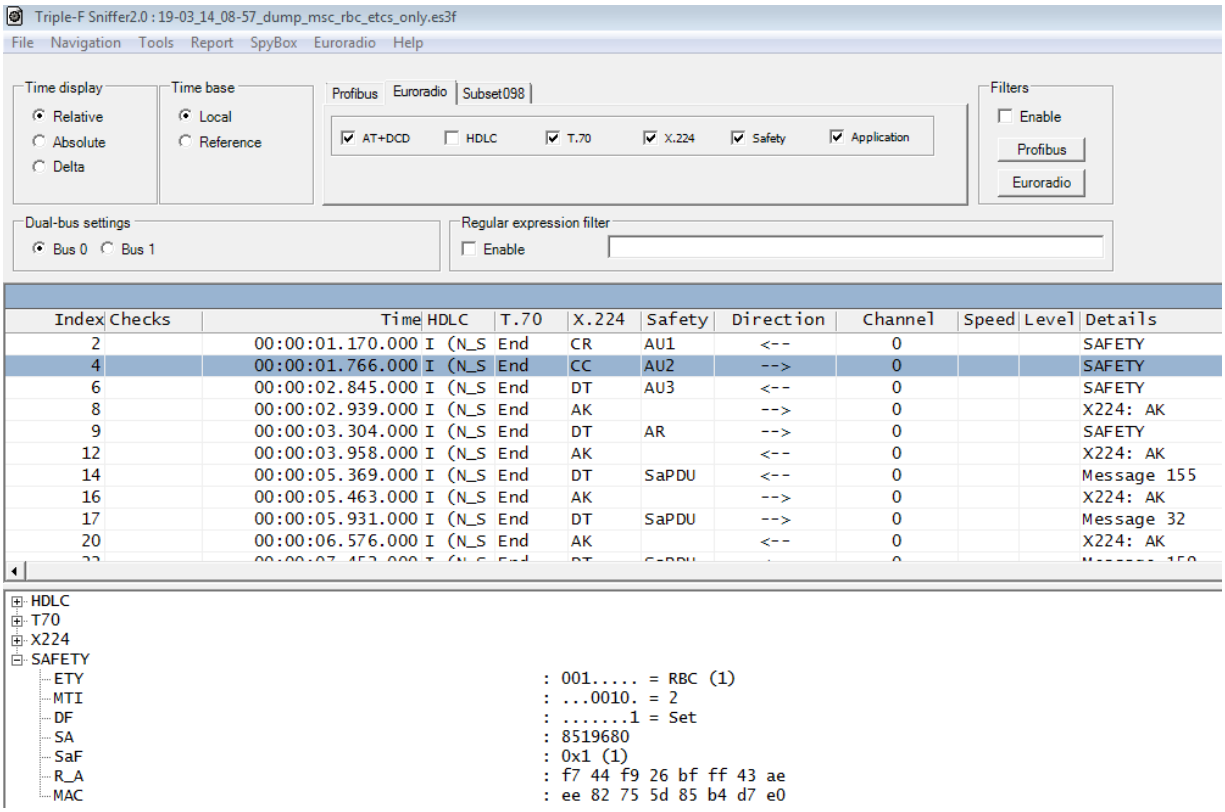
Figur 2.3 *Eksempel på nøkkelhåndtering mellom KMC-RBC –OBU og hvordan OBU-RBC etablerer en KSMAC [vedlegg]*

Kommunikasjonen mellom tog og RBC etablere en egen session key som heter KSMAC , som har en varighet så lenge toget trafikkere den aktuelle strekningen eller til toget mister kontakten med RBC. For teststrekningen Østre linje vil dette være fra toget starter fra Ski stasjon til toget ankommer Mysen stasjon som har en varighet på ca en time. Da stopper kommunikasjonen og KSMAC slettes. Når toget kjører fra Mysen til Ski etableres det en ny KSMAC. Nøklene utveksles via en sikkerkanal ved hjelp av MAC (Message Authenticaton Code) slik at informasjonen skal kunne være lesbar. Når MAC benyttes er informasjonen som sendes lesbar ikke kryptert under autoriseringsprosessen mellom Tog og RBC.

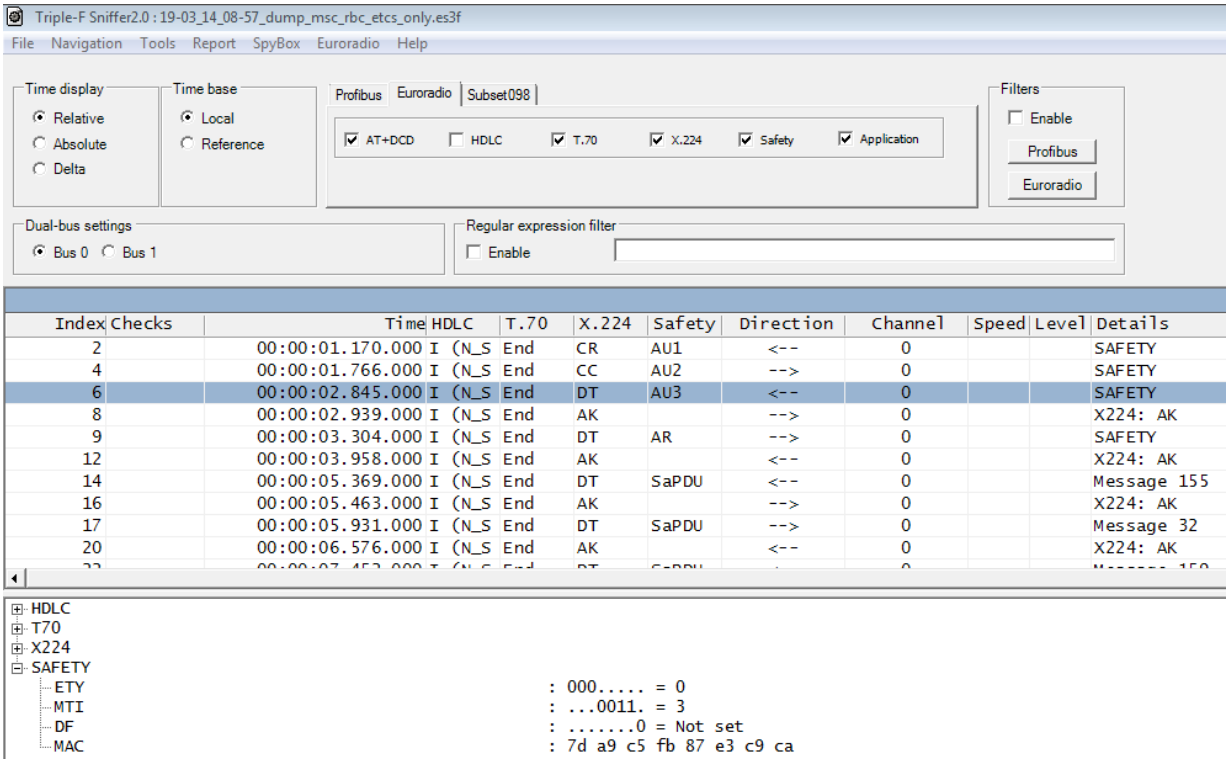
Dette gjennomføres ved en tre stegs autentiseringsprosess mellom tog og RBC ved hjelp av KMAC nøkler. De tre stegene benevnes som AU1, AU2 og AU 3. De tre stegene vises på figur 2.4, 2.5 og 2.6. Figurene er hentet fra teststrekningen Ise-Sarpsborg, som min veileder John Price har hentet utfra kommunikasjonen mellom tog og RBC.



Figur 2.4 *Autentifisering 1[John Price]*



Figur 2.5 *Autentifisering 2[John Price]*



Figur 2.6 *Autentifisering 3[John Price]*

De viktigste detaljene fra figurene 2.4, 2.5 og 2.6 er at MAC beregnes med KSMAC, og KSMAC avledes fra Ra, Rb, og KMAC. AU1 sendes uten MAC siden enhet B vet bare Rb når det sender AU1 (Ra er ukjent). Enhet A skal sende AU2 så lenge som det gjenkjenner enhet B og kan identifisere hvilken KMAC skal brukes for beregning av KSMAC. AU2 og AU3 er sendt med MAC siden KSMAC kan beregnes. Hvis enhet B ikke beregner den samme MAC for AU2 skal kommunikasjonen opphører umiddelbart. Det samme skjer hvis enhet A ikke beregner den samme MAC for AU3.

Som tidligere nevnt vil nøkkelhåndtering komme i kapittel 4 og 6, der vi ser nærmere på hvordan dette bør håndteres teknisk og med hensyn til administrasjon, sikkerhet og hvordan Jernbaneverket bør organisere dette.

3. Generelt trusselbilde for jernbanen i Norge

3.1 Generelt trusselbilde for Norge

Ulykker, terror og trusler har i dag en sentral plass i mediebildet. I den senere tid ikke bare ute i verden men også nå gjelder dette i Norge[6]. Ved at Norge har gjort seg bemerket ute i verden med Oslo avtalen, karikatur tegninger og deltagelse i internasjonale operasjoner som Afghanistan har Norge blitt et mål for terrorister, grupper, eller andre som ønsker uønskede villed hendelser eller ulykker på norsk jord. I et møte som ble holdt med NSM (Nasjonal Sikkerhets Myndighet) 31. oktober 2014, kunne Sjefingeniør Lars Olaussen informere om en klar økning av omfanget og alvorligheten i dataangrep mot Norge ukentlig. Det som for et par år siden skjedde en til to ganger i året skjer nå ukentlig. Det er i dag ikke fremmed makt, men interesse organisasjoner og grupper som utfører angrepene. Angrepene er avanserte og svært farlige.

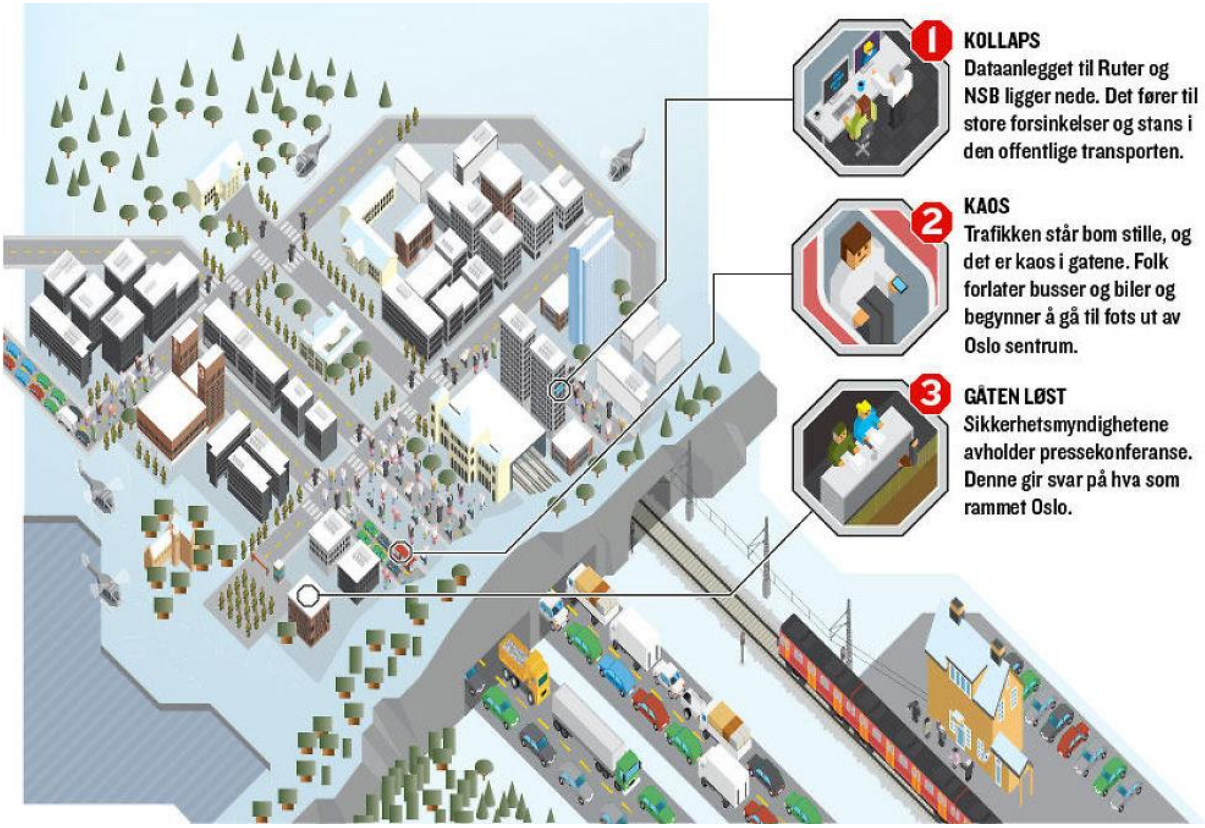
Trusselbilde mot Norge vurderes fortløpende som for eksempel når hendelser som terrorangrep i Paris skjer. Men det er fortsatt ingen endring i trusselbilde i Norge og det forholder denne oppgaven seg til. I et møte med PST (Politiets Sikkerhets Tjeneste) den 4. november 2014, kunne Senior Sikkerhetsrådgiver Thomas Haneborg informere om at trusselbilde mot Norge er alvorlig, men uendret den siste tiden. Det samme trusselbilde mot Norge er også gjeldende etter terrorangrepet i Paris januar 2015. Sjefen Benedicte Bjørnland for Politiets sikkerhetstjeneste (PST) sier [7] likevel at de ikke kan utelukke at noe lignende kan skje i Norge. Hun sier PST spesielt frykter personer som kommer ut fra et hjemmeavlet islamistisk miljø i Norge. Benedicte Bjørnland viste ellers til at det har vært en negativ utvikling i trusselbildet gjennom 2014, og at det tilspisset seg ytterligere mot slutten av fjoråret. Hun trakk fram likhetene ved angrepene i Belgia og Canada i fjor og onsdagens angrep i Frankrike, og pekte særlig på målutvelgelsen og metoden. Det gjelder gjerningsmannens profil, med tilknytning til grupper som IS og al-Qaida, myke symbolmål og at det brukes håndvåpen snarere enn eksplosiver.

PST har et utstrakt samarbeid med andre land og tjenester for å forebygge lignende handlinger i Norge. Når det gjelder norske fremmedkrigere som har vært og er i Irak og Syria, følger PST godt med.

3.2 Trusselbilde mot jernbanen i Norge

Med et trusselbilde som er alvorlig mot Norge, må vi være forberedt på at dette kan ramme jernbanen i Norge, like mye som jernbane, T-bane eller kollektivtransport blir angrepet i andre land. Angrep mot kollektivtrafikk er allerede blitt gjennomført i Europa. Blant disse kan nevnes terrorangrepet mot jernbanen i Madrid og angrepet mot T-banen i Russland begge angrepene gjennomført i 2004. Når en ser på disse hendelsene er det angrep mot perronger, tog og mennesker. Angrep på infrastruktur for kollektivtrafikk er det ingen kjente angrep, det nærmeste en kommer er fly kapring eller lignende.

Når ERTMS innføres, innfører vi også faren for det som kalles «Cyber Attack» som er dataangrep mot transportsystemer i dette tilfellet som nå også vil gjelde jernbanen. NSM sier i sin Sikkerhetstilstand 2014 om dataangrep [14] For fremmede etterretningstjenester, kriminelle og hackere er internett en arena for informasjonsinnhenting og spionasje. Aktørene som står bak truslene i det digitale rom spenner i følge rapporten. Fokus 2014 fra etterretningstjenesten, fra statlige etterretnings- og sikkerhetstjenester, via tradisjonelle militære motstandere, globale næringsbedrifter, terrorist- og ekstremistgrupper, til organiserte hackergrupper. Rapporten fremhever spesielt Russland og Kina som land som har etablert betydelig kapasitet til å utføre operasjoner innenfor cyberdomenet. Til forskjell fra fysiske innbrudd og angrep, er det ofte svært liten åpenhet rundt et dataangrep. Norske virksomheter som utsettes for dataangrep velger nærmest uten unntak, å ikke la angrepet bli gjort offentlig kjent. Dette betyr igjen at det blir liten samfunnsmessig bevissthet rundt den faktiske situasjonen i Norge. I lys av dette er Telenors åpenhet i etterkant av angrepet på egne systemer i begynnelsen av 2013, et meget godt eksempel på at åpenhet ikke nødvendigvis gir en negativ effekt for virksomheten. I [2] omtaler de Kreckhoffs lov som er en parallell til åpenheten til Telenor. Den sier for et kryptosystem skal være sikre bør alt om systemets spesifikasjoner være offentlig kjent. Dette for at en offentlig diskusjon kan finne sted, dette har som mål å gjøre systemet enda sikrere. Dette er mye omdiskutert men NSM har åpnet for dette ved for eksempel Telenor saken. Men prosedyre, prosesser og nøkkelhåndtering er fortsatt unntatt offentlighet, da dette utgjør sikkerheten til systemet, men ikke systemets spesifikasjoner alene som utgjør sikkerheten.



Figur 3.1 *Tenkt scenario på et dataangrep mot transportsystemet i Oslo VG artikkel 28. mai 2013 [8]*

Figur 3.1 viser et tenkt scenario ved Oslo S som er hentet fra VG artikkel slik kan Norge bli cyber-angrepet [8] som sier videre. Ved en slik hendelse vil det umiddelbart satt i gang med å analysere hva det er og prioriterer tiltak for å håndtere hendelsen. Så «setter vi stab» i lokalene til NSM, med deltagelse fra Kripos og Politiets sikkerhetstjeneste, Etterretningstjenesten og Cyberforsvaret, og dessuten informeres beslutningstakende politikere. Dette står det mere om i [8] Når slike hendelser opptrer vil det samles mye mennesker ved kollektivknutepunktene som Oslo S. Det kan være at cyber angrepet er en del av et større angrep som har til hensikt å ramme mennesker. Et tenkt scenario kan være at GSM-R nettet ved Oslo S blir jammet (forstyrrelse som ødelegger GSM signalene) med en GSM jammer. Dette medfører til tog ikke kan trafikkere fra eller til Oslo S. Etter noen timer vil det da være mange mennesker som ikke kommer hjem i rushtiden. Når antall mennesker er stort kan neste steg være å fyre av en bombe inne på Oslo S. Ved et slikt scenario vil en kunne drepe eller skade et stort antall mennesker samtidig som det skapes frykt, akkurat slik terrorhandlingen vil ha som mål med et slikt angrep.

Sommeren 2014 var det høynet terrorberedskap ved alle samferdselsknutepunkter og offentlig steder med stort antall mennesker i Norge. Under denne perioden gjorde jeg noen observasjoner. Antallet polititjenestefolk med bevæpning ved Oslo S var stort, og det ble gjennomført tilfeldige kontroller av reisende. Samtidig som politiberedskapen var høy, var søppeldunker ved Oslo S også på perrongene like åpne som før. Noen dager etter jeg gjorde denne observasjonen var søppeldunkene forseglet. Ved lett å plassere en bombe, GSM jammer eller lignende i en søppeldunk kunne skapt farlige situasjoner eller uønskede hendelser. Togene trafikkerte med samme antall ombordansvarlige som ved en normal situasjon. Hvorfor ble ikke det gjennomført en oppbemanning av alle vogner i et togsett? De ubetjente vognene var fortsatt like ubetjent ved en høynet terrorberedskap. Sett i lyset av at det er i toget eller ved perronger slike situasjoner erfaringsvis skjer. Begge observasjonene er nok ikke det mannen i gata la merke til, men mange som jobber eller har jobbet med sikkerhet vil dele de samme tankene og observasjonene av dette. Nå skal det også sies at å sikre tog mot terrorangrep er nærmest en umulig oppgave, men enkelt tiltak kan virke forbyggende og synergien av dette unngå at terrorangrep skjer eller blir iverksatt. Har vi blitt flinkere etter 22. juli og sommeren 2014? Mye er gjort, men mye gjenstår vil mange mene.

Det er ingen kjente trusler mot jernbanen i Norge i dag kunne Thomas Haneborg informere om under et møte med PST den 4. november 2014, men jernbanen er et mål som vi må ta hensyn til. Han kunne også legge til at det er ingen kjente eller kapasiteter som har til hensikt eller som mål å slå ut kritisk jernbane infrastruktur. Da er last, mennesker og togsett et enklere mål, men et angrep på tog eller godstog vil ikke kunne ødelegge infrastrukturen i vesentlig grad. Dette vil ikke si at vi ikke skal sette fokus på sikkerheten. Det er viktigere enn noen gang å utvikle Jernbaneverkets organisasjon på å tenke sikkerhet også innen lokalisering, organisering, kultur, personell og IT. Fordi denne er nå under stor endring ved at vi går fra relebaserte systemer til IT baserte signalanlegg.

Fra NSM sine sider [14] sier dem følgende, NSM erfarer at mange virksomheter mangler oversikt over sine egne verdier og egen sikkerhetstilstand. Sikkerhetsmessige utfordringer er ikke dokumentert og virksomheten har ikke formulert konkrete mål for sikkerhetsarbeidet. Ofte mangler det bevissthet omkring sikkerhetsmessig risiko og erkjennelse av at virksomheten kan være utsatt. Mange virksomheter har verken innhentet eller etterspurt trusselinformasjon som grunnlag for å utarbeide risiko- og

sårbarhetsvurderinger. Virksomheter synes å være villig til å akseptere en sikkerhetsmessig risiko som NSM vurderer som uakseptabel for samfunnet som helhet. Det har ikke vært mulig for meg å finne eller få tilgang til informasjon om Jernbaneverket har innhentet trusselinformasjon. Denne oppgaven kan kun baseres på den informasjon jeg har fått tilgang til ved møter eller samtaler med PST, NSM, egen informasjonsinnhenting og erfaring.

4. Faktorer som påvirker kryptonøkkelhåndtering

4.1 Introduksjon

Ved nøkkelhåndtering i ERTMS kreves det fysisk tilgang til RBC, KMC eller OBU. Dette fordi en standard for online nøkkelhåndtering i ERTMS ikke er ferdig. Dette vil bestemme mye av hva Jernbaneverket må sette i gang av tiltak for nøkkelhåndteringen kan gjennomføres på en sikker og best mulig måte.

Interne faktorer som påvirker kryptonøkkelhåndtering kan være krav til personell, lokalisering, fysisk sikring, organisering, kultur, personell og hvilke IT systemer vi har i Jernbaneverket. Alt dette er en del av Jernbaneverkets egen organisasjon og kultur. Vi har også ytrefaktorer som vil være med på å bestemme hvordan dette skal gjennomføres internt i Jernbaneverket. Ytrefaktorer kan være aktører innen terror, trusler og hacking. Der terror er omtalt i kapittel 3.2. Tilgjengelig kompetanse, type krypterings algoritme i ERTMS, hvordan nøkler må håndteres pga. tilgjengelig teknologi, personell fra leverandør som må brukes osv. Det vil være ved implementering av ERTMS tilgjengelige teknologien som til enhver tid er i den aktuelle ERTMS standarden som kan brukes og hvilken sårbarhet denne har. Jeg velger å dele faktorene opp i ytre og interne forhold som kan påvirke kryptonøkkelhåndteringen.

4.2 Interne faktorer

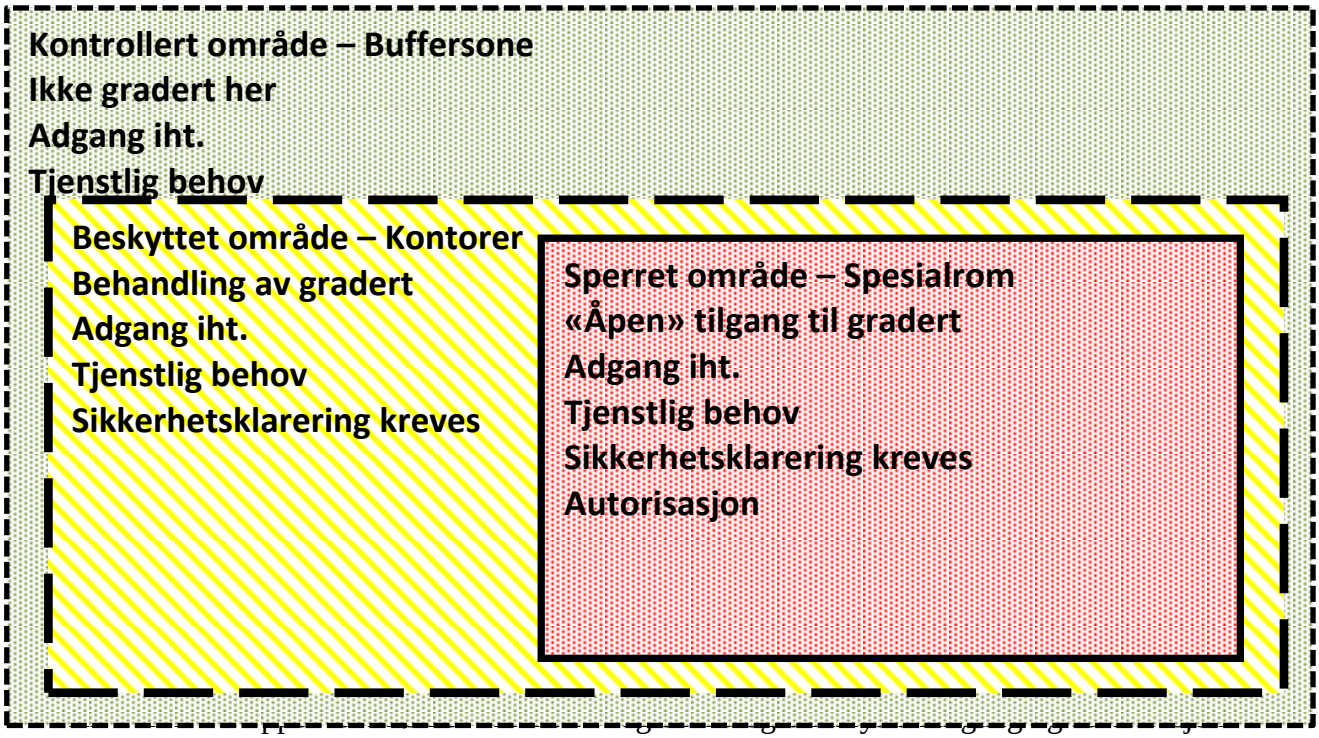
Sikkerhet blir av det Amerikanske forsvarsdepartementet beskrevet som følger i forskrift for informasjonssikkerhet [15] «Uavhengighet fra de tilstander som kan føre til død, skade, yrkesmessig sykdom, skade på utstyr og eiendom eller miljø.» Videre sier Henrik Børstad Eriksen [10] at denne beskrivelsen indikerer at sikkerhet er noe av det viktigste for en organisasjon å opprettholde, men at dette er ikke kostnadsfritt. Kostander, spesielt i samfunnsøkonomisk perspektiv angående sikkerhet i en organisering, er alltid et omdiskutert emne. Vi må tenke at det skal være sikkert nok, men ikke så sikkert at det går utover de oppgaver Jernbaneverket er satt til å gjennomføre for samfunnet for øvrig, under normal forhold. Da regnes ikke feil på infrastruktur eller rullende materiell med under normale forhold, selv om det med dagens signalanlegg kan virke slik. Siden det til tider er mye signalfeil på våre anlegg, er det også blitt et samlebegrep på feil på andre

komponenter som sporveksel, linje brudd etc. Mange vil mene i Jernbaneverket det er uheldig å samle feilhendelser i en samle post.

Ved å se på faktorer som påvirker Jernbaneverkets organiser av nøkkelhåndteringen i Norge, kan vi ta utgangspunkt i sikkerhetskrav til personell. En intern aktør som en ansatt er, vil det som regel være utilsiktede hendelser som oftest oppstår. En ansatt kan benytte en virusinfisert minnepinne uten selv være klar over dette. Dette kan lage en spredning av programvare som eventuelt kan ødelegge eller åpne opp for eksterne aktører for så kunne hacke systemet. Dette må gjennom opplæring og rutiner forhindres. Det en må påse er å sette klare krav til personell som skal være direkte inne i nøkkelhåndteringsprosessen. Med det menes at en har tilgang til KMC. Det vil av mange være naturlig at personell som har adgang til KMC har en sikkerhetsklarering for slikt arbeide fra NSM. En sikkerhetsklarering er en avgjørelse om at en person kan gis tilgang til sikkerhetsgradert informasjon. Klarering gis for graderingsnivåene: «KONFIDENSIELT», «HEMMELIG» og «STRENGT» HEMMELIG. Fra NSM personellsikkerhet [11] kan komme med råd om riktig nivå for klarering. De ansatte har tilgang på en mengde eller type data, som vil bestemme graden av sikkerhet. Informasjon utfra samtaler med NSM og PST er en klarering på minimum nivå «KONFIDENSIELT» eller kanskje også graden «HEMMELIG» naturlig. Men denne informasjonen og utfra dagens trusselbilde og hvilke konsekvenser en utro tjener kan medføre av død, skade, yrkesmessig sykdom, skade på utstyr, eiendom eller miljø og samfunnet for øvrig virker dette naturlig. Samtidig må vi ta med konsekvenser og hva samfunnet kan få av skade. en gradering av ansatte på «KONFIDENSIELT» nivå kan denne sikkerhetsklareringsgraden anses av mange som for lav i forhold til ansvar og oppgaver for slikt personell og informasjon de har tilgang til. Ved en slik sikkerhetsgradering vil det også være naturlig å gjennomføre opplæring av personell. NSM kan gjennomføre ulike sikkerhetskurs som Jernbaneverkets personell bør benytte for opplæring. Det bør også utnevnes en sikkerhetsleder for KMC. Sikkerhetsleder gjennomfører en årlig sikkerhetssamtale med alle ansatte ved KMC engang i året. Når det kun er sikkerhetsgradert personell som har tilgang til KMC, vil dette også medføre til å være færre ansatte som har tilgangen til KMC. Dette vil være med på å bidra til bedre sikkerheten som en bieffekt av dette.

Vi kan videre se på fysisk sikring og lokalisering av RBC og KMC spesielt. OBU med GCD installeres i toget. Plassering og sikring av GCD vil være en del av ansvaret til

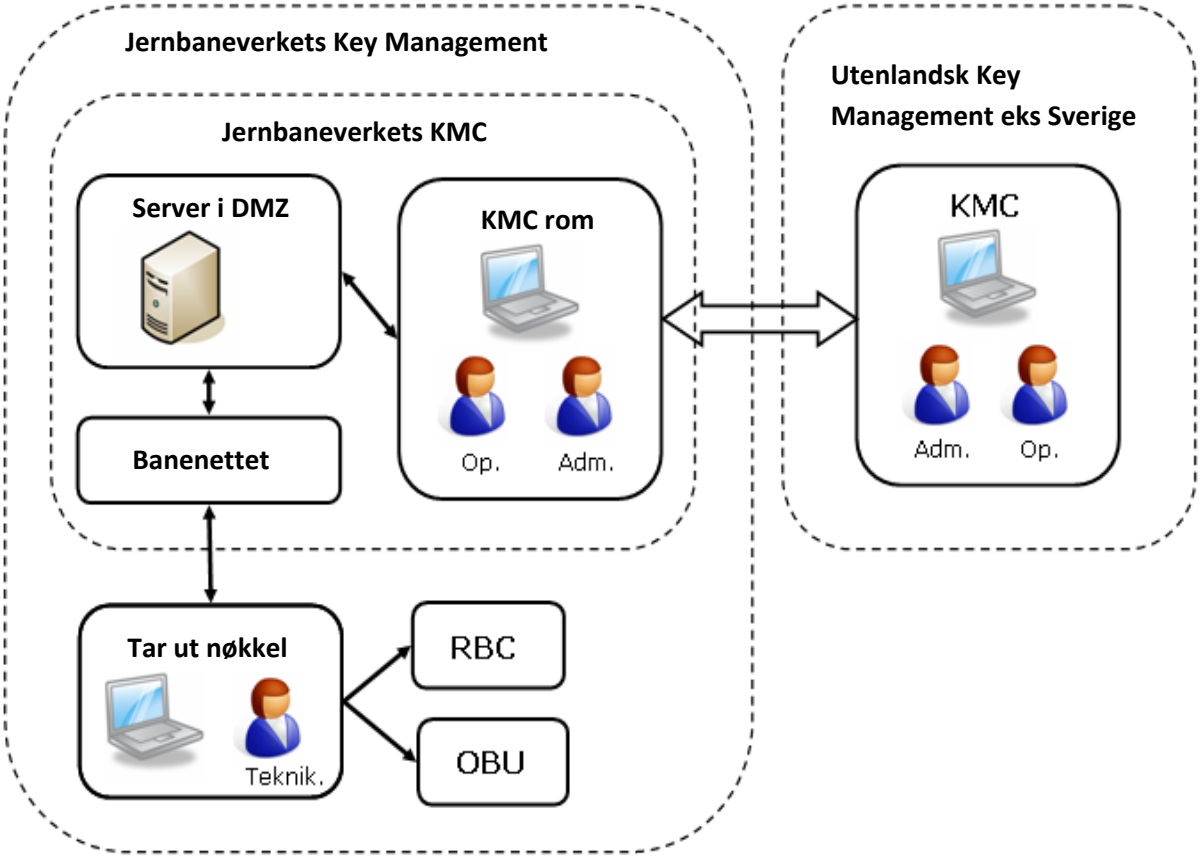
togselskapene. Oppgaven vil videre ikke se på denne delen. Når det gjelder fysisk sikring sier NSM i forbindelse med fysisksikring [12] er et grunnleggende sikringstiltak som enklest kan forklarets som tiltak for å hindre uvedkommende fysisk tilgang til skjermingsverdig informasjon og aktivitet. Sikringstiltaka etablerer sikre område gjennom inngangskontroll og fysiske barrierer. Styrken i tiltaka varierer med verdivurderinga av det som skal sikrest. Eksempelvis betyr dette at kravet til sikring av informasjon graderte «HEMMELIG» er strengere enn for informasjon gradert «KONFIDENSIELT». Her vil nok mange mene at KMC som lokasjon har gradering «HEMMELIG» som lokaliseringssted. I KMC generes nøkler i klar tekst, før de krypteres og kan installeres ute på RBC eller i togsett. Det er i KMC det er størst fare for kompromittering av nøkler. Hvordan lokalene til KMC kan bygges med soneinndeling er illustrert i [13] NSM angående fysisksikring mot inntrengere figur 4.1.



Figur 4.1 Illustrasjon av oppbygging av lokaler for HEMMELIG [13]

Jernbaneverket må organisere dette på en slik måte at en unngår personavhengighet i forbindelse med nøkkelhåndtering. Vi må ha mange nok som er opplært til å utføre de ulike operasjonene ved nøkkelhåndtering. Antall ansatte i organisasjonen vil bli mindre

ved et online system for nøkkelhåndtering, men inntil videre må dette gjøres manuelt. Hvor mange ansatte i organisasjonen som er nødvendig for å kunne fungere optimalt blir ikke tatt med i denne oppgave, men overlater dette til Jernbaneverket. Figur 4.2 viser hvordan en kan organisere dette i Jernbaneverket, lignende organisasjon er også med i [4] Handtering av krypteringsnyklar frør ERTMS av Jorge Gamelas.



Figur 4.2 *Eksempel på en Key Management organisasjon [4]*

Kommunikasjonen mellom KMC rom og server i DMZ (Demilitarized Zone) er ikke via nettet, men er en direkte kommunikasjon via kabel. Figuren viser også hvordan dette kan organiseres mellom land. Men dette utelater vi i denne oppgaven, fordi vi har fokus på nøkkelhåndtering i Norge og spesielt fokus på KMC, RBC og OBU.

Jernbaneverkets egne IT systemer må også hensyn ta en går fra relebaserte systemer til IT baserte signalsystemer, fordi IT systemene nå må også kunne behandle større grad av sensitiv informasjon der skade på signalsystemet kan gjøres uten fysisk tilgang til selve systemet. Personer kan sitte hvor som helst i verden å kunne skape uønskede villede hendelser. I[14] NSM rapport om sikkerhetstilstand 2014 sier dem følgende om IT.

Dataprogrammer som ikke er oppdaterte og andre sårbarheter i datasystemene, er ofte veien inn for kriminelle og hackere. Andre typiske fremgangsmåter er å sende epost med vedlegg som er infisert med virus, eller infisere nettsider med virus, som igjen infiserer de besøkende. I NSM rapport om sikkerhetstilstand 2014[14] sier så videre at sikkerheten i mange offentlige IKT-systemer er synes ikke god nok i forhold til risikobildet. Manglende responsmiljøer til å håndtere dataangrep, og manglende helhet i informasjonssikkerhets arbeid er sannsynlige sårbarheter. Det eksisterer for eksempel mange forskjellige, statlige nett med egne aksesspunkter til internett. Det betyr i praksis at det er mange dører og vinduer inn til systemene for de som ønsker å bryte seg inn. Det krever betydelige ressurser både personellmessig og økonomisk å sikre systemene. En vurdering av IT systemene til Jernbaneverket bør skje parallelt med implementering av ERTMS, siden det da vil behandle informasjon som er mer sensitivt for hacker enn før ved relebaserte anlegg.

4.3 Ytrefaktorer

Ytrefraktorer er som tidligere nevnt, faktorer ikke Jernbaneverket selv direkte har herredømme over, men bør gjøre tiltak mot og etterkomme eller tilpasse så langt som mulig. Når det gjelder terror og trusselbilde henvises det til kapittel 4.2.

Som nevnt i kapittel 2.2 er det trippel-DES kryptering som brukes pr i dag i ERTMS. I Forskrift om informasjonssikkerhet [15] sier følgende om kryptografiske mekanismer. Ved overføring, lagring og behandling av sikkerhetsgradert informasjon fastsetter NSM hvilke kryptografiske mekanismer som kreves. Sikring av sikkerhetsgradert informasjon ved bruk av kryptografiske mekanismer kan bare foretas med kryptoutstyr og metode for administrasjon av kryptonøkler og digitale sertifikater godkjent av NSM. Etter anbefaling fra Lars Olaussen i NSM bruker jeg NSM sitt utkast for nytt kryptokravdokument, siden det ikke vil komme vesentlige endringer etter høringen er gjennomført. I NSM sitt nye krypteringskravdokument inneholder følgende om DES kryptering [16] Vanligvis innstiller NSM til bruk av AES og ikke DES kryptering. Men krypteringen skal være basert på åpne og / eller offentlige standarder. Proprietære mekanismer for kryptering skal unngås. I møte med NSM kom det fram følgende: Det er 10 år siden NSM anbefalte AES

kontra DES, men om en likevel vil benytte DES er det ikke krypteringsalgoritmen i seg selv som utgjør sikkerheten, men hvordan Jernbaneverket vil organisere nøkkelhåndtering med tilhørende prosedyrer. Prosedyrer og organisering av nøkkelhåndtering må være unntatt offentlighet. Jernbaneverket må også påse at produktene som leveres fra leverandør er sertifiserte. Hvis ikke få dem sertifisert. Sertifisering kan NSM gjennomføre for Jernbaneverket. Føre var prinsippet er gjeldende for all kryptering og nøkkelhåndtering. I møter med ERA (European Railway Agency) kan Jernbaneverket være med å påvirke utviklingen på dette området.

Leverandøren av ERTMS har en viktig rolle ovenfor Jernbaneverket. Jernbaneverket kan gjennom kontrakter ivareta mye av de krav Jernbaneverket bør stille ovenfor leverandør. Under min oppgave skriving har kontrakten ikke vært tilgjengelig og de som har vært involvert har heller ikke informasjon om dette. Men gjennom kontrakten kan Jernbaneverket stille krav og ivareta sikkerhet, personell og organisering av arbeidet hos leverandøren i forbindelse med arbeidet med den norske ERTMS organisasjonen. Der det viktigste innholdet er å dele ansvarsområder med tilhørende ansvar, dette er spesielt viktig innen det som berør kryptonøkkelhåndtering.

Hacking av signalanlegg uten fysisk tilgang til systemet blir nytt i Jernbaneverket ved implementering av ERTMS. I kapittel 4.2 ivaretar intern aktører. Det er mange eksterne aktører som ville skade et IT basert signalanlegg. Skaden disse aktørene skaper kan enten være tilsiktede eller utilsiktede. I Johnsen NTNU 2012 [9] omhandler eksterne aktører med tilsiktede og utilsiktede tilsikter, den sier videre. En ekstern aktør som handler tilsiktet kan være alt fra profesjonell hackere til ungdommer på gutterommet som har funnet ondsinnet programkode på internett. En profesjonell hacker vil gjerne ha kunnskap innenfor felt som nettverk, operativsystemer, programmeringsspråk eller som har kunnskap om ERTMS. I Henrik Børstad mastergrad NTNU 2013[10] og i Guide to industrial control systems [17] er det gitt en gjennomgang av de aktørene mot industrielle kontrollnettverk. Likheten med aktører innen cyberangrep som operer mot industriellenettverk og mot Jernbaneverkets nøkkelhåndtering er direkte sammenlignbare, disse aktørene er gjengitt i tabell 4.1 og tabell 4.2. Som disse tabellene viser, så er de potensielle aktørene mot sensitive nettverk mange. Tilgang til finansielle midler, kompetanse og politiske ressurser er det enkelte av aktørene har er svært store.

Tabell 4.1 *Oversikt over trussel og aktører innenfor cyberangrep [17] og [10]*

Trussel aktør	Beskrivelse
Angriper	Denne gruppen omfatter de som finner sikkerhetshull og bryter seg inn i systemer for å kunne høste respekt innad i miljøet. Det har tidligere krevd mye kunnskap å kunne sette i stand et slikt angrep, men oversikter over sikkerhetshull og verktøy for å utnytte disse hullene de siste årene blitt lett tilgjengelig på Internett. Dette har senket terskelen for å iverksette ondsinnede angrep, og et eksempel på en utbredt skadevare programmert av svært unge angripere.
Botnettoperatører	Botnett baser seg på at PC-er blir infisert med programvare som muliggjør fjernstyring av de infiserte maskinene. Datakraften til disse infiserte maskinene kan så bli videresolgt til en tredjepart og utnyttet til for eksempel svindel nettstormangrep eller utsendelse av søppelpost.
Kriminelle grupper	Kriminelle grupper velger sine mål etter mulighet for økonomisk gevinst, og benytter metoder som søppelpost, svindleprogramvare og spionprogramvare for å utføre identitetstyveri eller annen form for svindel.
Utenlandsk etterretningsgrupper	Etterretningsgrupper med finansiell støtte fra for eksempel forsvarsdepartementet. Gruppene kan benyttes til å samle etterretningsinformasjon, planlegge og utføre cyberangrep mot strategiske mål. Mange land har i dag et velutviklet cyberforsvar. Land som USA, Israel, Kina, Russland og etter hvert Iran og Irak står frem som store aktører innen dette feltet.

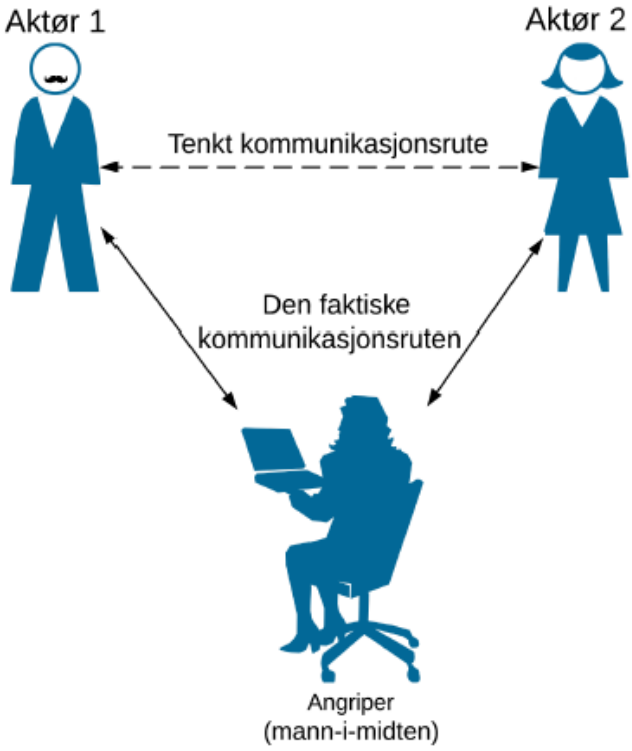
Tabell 4.2 *Oversikt over trussel og aktører innenfor cyberangrep [17] og [10]*

Trussel aktør	Beskrivelse
Innsideaktører	Personer med kjennskap eller tilgang til datasystemene kan benytte dette til sin fordel ved angrep av systemet. Dersom man har fysisk tilgang til systemene vil vanlige barrierer mot angrep kunne forbigås. Innsideaktører innebærer også tredjeparts kontraktører som bringer ondsinnet programvare inn i datasystem.
Phisere	Phisere får tak i identitetsinformasjon ved hjelp av en rekke forskjellige svindlemetoder, og benytter denne informasjonen til økonomisk gevinst. Enten direkte eller ved å videreselge informasjonen.
Spammere	Spammere tilbyr distribuering av søppel epost, gjerne med falsk informasjon for salg av produkter, distribuering av ondsinnet programvare eller for å angripe spesifikke mål. Spammere kan gjerne benytte seg av botnett for effektivt å spre spam.
Skadevareprogrammerere	Produserer skadevare for å skade et bestemt eller så mange mål som mulig ved et gitt sikkerhetshull.
Terrorister	Terrorister kan ha som mål å ødelegge eller sette kritisk infrastruktur ut av spill for å skape så store skader som mulig, enten på mennesker, miljø eller materiell. Terrorister kan også benytte phising for å finansiere sin virksomhet.
Industrispioner	Industrispionasje kan benyttes mot konkurrenter for å få innblikk i deres industrielle hemmeligheter.

I den siste tiden har det vært en del media oppslag om den falske basestasjonen for mobiltelefon ved Stortinget. Dette kan være et eksempel på utenlandsk etterretningsvirksomhet. De er spesielt ute etter informasjon av politisk art, men også

informasjon om infrastruktur, beredskap og forsvar. Under infrastruktur tilhører nøkkelhåndtering for ERTMS. Det at de allerede har kunne lage en falsk GSM basestasjon for mobil kan de være signaler på at dette også kan ramme GSM-R. GSM-R har allerede i dag en nøkkelrolle innen tog fremføring, så ved innføring av ERTMS vil dette ikke endre seg i vesentlig grad, men er en viktig faktor for hvordan vi bør organisere nøkkelhåndtering vår. Slike falske systemer kan i sin ytterste konsekvens fører til mann - i - midten angrep bedre kjent som «man in the middel attack». I [10] er dette beskrevet som der hvor angriperen plaserer seg mellom sender og mottaker som vist i figur 4.3. Dersom angriperen klarer å posisjonere, samt sikre seg at all trafikk mellom sender og

mottaker går gjennom seg selv, så vil ikke sikkerhetsmekanismer som for eksempel kryptering forebygge. Den eneste beskyttelsen mot slike angrep er at både mottaker og sender har svært strenge sikkerhetsrutiner som sørger for at angriperen ikke vil kunne komme i en slik posisjon at denne typen angrep blir mulig å gjennomføre. Dvs. en aktør kan operer som en falsk GSM-R basestasjon eller RBC ved og kommuniserer med toget med informasjon. Dette kan medføre toget for kjørsignal (grønt) selv om kravene for kjør ikke er oppfylt. Dette vil kunne medføre til avsporing eller tog – tog.



Figur 4.3 *Illustrasjon av et mann- i- midten angrep. Aktør 1 og aktør 2 har opprettet kommunikasjon, og tror at denne går direkte mellom hverandre. I virkeligheten har en angriper plassert seg mellom aktørene, og kan kontrollere all trafikk mellom dem.*

5. Erfaringer og praksis fra andre land

5.1 Innledning

Fortiden er det ikke så mange jernbaneinfrastruktur forvaltere med erfaringer med kryptonøkkelhåndtering og ERTMS. Jeg velger to land det er naturlig å sammenligne Jernbaneverket med og det er Baneverket i Sverige og Banedanmark i Danmark. Der Sverige har valgt offline nøkkelhåndtering inntil videre og Banedanmark har valgt online nøkkeldistribusjon.

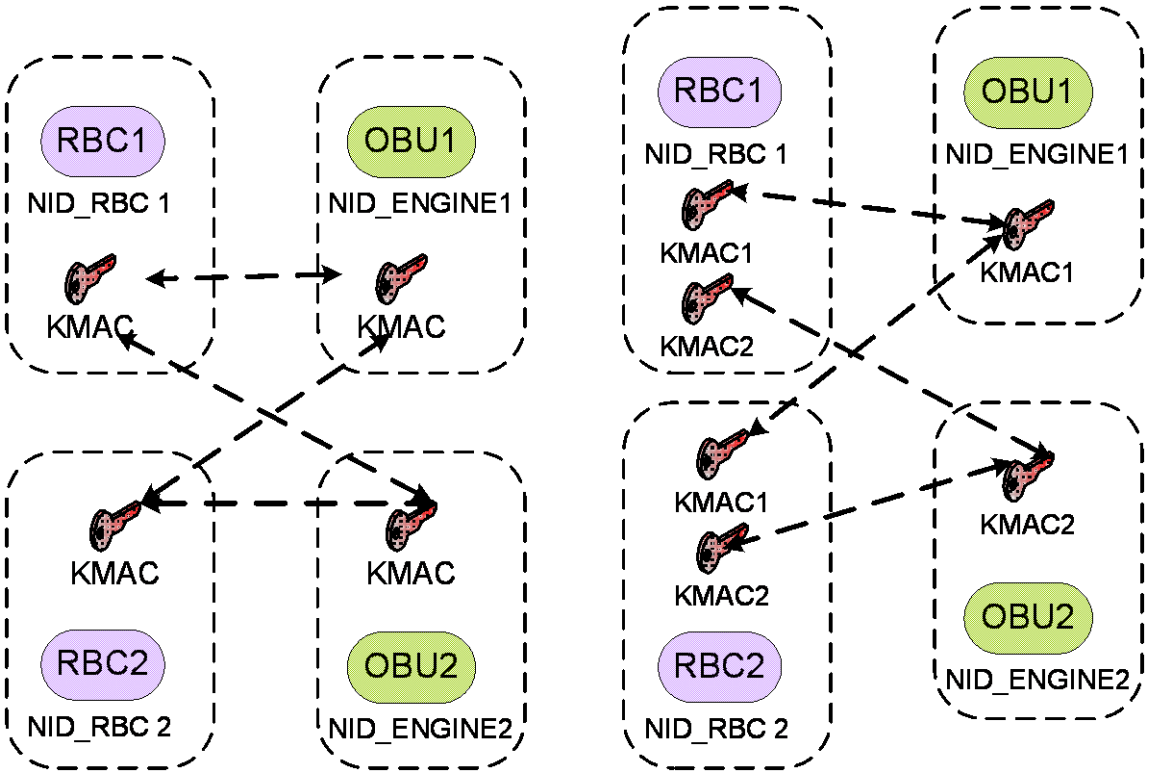
5.2 Erfaringer fra Sverige

Sverige er av de land som er mest likt Norge, når det gjelder måten å tenke overgangen fra konvensjonell til ERTMS signalanlegg. Det ble gjennomført telefonmøte med Jorge Gamels som har skrevet Hantering av krypteringsnyklar før ERTMS for Baneverket [4]. I Sverige vil de innføre ERTMS stegvis og vil være ferdig innen 2035. Implementering i Sverige vil være avhengig av nabolandenes planer og tekniske standarder. Ikke minst gjelder dette togoperatører som kjører igjennom for eksempel Danmark. Botniabanan som er fra Sundsvall til Västraspby, var første banestrekningen i Sverige med ERTMS som ble etablert i 2010. De andre banestrekningene som har fått ERTNMS er Ådalsbanan som er fra Sundsvall til Västraspby, Västerdalsbanan fra Repbäcken til Malung og Haparandebanan fra Buddbyn til Haparanda.

Den største utfordringen til Baneverket var å finne en standard for online nøkkelhåndtering, dette er ikke ferdig utviklet i ERTMS standarden pr dags dato. Med utgangspunkt i dette har Sverige valgt som Norge, en offline nøkkelhåndtering. Dette i påvente av en standard for online nøkkelhåndtering. Som Norge er det også en diskusjon i Sverige angående ansvaret for OBU (eierskap, installasjon og drift) og hvem som har det økonomiske ansvaret for innkjøp av dette. Dette er allerede blitt avklart i Danmark som jeg nærmere beskriver i kapittel 5.3.

Som Danmark har Sverige ivaretatt sikkerheten i kontrakten med Bombardier , der Bombardier sitter med ansvaret, men Baneverket har ansvaret overfor samfunnet for øvrig. Når det gjelder informasjon om hvordan selve nøkkelhåndteringen gjennomføres vil ikke Gamels utdype nærmere, enn at ulike nøkler har ulik levetid for å gjøre det mere

komplekst mot kompromittering av nøkler. Men utfra [4] finner en hvordan grupper med KMAC nøkler kan gjennomføres. Dette kan gjennomføres fordi ERTMS støtter at ulike KMAC kan brukes får kommunisere via Euroradio mellom ERTMS enheter. En ERTMS enhet kan bruke en KMAC for å kommunisere med en eller flere ERTMS enheter, en annen KMAC for å kommunisere med en annen eller andre ERTMS enheter osv. Koblingen mellom nøklene og enhetene gjøres via den unike ETCS identiteten som hver ERTMS komponent har. Tilsammen med nøklene, får en ERTMS enhet informasjon om hvilken ETCS identiteter som tilhører samme nøkkel dvs. hvilken nøkkel skal brukes ved etablering av en Euroradio forbindelse med en spesifikk ERTMS enhet. Ulike alternativer for dette vises i figur 11 hentet fra Hantering av krypteringsnyklar før ERTMS [4].



Figur 5.1 *Ulike alternativer for gruppering av KMAC[4]*

For å kunne etablere en strategi for gruppering av KMAC nøkler, ble det utført et forsøk på dette i Hantering av krypteringsnyklar før ERTMS [4]. For eksempel 2 RBC og 4 OBU, hvor mange ressurser kreves det for å gjennomføre en KMAC oppdatering, idriftsetting av ny RBC eller OBU og avinstallering av eksisterende KMAC. Tabell 5.1 beskriver antallet KMAC bytter som kreves ulike type KMAC gruppering og funksjon. De ulike KMAC grupperingen er en unik KMAC pr domene, en unik KMAC pr RBC og OBU, en unik KMAC pr RBC og

en unik KMAC pr OBU. Dette med hensyn til KMAC oppdatering, idriftsetting av ny RBC eller OBU og avinstallering av en KMAC. Det er her viktig å være OBS på at nøkkelhåndtering krever fysisk tilgang til både RBC og OBU. KTRANS vil håndteres med USB. Der KMAC er en fil som overføres via https som igjen er beskyttet med en KTRANS.

Tabell 5.1 *Ulike forslag til KMAC grupperinger [4]*

Förslag 1 – En unik KMAC per domän	**ERTMS enheter**	**Nya RBC/OBU**	**Ny RBC**	**Nya OBU**	**Uppdatera KMAC**	**Borttagning av KMAC**	**Kommentar**
	RBC 1	K1	-	-	K2	K2 bort	KMAC måste tas bort/bytas i alla RBC och OBU.
	RBC 2	-	K1	-	K2	K2 bort	
	OBU 1	K1	-	-	K2	K2 bort	
	OBU 2	-	-	-	K2	K2 bort	
	OBU 3	K1	-	K1	K2	K2 bort	
	OBU 4	K1	-	K1	K2	K2 bort	
	Ändringar	**3**	**1**	**2**	**6/-**	**6**	
Förslag 2 – En unik KMAC per par RBC/OBU	RBC 1	K1,2	-	K1,2,5,7	K10,12,15,17	K15 bort	Alla OBU/RBC får nya KMAC vid driftsättningen av en ny RBC/OBU.
	RBC 2	-	K3,4	K3,4,6,8	K13,14,16,18	-	
	OBU 1	K1	K1,3	-	K10,13	-	
	OBU 2	K2	K2,4	-	K12,14	-	
	OBU 3	-	-	K5,6	K15,16	K15 bort	
	OBU 4	-	-	K7,8	K17,18	-	
	Ändringar	**3**	**3**	**4**	**6/12**	**2**	
Förslag 3 – En unik KMAC per RBC	RBC 1	K1	-	-	K11	K11 bort	Alla OBU får nya KMAC vid driftsättningen av en ny RBC.
	RBC 2	-	K2	-	K12	-	
	OBU 1	K1	K1,2	-	K11,12	K11 bort	
	OBU 2	K1	K1,2	-	K11,12	K11 bort	
	OBU 3	-	-	K1,2	K11,12	K11 bort	
	OBU 4	-	-	K1,2	K11,12	K11 bort	
	Ändringar	**3**	**3**	**2**	**6/-**	**5**	
Förslag 4 – En unik KMAC per OBU	RBC 1	K1,2	-	K1,2,3,4	K11,12,13,14	K11 bort	Alla RBC får nya KMAC vid driftsättningen av en ny OBU.
	RBC 2	-	K1,2	K1,2,3,4	K11,12,13,14	K11 bort	
	OBU 1	K1	-	-	K11	K11 bort	
	OBU 2	K2	-	-	K12	-	
	OBU 3	-	-	K3	K13	-	
	OBU 4	-	-	K4	K14	-	
	Ändringar	**3**	**1**	**4**	**6/-**	**3**	

Det er mye som tyder på at Sverige har valgt et av disse forslagene på gruppering av KMAC nøkler i tabell 5.1. Dermed vil Sverige har ulik levetid på sine nøkler som igjen gir en bedring av sikkerheten mot kompromittering av krypteringsnøkler.

5.3 Erfaringer fra Danmark.

Siden det er lite informasjon å finne via nettet eller andre kilder, ble det arrangert et møte mellom Jernbaneverket og Banedanmark i regi av denne masteroppgaven. Møtet ble avholdt den 6. mars 2015 i København. Tilstede fra Banedanmark var prosjektleder Søren Degnegaard og medarbeider Anders Dyrekilde. Fra Jernbaneverket deltok også Roy Seland som er ansvarlig for KMC i Norge.

I Danmark har de valgt for sin nøkkelhåndtering å gjøre dette online. De vil bruke ERTMS nivå 2 med baseline 3. Danmark har som plan å være ferdig med sin ERTMS utbygging innen høsten 2021. Den første strekningen med ERTMS er planlagt i drift mai 2016.

Danmark har som Sverige ivaretatt sikkerheten igjennom sine avtaler med leverandør. Når det gjelder OBU er Banedanmark ansvarlig for denne, men de leier den ut til ulike jernbaneforetak som selv er ansvarlig for installasjon og drift. Dette for å ivareta økonomi eller budsjetter ved ERTMS implementering. Dette vil i følge Søren Degnegaard medføre og sikre fremdriften av utrulling av ERTMS uavhengig av økonomiske forhold til de ulike togoperatørene. Som kjent er dette en større diskusjon i Norge, hvordan dette skal gjennomføres. På dette punktet vil jeg støtte meg til Søren sine synspunkter.

Togene vil kjøre med GPS på baseline 3. Mye tyder på at Euroradio protokoll og autentisering blir bedre med online key management system. Det pågår nå en demokratisk prosess i ERTMS user group for å standardisere online key mangament, denne prosessen er nå ledet av Danmark.

Som tidligere nevnt har Danmark ivaretatt sikkerheten igjennom sine avtaler med leverandørene, men de har gått lengre enn Sverige på dette punktet. Danmark skal kun operasjonelt bruke det nye ERTMS anlegget, alt annet som drift, vedlikehold og sikkerhetsansvaret ligger hos leverandøren og gjennomføres med prosjektledelse fra Banedanmark. Men ved en hendelse/ulykke er Banedanmark til slutt ansvarlig overfor styrende myndigheter, men de kan legge ansvaret over på en av leverandørene. I Norge og Sverige eies og driftes GMS-R av infrastruktur ansvarlig, i Danmark er det Eltel som har ansvaret for GMS-R med utstyr levert fra Nokia. Danmark planlegger med totalt 37 RBC'er som er distribuert. Leverandøren bestemmer alt fra plassering og forrigling. Dette er også ulikt hvordan dette er tenkt gjennomført i Norge og Sverige. I Norge og Sverige er signalforriglingen infrastruktureier sitt ansvar, dette mye på grunn av at Norge og Sverige har

valgt å beholde sine egne nasjonale regelverk for togframføring. Regelverket for togframføring i Danmark fornyes ved implementering av ERTMS i tett samarbeid mellom Banedanmark og leverandører.

Danmark har valgt TLS (Transport Layer Security) for utveksling av nøkler. Dette er også en metode som støttes av NSM i Norge [18]. NSM forklarer TLS på følgende måte: TLS er en teknologi for å sikre autentisiteten til en kommunikasjons part, samt sikre konfidensialiteten til informasjonen som formidles mellom kommunikasjonspartnere. TLS er en videreutvikling av Secure Sockets Layer (SSL), som ble utviklet av Netscape på midten av 90-tallet.
Når man etablerer en forbindelse med TLS, begynner man med å forhandle hvilken versjon av SSL/TLS som skal benyttes og hvilke kryptografiske mekanismer man ønsker. Dersom klienten og tjeneren finner en versjon og kryptomekanismer de kan bli enige om, etablerer de den sikre forbindelsen. Hvis ikke, termineres forbindelsen. Banedanmark vil via TLS forbindelse distribuere KMAC nøkler. Når nøklene er distribuert vil TLS forbindelse legges ned og nøklene er installert. For å få dette til må KTRANS fjernes på et online system. I følge prosjektet bør dette lett kunne gjennomføres, da en KTRANS ikke vil ha noen funksjon via en TLS forbindelse. TLS forbindelsen vil sikre KMAC nøkkelen istedenfor KTRANS. Videre vil Banedanmark automatiserer nøkkelhåndteringen til OBU'er. Dette er planlagt gjennomført ved å installere en timer som bestemmer når nøkkel skal skiftes. Når tiden på timer er ute, vil OBU (når den er aktiv) ta kontakt med KMC å be om en ny nøkkel. Prosjektet har valgt at leverandøren er ansvarlig for prosedyrer og prosesser ved nøkkelhåndtering. Leverandøren har drift og vedlikehold ansvaret også for KMC. Men Banedanmark setter krav til dette overfor sin leverandør.

Siden mye av nøkkelhåndteringen i Danmark er leverandøren sitt ansvar, er dette en helt ny måte å håndtere nøkkelhåndtering på i forhold til det Norge og Sverige har innen dette området. Deler av denne modellen er noe som Norge bør videre ved full utrulling av ERTMS. Denne modellen har både positive og negative sider. Men Banedanmark er uansett ansvarlig ovenfor for departementet, så hvordan blir ansvarsfordelingen ved en eventuell hendelse kan bli utfordrende om dette ikke er juridisk godt nok formulert i kontrakt.

6 Risikoanalyse og diskusjon for krypto nøkkelhåndtering for ERTMS i Norge

6.1 Innledning

Som endel av denne masteroppgaven fikk vi gjennomført en risikoanalyse i samarbeid med prosjektet for test strekningen Østrelinje på ERTMS. Deltakere var fagpersoner fra ERTMS miljøet i Jernbaneverket og RAMS rådgiver fra ERTMS prosjektet. I 8-STY-603102 RAMS introduksjon og oversikt[19] Forklares RAMS på følgende måte. RAMS er en samlet betegnelse for jernbanesystemets egenskap for sikkerhet (S) og tilgjengelighet (A). Tilgjengelighet er uttrykt ved kombinasjonen av jernbaneinfrastrukturens pålitelighet (R) og i hvilken grad det er mulig å gjøre vedlikehold (M) på systemene. De tre siste parameterne utgjør til sammen RAM-egenskapene til jernbaneinfrastrukturen. Som en del av masteroppgaven er Risikoanalyse KMS nøkkelhåndtering vedlagt som er et resultat av dette arbeidet. Dette dokumentet har dokumentnummer ERT-10-Q-00248 Rev 00E i Jernbaneverkets dokumentarkiv. Dokumentet er et grunnlag for min videre analyse, men jeg vil utvide måten å analysere på her i denne oppgaven ved å ta med mine egne vurderinger og analyser.

6.2 Bakgrunn for hvorfor risikoanalyse

En risikoanalyse er en del av RAMS-arbeidet i jernbaneverket. I 8-STY-603102 RAMS introduksjon og oversikt [19] sies det videre Jernbaneverket opererer med mål for vår drift satte jernbaneinfrastruktur, hvor følgende målområder er av relevans for vårt RAMS-arbeid:

- sikkerhet
- punktlighet (antall tog i rute til endestasjon)
- regularitet (antall innstilte tog i henhold til ruteplan)
- oppetid (forsinkelsesnivå i togtrafikken)

Målene for perioden 2014 – 2023 fremkommer av nasjonal transportplan [21]. I tabell 6.1 er målene som nasjonal transportplan har satt for perioden 2014-2023.

Tabell 6.1 *Mål for punktlighet, regularitet og oppetid hentet fra nasjonal transportplan 2014-2023 [19]og [20]*

	Status 2012	Mål 2017	Mål 2023
Punktlighet for Gardermobanen i pst.	96,2	95,0	95,0
Punktlighet for persontog i pst.	91,2	90,0	90,0
Punktlighet for godstog i pst.	81,0	90,0	90,0
Oppetid i pst.	98,8	99,3	99,3
Regularitet for persontog i pst	97,8	99,0	99,2

Oppetid er et uttrykk for jernbaneinfrastrukturens tilgjengelighet. Jernbaneverket har definert oppetid som mål for jernbaneinfrastrukturens tilgjengelighet. Oppetid er av Jernbaneverket brukt for å beskrive forsinkelsesnivået i form av forsinkelsestimer.

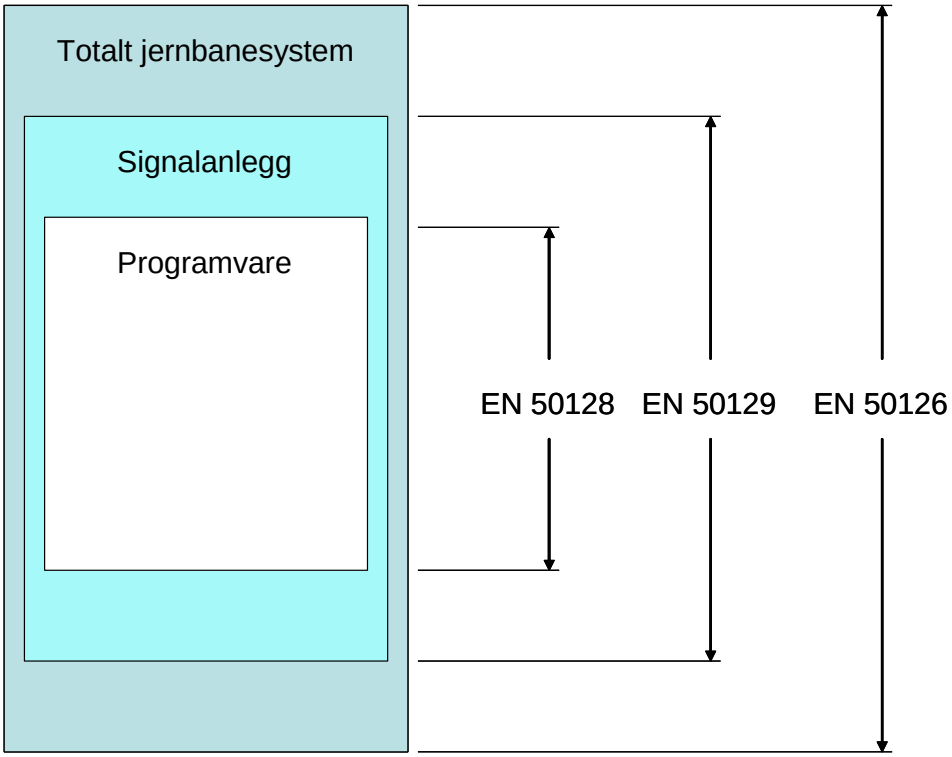
Oppetid = Togtimer – Forsinkelsestiner / Togtimer.

Jernbaneverkets oppnåelse av krav til oppetid forutsetter at det i størst mulig grad er en feilfri og tilgjengelig jernbaneinfrastruktur for togtrafikk. Feil på jernbaneinfrastrukturen og eller manglende evne til vedlikehold, vil kunne bidra til et forsinkelsesnivå som påvirker den planlagte togproduksjonen, enten ved at togene blir innstilt (regularitet) eller ved at de ikke ankommer endestasjonen i henhold til planlagt ruteplan (punktlighet).

Jernbaneverket definerer en forsinkelse som et tog som er mere enn 5 minutt forsinket i henhold til planlagt ruteplan til endestasjon. Jernbaneverket utfører RAMS arbeid på grunnlag av ulike standarder og får å oppfylle de krav de stiller. I8-STY-603102 RAMS introduksjon og oversikt [19] forklares de forskjellige standardenes funksjoner, som kan beskrives som følgende:

- EN 50126 adresserer systemaspekter i vid forstand og favner det totale jernbanesystemet.
- En 50128 fokuserer på metoder som skal benyttes for å frambringe programvare som møter kravene til sikkerhetsintegritet.
- En 50129 adresserer godkjenningsprosessen for individuelle systemer innenfor det overordnede systemet for kontroll og sikring av jernbanen.

I figur 6.1 illustreres hvordan de ulike standardene har innflytelse/krav til de ulike delene i et jernbanesystem.



Figur 6.1 *De forskjellige standardenes fungerende område i et jernbanesystem[12]*

Når vi ser på RAMS og hvilke krav for oppetid som gjelder for jernbanen, er nøkkelhåndteringen i ERTMS en vesentlig del for å oppnå de mål som nasjonal transportplan har satt overfor jernbaneverket. Nøkkelhåndtering vil også være en del av sikkerheten selv om det i dag er definert som SIL (Safety Integrity Level) 0 system dvs. ikke sikkerhetskritisk. I 8-STY-603102 RAMS introduksjon og oversikt [19] sier de følgende om SIL. I enhver tilnærming til risiko vil det være nødvendig å skille mellom systematiske og tilfeldige feil. Systematiske feil er relatert til resultatene av menneskelige feilgrep, eksempelvis feil i programvare, designfeil, etc. Tilfeldige feil er på sin side relatert til svikt og forstyrrelser som skjer som resultat av rene fysiske forhold, for eksempel svikt i et relé, korrosjon, materialtretthet, etc. Erfaring fra sikkerhetskritiske systemer indikerer at systematiske feil har et større farepotensiale enn tilfeldige feil.

På basis av en grundig analyse tilordnes systemet et sikkerhetsintegritetsnivå (safety integrity level, SIL), som igjen bestemmer hvilke metoder som skal benyttes for design og implementering av systemet. Høyere nivå gir strengere krav til valg av metoder. Generelt skal alle systemer som kan ha innflytelse på sikkerhet tilordnes et sikkerhetsintegritetsnivå. Når

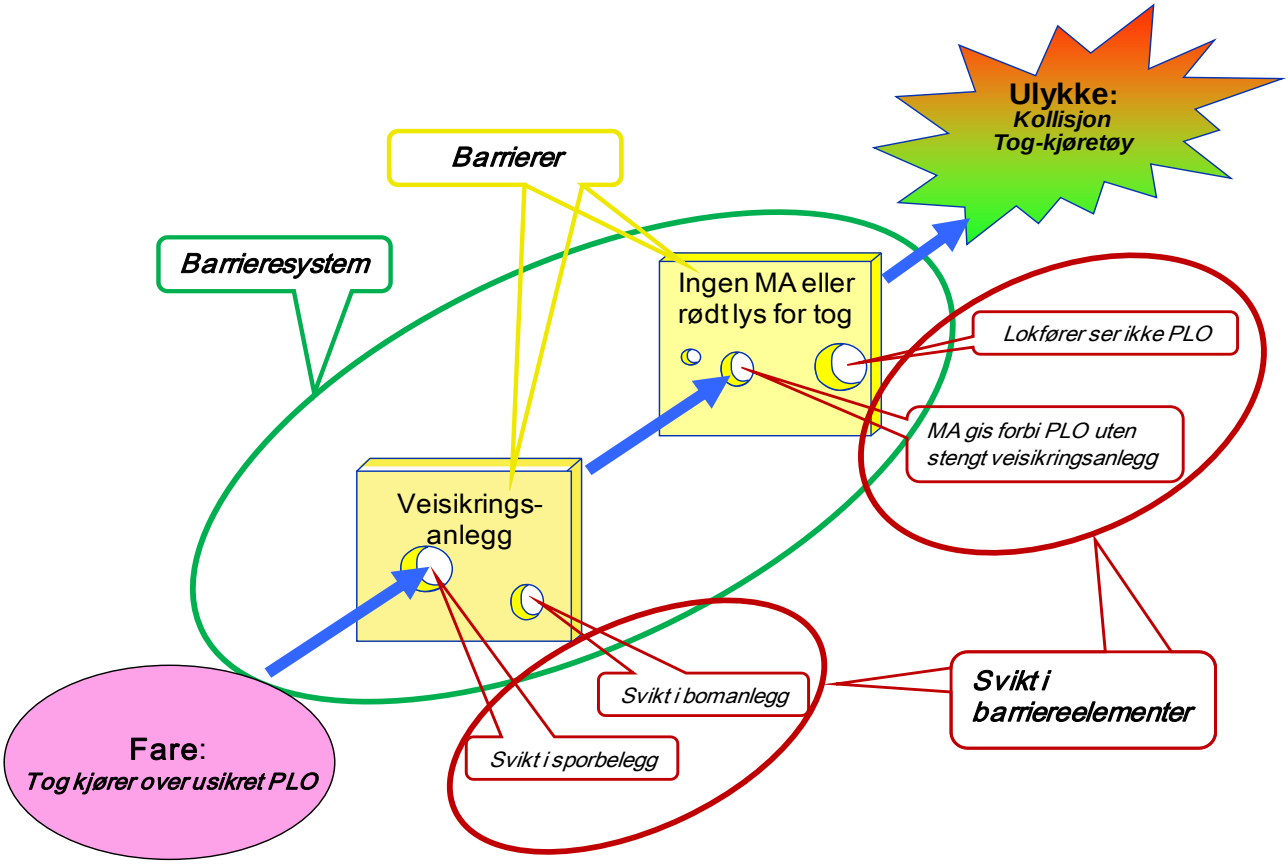
det gjelder nøkkelhåndtering så har den isolert sett SIL 0. Mange vil her mene at dette er feil, siden kommunikasjonen mellom RBC og tog sikrer en sikker togframføring. Men i sammenhengen med kommunikasjonen RBC og tog vil dette ha en SIL verdi i systemet som en enhet. Men igjen kan vi ta dette videre ved å se på sikkerhetsbegrepet. I 8-STY-603102 RAMS introduksjon og oversikt [19] sier dem følgende om sikkerhetsbegrepet. For effektiv sikkerhetsledelse er det selvsagt viktig å definere hva sikkerhetsbegrepet innebærer. Dette er av betydning ikke bare den for praktiske gjennomføringen av sikkerhetsarbeidet, men også for forståelsen av jernbanevirksomhetens juridiske ansvar med hensyn til sikkerheten av de systemene den forvalter. Utviklingen i Europa i retning av større bruk av kryssaksept krever dessuten at sikkerhetsbegrepet defineres likt i de forskjellige landene. Dette er en viktig forutsetning i CENELEC-normene, og er også reflektert i europeisk lovgivning. Viktig i så henseende er direktiv 2004/49/EC vedrørende jernbanesikkerhet (sikkerhetsdirektivet), som i Norge er representert gjennom Sikkerhetsstyringsforskriften. Direktivet krever at ERA (European Railway Agency) utarbeider forslag til felles sikkerhetsmetoder og sikkerhetsmål. Sikkerhetsdirektivet omfatter imidlertid mer enn funksjonssikkerhet, som er fokus for CENELEC-normene. Andre aktuelle forhold som også er dekket av direktivet er elektrisk sikkerhet, brannforebygging, elektromagnetisk kompatibilitet, etc. Direktivet skal legge til rette for sammenligning og optimalisering av sikkerheten ved europeiske jernbaner, blant annet ved en gradvis innføring av felles sikkerhetsmål på overordnet systemnivå og felles sikkerhetsmetoder.

Ved en risikoanalyse vurderes også de ulike barrierer et system vil ha. En barriere er et hinder for at en ulykke skjer for eksempel tog – tog. Til flere barrierer et system samlet har før en topphendelse, mere robust er systemet mot en ulykke. I tabell 6.2 forklares de ulike barrieretypene vi i Jernbaneverket operer med.

Tabell 6.2 *Barrieretyper vi operer med i Jernbaneverket*

Barrieretyper		"Styrke"
Fysiske barrierer: dvs. en konstruksjon som fysisk hindrer en feil handling/feilutvikling å eskalere til en ulykke **Eksempel**: Ledeskinne, sporsperre, parallell redundans, etc.		12 *(Bedre)* 11 *(Normalt god)* 10 *(Dårligere)*
Funksjonell barriere: dvs. et system som skaper et vilkår som må oppfylles for at en riktig handling/aktivering av funksjon skal kunne utføres. **Eksempel**: ATC, traksjonssperre, etc.		9 *(Bedre)* 8 *(Normalt god)* 7 *(Dårligere)*
Symbolske barrierer: dvs. skilting, merking og lignende som gir en åpenbar indikering for å utføre en riktig handling. **Eksempel**: En symbolsk barriere en vedlikeholdsaktivitet hvor kontrollobjekt og inspeksjonskriterium er gitt i spesifikk prosedyre		6 *(Bedre)* 5 *(Normalt god)* 4 *(Dårligere)*
Immatrielle barrierer: dvs. regelverk, reglementer, prosedyrer, opplæring og sikkerhetskultur som gir mennesket i organisasjonen kunnskap, erfaring, holdninger og atferd for å utløse en riktig handling. **Eksempel**: En immateriell barriere kan være en vedlikeholdsaktivitet hvor deteksjon er avhengig av personens kunnskap og erfaring		3 *(Bedre)* 2 *(Normalt god)* 1 *(Dårligere)*

I figur 6.2 illustreres hvordan ulike barriere kan forseres og en topphendelse kan oppstå. Figuren viser et eksempel fra et veisikringsanlegg.



Figur 6.2 *Eksempel på barrierer for et veisikringsanlegg og mulighet for svikt som kan føre til en av Jernbaneverkets topphendelser*

En risikoanalyse skal avdekke om standardene er fulgt, sikkerheten er ivaretatt og barrierene er gode nok for et delsystem eller systemet som helhet. Risikoanalysen som gjennomføres i denne oppgaven har kun fokus på nøkkelhåndtering i forbindelse med ERTMS og eventuelt sikring av viktige fysiske komponenter i den forbindelse.

6.3 Risikoanalyse og diskusjon

Fokuset for analysen gjort i samarbeid med Østrelinje prosjektet er å vurdere trusler og risikoer ved nøkkelhåndtering, vurdere levetid for nøkler og komme med anbefalinger til hvordan sikkerheten kan ivaretas på best mulig måte. Fokus vil være identifikasjon av ulike farer eller trusler for hvert system eller område. Derigjennom å vurdere barriere og mulige tiltak for å unngå uønskede hendelser eller ulykker. I Tabell 6.3 vises en

oppsummering av de farer vi fant med mulige tiltak for å unngå uønskede hendelser eller ulykker. I arbeidet med Risikoanalysen KMS nøkkelhåndtering.

Tabell 6.3 *Risikoanalysens indentifiserte farer, funn, tiltak og vurdering [vedlegg]*

System/område	Fare	Hvordan/hvem?	Eksisterende barrierer	Vurdering av eksisterende barrierer	Mulige tiltak	Kommentar
Falsk MA	**Pirat-RBC sender farlig MA med en gyldig nøkkel**	**Se Id 1-9 under**	**Se Id 1-9 under**	**Se Id 1-9 under**	**Se Id 1-9 under**	**Dette er topphendelsen. Id. 1 – 9 under er mulige basishendelser som, i kombinasjon med en pirat-RBC, kan føre til topphendelsen.**
Nøkkel (KMAC)	Mister USB med nøkkel (USB brukt til overføring fra tekniker PC til RBC (pr. i dag ikke mulig til tog)	Tekniker mister nøkkel eller kontroll på den	• KTRANS kryptering av USB • Fysisk sikring av USB • Opplæring og godkjenning av personell	Vurderes som god, men security USB og sikkerhetssamtale bør vurderes	• Ikke bruk USB • Security USB • Sikkerhetsklarering av personell (også eksterne) • Årlig sikkerhetssamtale • Må være JBV/NSB-ansatt?	USB må kunne brukes, men den bør da være en security USB
	Tekniker mister nøkkel fordi den ikke er slettet etter håndtering – funnet av angriper	Tekniker glemmer å slette nøkkel fra sin PC	Systemet er bygget opp slik at tekniker skal slette filen når den er lastet over (prosedyre)	Vurderes som god, men dedikerte JBV PC-er eller egen USB med nødvendig programvare og sikkerhetssamtale bør vurderes.	• Dedikerte PC-er (kan være under JBV-kontroll og eiendom) • Må være JBV/NSB-ansatt • Sikkerhetsklarering av personell (også eksterne). • Årlig sikkerhetssamtale • Egen USB med nødv. OS/programvare	Prosedyre krever at tekniker sletter nøkkel etter spørsmål fra systemet. Norsk sikkerhetsklarering kan være et problem fordi tekniker kan være fra utenlandsk leverandør. Sikker sletting av nøkkel på en vanlig PC anses som en utfordring i dag.
Kryptering	"Re-play attack" pga. utilstrekkelig tilfeldighet i generator	Pga. utilstrekkelig tilfeldighet kan angriper se at det kommer en	• True random generator er implementert • Sertifisert implementasjon av FIPS	True random generator (sertifisert av FIPS) anses som en god nok barriere og at		

System/område	Fare	Hvordan/hvem?	Eksisterende barrierer	Vurdering av eksisterende barrierer	Mulige tiltak	Kommentar
	eller dårlig implementasjon av algoritme	lik melding som tidligere		OBU med GCD forutsettes å ha true random generator for session key		
		"Long key exposure time"	Nøkkellengde sikrer stort antall kombinasjoner	Ingen reell risiko innenfor levetiden til systemet (maks 5 år)		
		Key re-use	Bruker forskjellige nøkler til hvert tog	God nok forutsatt at GCD har true random generator		
Code security	Angriper får adgang til systemet (KMS)	Angriper får lurt virus inn i KMS via USB-pinne ("Stuxnet")	• Minnebrikker må være forhåndsgodkjent. • Fysisk sikring av lokasjon. • Adgangskontroll. • KMS-server er beskyttet av en aksess-ID for hver bruker.	Vurderes som god nok fordi barrierene består av flere kombinasjoner (både fysisk og teknisk tilgang)		
	Angriper får tilgang til OBU	Får lastet inn ny SW i OBU via innlasting av nøkkel	Fysisk sikring av OBU med GCD	Vurderes ikke her da det er togoperatørens ansvar	Togoperatøren må ha god nok fysisk sikring og rutiner	
		Får lastet inn SW med virus i GCD ifm. innlasting av nøkkel	• Ny SW er utstyrt med en checksum? (denne barrieren flyttes til tiltak hvis det ikke er tilfelle p.t.) • Testleder/sluttkontrollør vil sjekke installasjonen (uavhengig av installatør)	Vurderes som god nok forutsatt gode prosedyrer for testleder/sluttkontrollør	• Eget (JBV/NSB) teknisk utstyr benyttes. • Vurdere å implementere checksum dersom dette ikke eksisterer (gjelder Bombardier)	
"Ser over skulder"	Angriper får adgang til systemet eller nøkkel	Angriper ser nøkkel eller adgangs-informasjon over skulder på operatør	• Nøkkel vises ikke i klartekst • Tilgangskontroll • Instruks og opplæring	Vurderes som god nok fordi barrierene består av flere kombinasjoner (både fysisk og teknisk tilgang)		
Key Management Database	Angriper får adgang til systemet	Ekstern aktør	• KMD er ikke knyttet til internett • Adgangskontroll • Fysisk sikring • Passordbeskyttelse • Kryptert innhold	Vurderes som god nok fordi barrierene består av flere kombinasjoner (både fysisk og teknisk tilgang)		
		Intern: Utro tjener	• Passordbeskyttelse	Vurderes som god, men mulige	• Må være JBV-ansatt	

System/område	Fare	Hvordan/hvem?	Eksisterende barrierer	Vurdering av eksisterende barrierer	Mulige tiltak	Kommentar
			• Adgangskontroll	tiltak må vurderes	• Sikkerhetsklarering av personell (også eksterne) • Årlig sikkerhetssamtale	
RBC	Angriper får adgang til systemet	Ekstern aktør	• Adgangskontroll • Fysisk sikring • Passordbeskyttelse	Vurderes som god nok fordi barrierene består av flere kombinasjoner (både fysisk og teknisk tilgang)		Det forutsettes rutine for passordadministrasjon
		Intern: Utro tjener	• Passordbeskyttelse Instruks og opplæring • Adgangskontroll med logg	Vurderes som god, men mulige tiltak må vurderes	• Må være JBV-ansatt • Sikkerhetsklarering av personell (også eksterne) • Årlig sikkerhetssamtale	
OBU	Angriper får adgang til systemet	Ekstern: Under hensetting	• Adgangskontroll • Vakthold • Fysisk sikring	Vurderes som god, men det er togoperatørens ansvar.	Alarmsystem	Ansvar til togoperatør. Utenfor scope til nøkkelhåndtering
		Intern: Togpersonell	• Opplæring og godkjenning av personell • Ikke mulig å få nøkkel ut av GCD	Vurderes som god, men det er togoperatørens ansvar.		Ansvar til togoperatør. Utenfor scope til nøkkelhåndtering
Key Management Distribution Server	Angriper får adgang til systemet	Ekstern aktør	• Brukernavn/password • Fysisk sikring • Adangskontroll • Fysisk plassering (annet sted enn KMS) • Tilknyttet DMZ • Tidsbegrensning for datalagring på server	Vurderes som god nok fordi barrierene består av flere kombinasjoner (både fysisk og teknisk tilgang)		
		Intern: Utro tjener	• Passordbeskyttelse Instruks og opplæring • Adgangskontroll	Vurderes som god, men mulige tiltak må vurderes	• Må være JBV-ansatt • Sikkerhetsklarering av personell (også eksterne) • Årlig sikkerhetssamtale	
Ansatte	Angrep fra ansatt som slutter	"Intern": Utro tjener		Vurderes som god nok forutsatt gode nok	Sjekk at prosedyrer for avslutning av	

System/område	Fare	Hvordan/hvem?	Eksisterende barrierer	Vurdering av eksisterende barrierer	Mulige tiltak	Kommentar
				prosedyrer for avslutning av arbeidsforhold	rettigheter, tilganger, passord, osv. er gode nok	

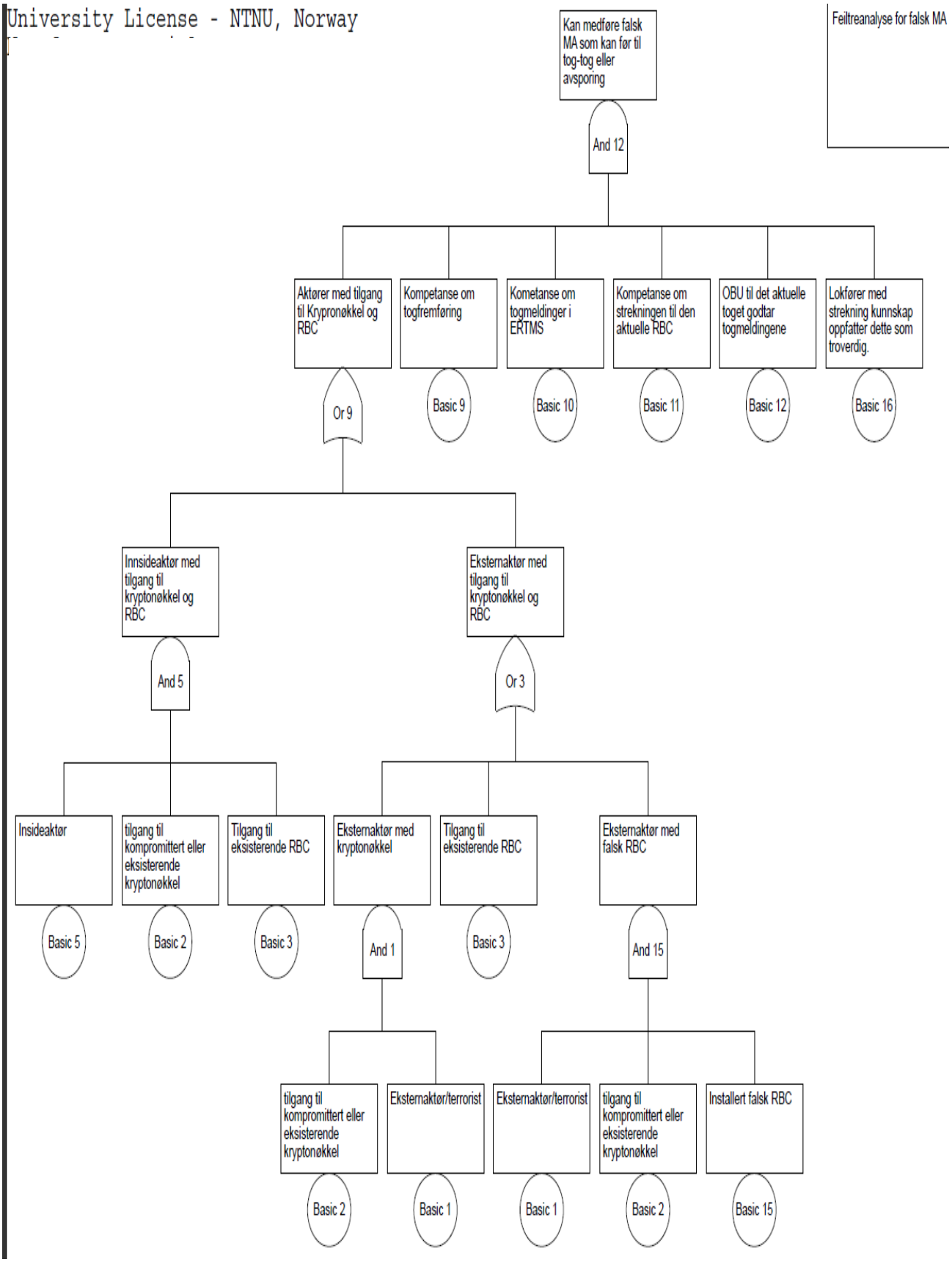
Alle vurderingene er gjort med utgangspunkt i den trusselvurderingen som er gjort i kapittel 3.

Denne analysen resulterte i tiltak, her er det viktigste:

1. Ikke bruk USB .
2. Om USB benyttes bruk security-USB.
3. Sikkerhetsklarering av internt og eksternt personell.
4. Årlig sikkerhetssamtale.
5. Dedikerte PCer for nøkkelhåndtering.
6. Innføring av checksum ved nøkkelbytte om dette ikke allerede eksisterer.
7. Innføring av gode prosedyrer og rutiner i forbindelse med at personell slutter i jobben.

Dette er tiltak som kan godt forankret i både trusselvurdering og risikofaktorer. I tillegg til at analysen har vurdert mulige systemer/områder som er mest sårbare ved nøkkelhåndtering dette er områder som for eksempel: Nøkkel, RBC, OBU, interne og eksterne ansatte.

Jeg vil videre se på hvordan en «falsk» MA kan oppstå ved en feiltreanalyse. Figur 6.3. viser feiltre for hvordan en slik falsk MA kan oppstå. I denne analysen er også «falsk» RBC vurdert, noen som ikke var vurdert i Risikoanalysen. Som figur 6.3 viser så er det mange barrierer før en falsk MA kan bli reel. De største barrierene er kompetanse innen togframføring, strekning og RBC meldinger til og fra tog som en aktør må kunne for å kunne gi en troverdig falsk MA. Siste barriere vil være lokfører med strekningskunnskap som må oppfatte den falske MA som troverdig for strekningen.



Figur 6.3 *Feiltreanalyse med topphendelse falsk MA*

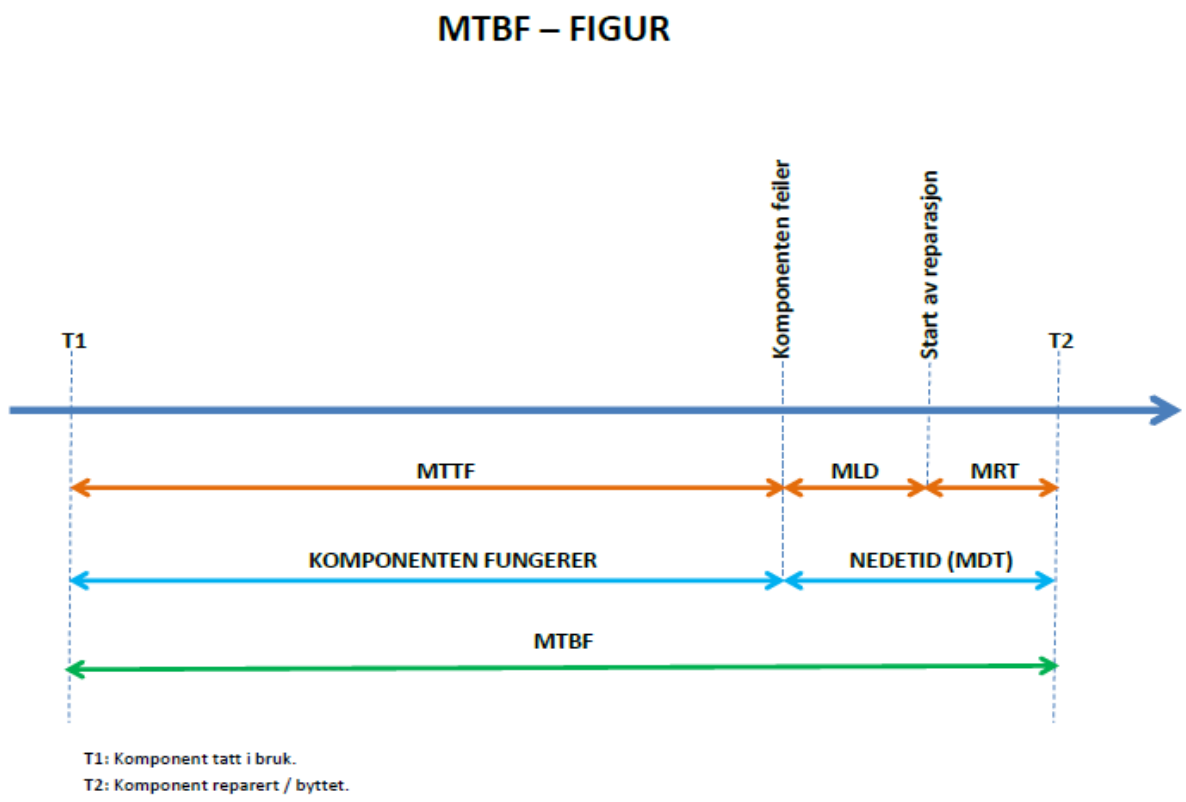
Som feiltreanalysen viser må aktører både internt og eksternt ha tilgang til kryptoinformasjon. Kryptoalgoritmen som benyttes er trippel DES. Teoretisk vil det ta ca 25 år før en hacker kan bryte nøkkelen. Fra Subset-038: Off-line Key Management FIS. 2005, v 2.1.9 [20] er det en beregning på dette. Se figur 6.4 som er viser denne beregningen.

6.4.2.4 According to the EFF Deep Crack (http://www.eff.org/Privacy/Crypto/Crypto_misc/DESCracker/) a 250,000 $ machine can crack a simple DES (56-bit key) in 22 hours. However, key protection uses triple DES which means that it contains at least three DES cumulative calculation. By approximation a 168-bit key is cracked in $\frac{22 \bullet 2^{167}}{2^{55}} = 22 \bullet 10^{112}$ hours with a 250,000 $ machine. Moreover, Moore's "law" which has not yet been refuted, states that "speed of computers doubles every 18 months". With this law and with the requirements that this specification will be valid for 25 years,

Figur 6.4 *Beregninger av levetid for nøkkel med trippel DES kryptering [20]*

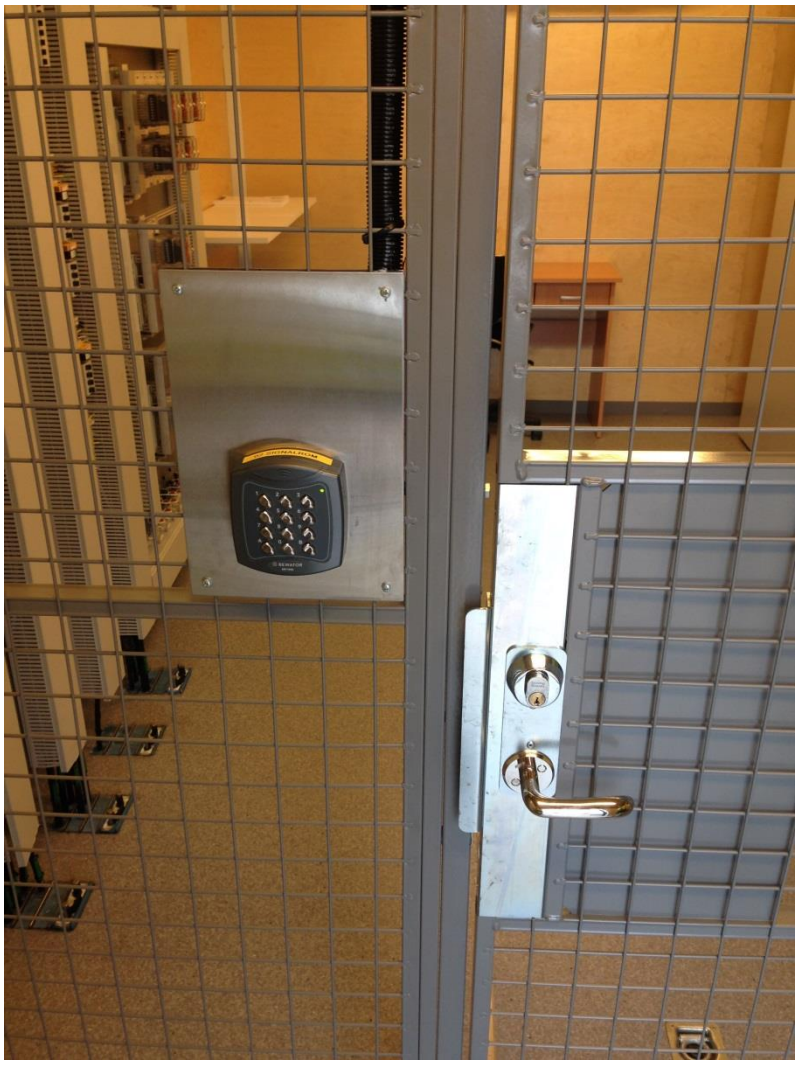
Men som beskrevet i kapittel 4 er dagens situasjon en hel annen. Angrep eller hacking som for et par år siden hendte to til tre ganger i året skjer nå daglig. Jeg ser på OBU som den minst beskytta og fysisksikret enheten i ERTMS systemet. Dermed er denne mest sårbar. Samtidig har GCD i OBU en begrenset levetid på grunn av levetiden av backup batteriene, som har en levetid på maksimalt fem år. Med støtte hos NSM vil jeg begrense levetiden til kryptonøkkelen til OBU til maksimalt tre år. Kryptonøkkel for RBC som bør være bedre beskyttet enn OBU, vil jeg anslå en maksimal levetid på fem år. Dette tema var også drøftet under møte med NSM. Der er NSM var klare på at levetid på kryptonøkler over syv til ti år er urealistisk med dagens teknologi. Men de var også klare på ved offline nøkkelbytte er også denne delen en sårbar operasjon i seg selv. Det er min påstand at slik type informasjon beskyttes best gjennom en organisasjon som er bygget på en sikkerhetskultur i alle ledd. Dette er uavhengig av hvilken type kryptoalgoritme som benyttes. Det er organisasjonen som til slutt utgjør sikkerheten. Det som har en betydning når det gjelder dagens tilgjengelige standard for nøkkelhåndtering i ERTMS som er offline håndtering, er tiden det tar å bytte nøkkel. Fra en situasjon eller trussel oppstår til alle nøkler er bytte kan ta lang tid. Vi snakker om fra 12 timer til 1-2 dager nedetid alt

etter hvor mange nøkler som må byttes. Hver enkelt OBU har sin egen definerte nøkkel som er registret i en database i den aktuelle RBC som toget skal benytte for en strekning. Dette medfører at RBC er en veldig sårbar enhet som inneholder store mengder kryptoinformasjon. En hacking av informasjon i en RBC har størst skade omfang. Det derfor denne er godt fysisk sikret. For det enkelte tog er det viktig at OBU med GCD er tilstrekkelig beskyttet også når toget er parkert. Ved et online system vil tilsvarende hendelse ha liten betydning. Da kan nøklet distribueres raskt både til OBU'er og nye nøkkeldatabaser installeres raskt i RBC'er. Tiden en kan forventes seg med et slikt system er ca 2-4 timer nedetid. Figur 6.5 viser en sammenheng mellom MTBF (Mean Time Between failure), MTTF (Mean Time To Failure), MDT (Mean Down Time), MRT (Mean Repair Time) og MLD (Mean Logistic Time). Der MRT er den tiden vi har på å rette feilen som er nedetiden til systemet. Når vi ser dette i sammenheng med oppetidskravet fra NTP[21] på 99,3 % der oppetid er definert som tilgjengelighet til infrastrukturen. Min påstand er en utrulling av mange ERTMS strekninger ikke kan gjennomføres ved offline nøkkelhåndtering. Dette fordi en reinstallasjon av nye versjoner av nøkler tar for lang tid i forholdet til dette kravet og risikoen blir for stor i forhold til oppetidskravet. Dette betyr at MLD er for lang i forhold til kravet fra NTP.



Figur 6.5 *Sammenhengen mellom MTBF,MDT, MTTF,MLD og MRT*

Mine observasjoner er at det lite eller ingenting som gjøres på dette området i Jernbaneverket. Under er figur 6.6 som viser en ERTMS installasjon som er gjennomført på et sted på Østlandet. Som figuren viser er det lite eller ingen skikkelig beskyttelse. Det mangler alarm og utstyret er installert i et «vanlig» teknisk hus med universalnøkkel. For at dette skal være en sikkerinstallasjon må teknisk hus være utstyrt med adgangsalarm på inngangsdører. ERTMS utstyret installeres i et eget rom som er utført i betong for tak, vegger og gulv med en solid jern- eller ståldør med kodelås og ny adgangsalarm. Da vil installasjonen være beskytte mot inntrengere. Inntil eventuelt vaktselskap har rykket ut, og eventuelt avverget inntrengeren å få tilgang til ERTMS utstyret. Det forutsettes at tidsbruken for å komme gjennom en jern- eller ståldør med skikkelig lås funksjon er lengre enn utrykningstid til vaktselskap. En gitterdør som figur 6.6 viser kan lett klippes adgang i uten å benytte døren eller utløse eventuelt alarmer.



Figur 6.6 *Eksempel på sikring av ERTMS installasjon i Jernbaneverket et sted på Østlandet*

Min antagelse er når det gjelder krypteringsnøkkelhåndteringen i Jernbaneverket vil den største trusselen komme fra egne ansatte, innleide eller leverandør personell. Dette kan være ubevist eller beviste handlinger som kan medfører en til en uønsket hendelse. Dette blir bekreftet i artikkel fra Teknisk Ukeblad tittel Britisk ekspert, nye signalanlegg kan bli mål for terrorister [22] som kom ut kun få dager før jeg skulle levere denne masteroppgaven. Der Professor Stupples ekspert og rådgiver for britiske myndigheter sier følgende. Signalsystemet er alt i bruk i andre steder i verden, og det har så langt ikke vært rapportert om noen digitale angrep på anlegget.

Systemet i seg selv er utviklet for å øke sikkerheten, ved å redusere risikoen for menneskelig feil.

Professor Stupples mener likevel at hackere utgjør en reell trussel, som kan forårsake stygge ulykker. Han understreker at systemet er beskyttet mot angrep fra utsiden, og at trusselen vil måtte komme fra en på innsiden.

– En utro ansatt vil kunne infisere systemet, mener han.

Dette samsvarer godt med fokuset denne oppgaven representerer. Etter denne artikkelen skjer det nå tiltak i Jernbaneverket. Min vurdering er at Jernbaneverket har både endringsvilje og opparbeider kompetanse på en slik måte at de kan komme godt i gang med en ny organisasjon og sikkerhetskultur som er velfungerende. Sikkerheten ligger i hvordan Jernbaneverket velger å organisere og utvikle kontinuerlig sin sikkerhetskultur og sikkerhetsarbeid i forbindelse med ERTMS i Norge.

På bakgrunn av innsamlet materiale foreslås flere tiltak og anbefalinger til Jernbaneverket. Det viktigste tiltaket er å etablere en god kultur for sikkerhet som et mål for hele organisasjonen, inkludert ledelsen. Funnene som er gjort gjennom arbeidet med oppgaven tyder på at dette er en oppgave som Jernbaneverket ikke har vært villig til å ta, resultatet blir da at det ikke blir tatt grep i organisering og fysisk sikring av kritiske systemer eller personell. Jernbaneverket anbefales å starte arbeidet med fysisk sikring og etablering av en god sikkerhetskultur i sin organisasjon. Jernbaneverket bør sikkerhetsklarer ansatte som arbeider i KMC eller på annen måte jobber med nøkkelhåndtering med klarering «HEMMELIG» med påfølgende kurs. Det bør også utnevnes en sikkerhetsleder for KMC. Sikkerhetsleder gjennomfører en årlig sikkerhetssamtale med alle ansatte ved KMC engang i året. Jernbaneverket anbefalelses videre å følge de krav NSM setter for krypteringsalgoritmer. Jernbaneverket bør også være en pådriver overfor ERA (European Railway Agency) for å få implementert AES og en standard for online nøkkelhåndtering i ERTMS. Dette i tett samarbeid med Danmark som planlegger online nøkkelhåndtering. Det anbefalelses å ivareta sikkerhetsarbeidet i kontrakten med leverandør. Der ansvarsområde angående sikkerhet og ansvar for sikkerheten til enkelte komponenter tydelig gjøres, dette anses som den viktigste delen i forbindelse med nøkkelhåndtering der leverandør også er involvert.

Når det gjelder levetid for de ulike krypteringsnøklene tar jeg utgangspunkt i OBU (Ombord Utrustningen) til togene, da denne delen er dårligst sikret å fare for nøkkel kompromittering er størst. GCD (Generic Crypto Device) som er en del av OBU'en har en levetid på maksimalt fem år på grunn av backup batterienes levetid.

Det anbefales at nøkkel for OBU har en levetid på maksimalt tre år. For RBC (Radio Block Center) som anses som bedre sikret, anbefales en levetid på maksimalt fem år. Inntil videre anbefales det å arbeide med de tiltak som er beskrevet. Jernbaneverket må samarbeide med Danmark og ERA, for å ta nøkkelhåndterings standard i ERTMS teknologisk videre og for å forbedre sikkerheten i ERTMS kontinuerlig.

7 Forslag til videre arbeid

For å utvikle kryptonøkkelhåndtering i ERTMS videre fra den standarden den er i dag, må Jernbaneverket være med å bidra aktivt i ERA og samarbeid med andre EU-land. Dette er en evigvarende prosess som EU må arbeide kontinuerlig med. Jernbaneverket bør starte arbeidet med å etablere en bedre sikkerhetskultur i sin organisasjon, som er bedre enn den som oppleves blant ansatte i dag. En viktig milepæl for videre utvikling av kryptonøkkelhåndtering i ERTMS er å utvikle en online nøkkelhåndteringsstandard for dette. Dette for å gjøre systemet mere robust å kunne imøtekomme de sikkerhets- og oppetidskrav som stilles til jernbanen i Europa. Derigjennom kan Jernbaneverket imøtekomme de krav Samferdselsdepartementet har vedtatt i NTP ovenfor jernbaneinfrastrukturen i Norge.

8 Referanseliste/bibliografi

[1] ERTMS National Implementation 12.6.2014-ver 001 av Jernbaneverket

[2] ETCS for Engineers av Peter Stanley (Editor)

[3] http://www.jernbaneverket.no/no/Jernbanen/Jernbanedrift---eit-komplisert-samspel/Jernbaneverket-satser-pa-ny-teknologi-for-signalanlegg/ Publisert av Njål Svingheim, 19.07.2010, lest 20.10.2014

[4] Hantering av krypteringsnyklar før ERTMS, KMS08-02, dato 08-10-31 av Jorge Gamelas

[5] UNISIG EuroRadio FIS Ref: Subset-037 ISSUE: 3.0.0 Date:2 mar 2012

[6] NOU 2000: 24 Et sårbart samfunn. Utfordringer for sikkerhets-og beredskapsarbeidet i samfunnet. Utgitt av Justis- og politidepartementet 4 juli 2000. http://www.dinkom.no/Global/Dokumenter/Politiske%20dokumenter/NOU%202000%2024%20Et%20s%C3%A5rbart%20samfunn.pdf , lest 22.12.2014

[7] http://www.aftenposten.no/nyheter/iriks/PST-Trusselbildet-mot-Norge-er-ikke-endret-7852401.html Lest 22.01.2015

[8] http://www.vg.no/nyheter/innenriks/forsvaret/slik-kan-norge-bli-cyber-angrepet/a/10103585/ Lest 22.01.2015

[9] Johnsen, S.O (2012a). An investigation of Resilience complex socio-Technical systems to improve safety and continuity Integrated Operations. NTNU

[10] Henrik Børstad Eriksen 2013, Struktur og sikkerhet av nettverk ved integrerte operasjoner, NTNU/Masteroppgave

[11] https://www.nsm.stat.no/tjenester/personellsikkerhet/slik-blir-du-sikkerhetsklarert/ofte-stilte-sporsmal-om-sikkerhetsklarering/ Lest 10.02.2015

[12] https://www.nsm.stat.no/tjenester/fysisk-sikring/ Lest 10.02.2015

[13] https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/veiledning-i-fysisk-sikring-mot-ulovlig-inntrengning.pdf Lest 11.02.2015

[14] https://www.nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/rst_2014.pdf Lest 12.02.2105

[15] https://lovdata.no/dokument/SF/forskrift/2001-07-01-744 Lest 12.02.2015

[16] https://www.nsm.stat.no/globalassets/dokumenter/2015-01-06-nsm-cryptographic-requirements-3-draft.pdf Lest 12.02.2015

[17] Stouffer, K., Falco, J., and Scarfone, K. (2007). Guide to Industrial Control Systems (ICS) Security. NIST.

[18] https://www.nsm.stat.no/blogg/tls-ikke-ssl-takk/ Lest 02.03 2015

[19] 8-STY-603102_RAMS-introduksjon og oversikt, Dokumentansvarlig Tuven Ruth, Gyldig fra 29.01.2014. Lest på www.Jernbaneverket.no. Lest den 19.03.2015

[20] Subset-038: Off-line Key Management FIS. 2005, v 2.1.9

[21] Nasjonal transportplan 2014-2023. https://www.regjeringen.no/nb/dokumenter/meld-st-26-20122013/id722102/?docId=STM201220130026000DDDEPIS&ch=1&q=

[22] http://www.tu.no/samferdsel/2015/04/24/britisk-ekspert-nye-signalanlegg-kan-bli-mal-for-terrorister Lest 25.04.2015.

Vedlegg

Risikoanalyse KMS nøkkelhåndtering ERT-10-Q-00248 rev 00E.

Jernbaneverket

ERTMS ERFARINGSSTREKNING
ØSTFOLDBANEN ØSTRE LINJE

Risikoanalyse
KMS nøkkelhåndtering

00E	Endelig utgave	11.05.2015	XHELEIN	XHALLEN	RAJA
Rev.	Revisjonen gjelder	Dato	Utarb. Av	Kontr. Av	Godkj. av

Tittel: **ERTMS ERFARINGSSTREKNING** **ØSTFOLDBANEN ØSTRE LINJE** **Risikoanalyse** **KMS nøkkelhåndtering**	Sider: **18**		
	Produsert av:	**JERNBANEVERKET INFRASTRUKTUR**	
	Prod.dok.nr.:		Rev:
	Erstatter:		
	Erstattet av:		
Prosjekt: 960215 ERTMS Erfaringsstrekning Parsell: Østfoldbanen Østre linje	Dokumentnummer: **ERT-10-Q-00248**	Revisjon: **00E**	
Jernbaneverket	Drift dokumentnummer:	Drift rev.:	

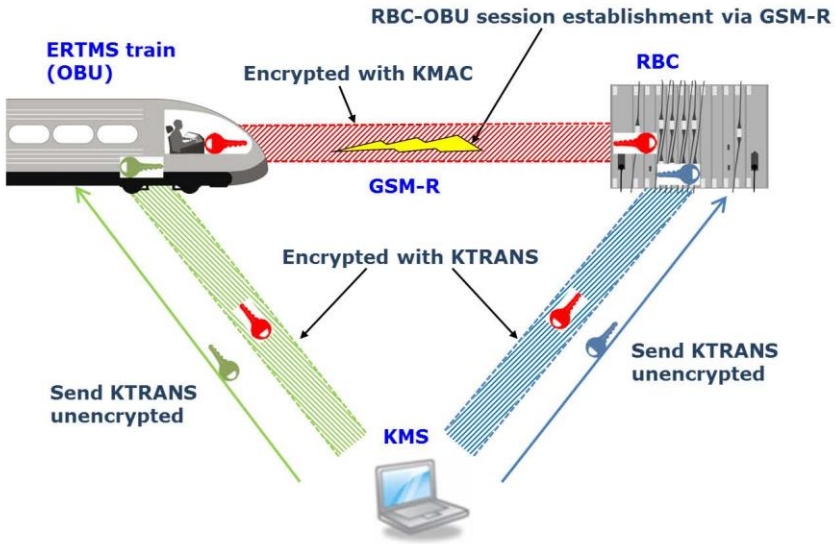
SAMMENDRAG

ERTMS (European Rail Traffic Management System) er det nye felles signalanlegget for EU og Europa. ERTMS består av to deler: ETCS (European Train Control System- europeisk tog styringssystem) og GSM-R (Mobiltelefoni spesielt for jernbane). ERTMS innføres for å forenkle togtrafikk mellom landegrenser og fornye det 50 år gamle eksisterende signalanlegget. I forbindelse med at Jernbaneverket skal starte en pilot med ERTMS på Østfoldbanen Østre linje (ØØL)fra 2015, trenger de et rammeverk for håndtering av krypteringsnøkler. Prosjektet har ikke kommet fram til et nøkkelhåndteringssystem/ prinsipper for krypteringsnøkkel for kommunikasjonen mellom tog (Ombordutrustning) og togradioblokksenter (RBC). Denne kommunikasjon går via GSM-R, som tidligere nevnt er en del av ERTMS.

Formålet med analysen i dette dokumentet er å vurdere farer ved KMS-nøkkelhåndtering, vurdere levetid for nøkler og derigjennom komme med anbefalinger til hvordan sikkerheten kan ivaretas på best mulig måte. Fokus er identifikasjon av nødvendige prosedyrer, organisering og tekniske krav. Analysen er avgrenset til å gjelde generering, håndtering og bruk av KMAC, KTRANS og K-KMC. Kompromittert RBC (eller falsk RBC) faller utenfor omfanget til denne analysen fordi det ikke har noe å gjøre med selve nøkkelhåndteringen. Ansvaret til togoperatørenes rolle når det gjelder nøkkelhåndteringen er heller ikke omfattet av denne analysen.

Analysen er basert på en del viktige antakelser og forutsetninger, se kapittel 1.4.

Systemet som vurderes i analysen er illustrert i figuren under.



Analysen har resultert i en del anbefalte tiltak. Disse er oppsummert i tabellen under.

Nr.	Mulige tiltak	Relatert til Id. i analysetabell (kapittel 8)	Anbefales (Ja/Nei)
1	Ikke bruk USB	1.1	Nei
2	Benytte security-USB	1.1	Ja
3	Sikkerhetsklarering av personell (også eksterne)	1.1, 1.2, 5.2, 6.2, 8.2	Ja
4	Årlig sikkerhetssamtale	1.1, 1.2, 5.2, 6.2, 8.2	Ja
5	Må være JBV/(NSB)-ansatt	1.1, 1.2, 5.2, 6.2, 8.2	Ja
6	Dedikerte PC-er (kan være under JBV-kontroll og eiendom)	1.1, 1.2	Ja
7	Egen USB med nødv. OS/programvare	1.2	Ja
8	Eget (JBV/NSB) teknisk utstyr benyttes	3.3	Ja
9	Vurdere å implementere checksum dersom dette ikke eksisterer (gjelder Bombardier)	3.3	Ja
10	Sjekk at prosedyrer for avslutning av rettigheter, tilganger, passord, osv. ved avslutning av arbeidsforhold er gode nok	9.1	Ja

Tiltakene vil bli videre vurdert og fulgt opp av ansvarlige for KMC (dvs. OPM). Siden KMS er et SIL0-system vil analysen, med farer og mulige tiltak, ikke bli registrert i prosjektets farelogg.

Basert på vurderingene av eksisterende barrierer har analysegruppen konkludert med at planlagt system for nøkkelhåndtering er tilstrekkelig sikkert. Analysegruppen forutsetter at de anbefalte forslag til tiltak blir vurdert iht. ALARP.

INNHOLDSFORTEGNELSE

1 INNLEDNING

1.1 Bakgrunn

ERTMS (European Rail Traffic Management System) er det nye felles signalanlegget for EU og Europa. ERTMS består av to deler: ETCS (European Train Control System- europeisk tog styringssystem) og GSM-R (Mobiltelefoni spesielt for jernbane). ERTMS innføres for å forenkle togtrafikk mellom landegrenser og for å fornye det 50 år gamle eksisterende signalanlegget. Hovedårsaken for at Norge innfører ERTMS, er å fornye signalanlegg til noe mer moderne enn gammel reléteknologi. I dag er det over 24 forskjellige signalsystemer i Europa.
I forbindelse med at Jernbaneverket skal starte en pilot med ERTMS på ØØL fra 2015, trenger de et rammeverk for håndtering av krypteringsnøkler. Prosjektet har ikke kommet fram til et nøkkelhåndteringssystem/ prinsipper for krypteringsnøkkel for kommunikasjonen mellom tog (Ombordutrustning) og togradioblokksenter (RBC). Denne kommunikasjon går via GSM-R, som tidligere nevnt er en del av ERTMS.
Denne analysen er laget i forbindelse med masteroppgave «Prinsipper for bruk av krypteringsnøkler for ERTMS i Norge» til masterstudent Henning Andenæs ved NTNU, Fakultet for ingeniørvitenskap og teknologi, Teknisk kybernetikk.. Denne analysen blir en del av denne masteroppgaven.

1.2 Formål

Fokus for analysen er å vurdere farer ved KMS-nøkkelhåndtering, vurdere levetid for nøkler og derigjennom komme med anbefalinger til hvordan sikkerheten kan ivaretas på best mulig måte. Fokus er identifikasjon av nødvendige prosedyrer, organisering og tekniske krav.

1.3 Omfang og avgrensninger

Analysen er avgrenset til å gjelde generering, håndtering og bruk av KMAC, KTRANS og K-KMC. Kompromittert RBC (eller falsk RBC) faller utenfor omfanget til denne analysen fordi det ikke har noe å gjøre med selve nøkkelhåndteringen.
Ansvaret til togoperatørenes rolle når det gjelder nøkkelhåndteringen er heller ikke omfattet av denne analysen.

1.4 Antakelser og forutsetninger

Følgende antakelser og forutsetninger gjelder for analysen:

- Trusselbildet som ligger til grunn for analysen er samme som i dag
- Maks 5 års levetid på nøkkel og GCD
- Analysen gjelder ØØL (Ski) – (Sarpsborg)
- Analysen gjelder for Bombardiers utstyr, både infrastruktur og OBU, Baseline 2
- KMS og RBC er fysisk sikret med adgangskontrollsystem
- Sikring av OBU er togoperatørens ansvar
- Analysen gjelder for all nøkkelhåndtering ifm. nytt utstyr, feilhåndtering og nøkkelbytte
- Analysen forutsetter at togoperatørene lager reservedeler ifm. nøkkelhåndtering iht de krav JBV vil sette for dette
- KMS vil være bemannet 24/7
- OBU med GCD forutsettes å ha true random generator for session key
- Det forutsettes at KMS har tilstrekkelig gode rutiner for passordadministrasjon

1.5 Terminologi

BASIC	Beginner's All-purpose Symbolic Instruction Code
BT	Bombardier Transportation
CIPHERTEXT	Encrypted plain text
COTS	Commercial Off the Shelf (commercially available product)
DMZ	Demilitarized zone (is a computer host or small network inserted as a "neutral zone" between a company's private network and the outside public network)
EeØØL	Erfaringsstrekning Østfoldbanens Østre Linje (project producing the KMS)
EOS	ERTMS Onboard System, an OBU type used in Norway and Sweden
ERTMS	European Rail Traffic Management System
ETCS	European Train Control System
FAT	Factory Acceptance Test
FIPS	Federal Information Processing Standards
FFFIS	Form, Fit and Function Interface Specification (a fully specified interface)
GCD	Generic Crypto Device
GSM-R	GSM (Global System for Mobile communication) for Railways
HTTPS	Hypertext Transfer Protocol Secure
KMAC	Key for Message Authentication Codes
KMC	Key Management Centre (organisation)
KMS	Key Management System (technical database tool)
KTRANS	Key for Transferring KMAC keys to OBU/RBC
K-KMC	Key for transferring KMAC keys to other KMC
MA	Movement authority
NSB	Norges Statsbaner AS
OAM	Operation and Maintenance organisation (norsk: FDV)
OPM	Operasjonssenter Marienborg
OBU	Onboard Unit
OS	Operating System
PC	Personal Computer
QA	Quality Assurance
RAM	Reliability, Availability, and Maintainability
RAMS	Reliability, Availability, Maintainability, and Safety
RBC	Radio Block Centre
SAT	Site Acceptance Test
SIL	Safety Integrity Level
TDD	Test-Driven Design
TSI	Technical Specification for Interoperability
VBA	Visual Basic for Applications
V&V	Verification & Validation

1.6 Arbeidsgruppens sammensetning

Vurderingene i denne analysen er gjennomført i to analysemøter som vist i Tabell 1-1under.

Navn	Analysemøter		Stilling/rolle	Bedrift/enhet
	28.01.15	03.02.15		
Roy Seland	X	X	Systemansvarlig KMS og Kryptering	JBV OPM
Henning Andenæs	X	X	Masterstudent, NTNU	JBV Signaltjenester
John Price	X		Signalingeniør, KMS	JBV ERTMS ØØL
Øyvind Knapskog	X		RAMS- og kvalitetsleder	JBV ERTMS ØØL
Einar S. Helseth	X	X	RAMS-rådgiver	JBV ERTMS ØØL

Tabell 1-1 Analysegruppens sammensetning

Analysendokumentet har vært på høring hos analysedeltagerne.

Det er vurdert at gruppen har den nødvendige kompetansen som kreves for det analyserte temaet.

2 AKSEPTKRITERIER OG METODE

2.1 Akseptkriterier

KMS er et SIL 0 system, dvs. ikke sikkerhetskritisk. Det primære formålet med denne analysen er å identifisere farer og problemstillinger forbundet med uautorisert tilgang til nøkler eller utstyr for generering/bruk av dem. Analysen skal ikke vurdere om risikonivået er akseptabelt eller ikke og det er dermed ikke relevant å anvende JBVs risikoakseptkriterier fullt ut i denne rapporten. Analysen vil fokusere på vurderinger av eksisterende og mulige nye barrierer/tiltak.

For analysen gjelder derfor følgende kriterium:

- Alle tiltak som med rimelighet kan iverksettes (praktisk gjennomførbarhet) skal iverksettes (ALARP-kriterium)

2.2 Metode

Analysen ble gjennomført på følgende vis:

1. Gjennomgang av systembeskrivelse
2. Identifikasjon av mulige konsekvenser av uautorisert tilgang til nøkler
3. Identifikasjon av mulige systemer/områder for å få tilgang til nøkler
4. Identifikasjon av mulige farer for hvert system/område
5. Analyse av hver fare mht. hvordan/hvem, identifikasjon av eksisterende barrierer og identifikasjon av mulige tiltak
6. Vurdering av eksisterende barrierer og mulige tiltak
7. Konklusjon

Analyseresultater er gjengitt i kapittel 4 og i analysetabeller i kapittel 8.

2.3 Usikkerhet ved analysen

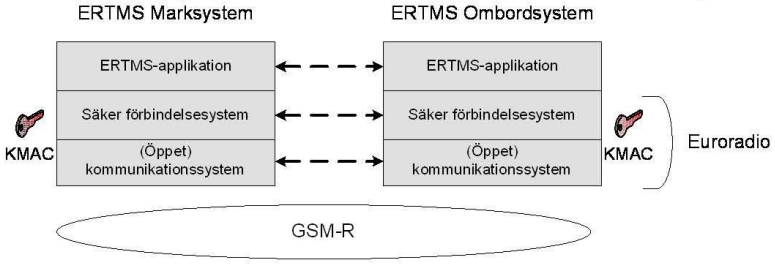
Usikkerheten ved analysen er knyttet til om alle farer er avdekket gjennom analysen, samt gjennom den videre bearbeiding av notatene etter analysemøtet. Utkast til analyserapport er sendt til alle analysedeltagere for kommentarer før endelig utgave er utarbeidet. Det forventes at eventuelle misforståelser blir fanget opp i denne kvalitetssikringsprosessen.

3 SYSTEMBESKRIVELSE

KMS for Østfolbanens Østre linje bygges og implementers iht. [1].Sentrale roller som er involvert i KMS nøkkelhåndtering fremgår av delkapitlene under.

3.1 Konsept

Kommunikasjonen mellom ERTMS-marksystem Radio Block Center (RBC) og ERTMS-ombordutrustning On Board Unit(OBU) bruker GSM-R som er definert som et åpent nett. GSM-R i sammenheng med nøkkelhåndtering betraktes som et usikkert nettverk. For å kunne etablere en sikker forbindelse mellom ERTMS marksystem og ombordsystem brukes Euroradio protokoll. Euroradiolaget sitter mellom ERTMS-applikasjonslaget (marksystem eller ombordutrustning) og selve GSM-R nettet. Figuren under viser dette skjematisk.

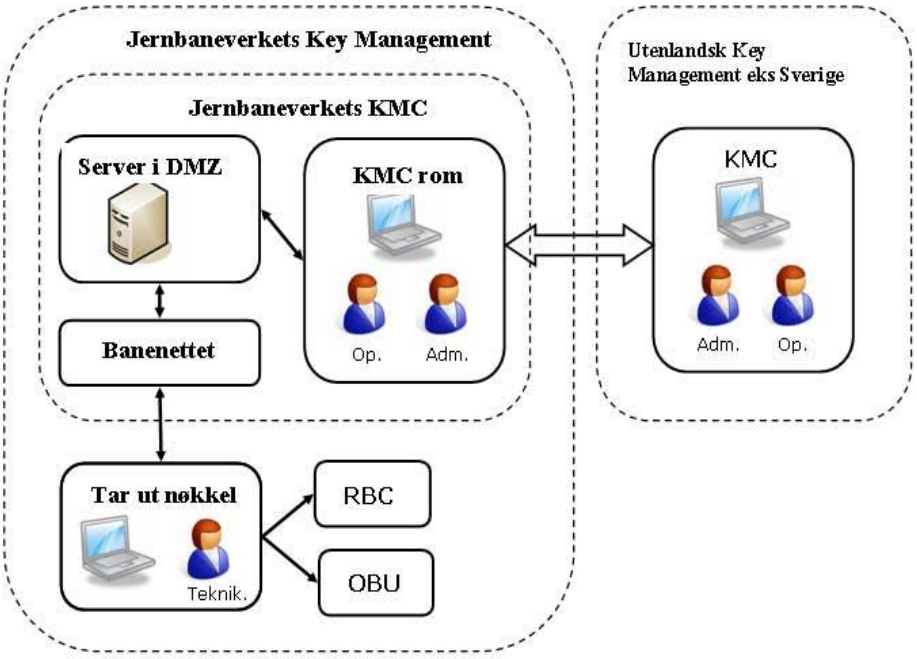


ERTMS-applikasjonen (RBC) etablerer en sikker forbindelse til en annen ERTMS- applikasjon (OBU) via Euroradio laget. Euroradio etablerer en sikker forbindelse mellom mark og ombord utstyret som bruker ETCS applikasjoner for ERTMS- kommandoer. For å etablere en sikker kanal brukes Euroradio protokollen for symmetrisk kryptering. En krypteringsnøkkel deles mellom de ulike ERTMS enhetene som trenger å etablerere en forbindelse. Kryptonøkkelen kalles KMAC i Euroradio sammenheng. Ved oppkobling genererer hver Euroradio enhet (RBC og OBU) en ny nøkkel denne kalles sesjonnøkkel, "sessionkey" (KSMAC) for kun denne ene forbindelsens varighet. Brytes forbindelsen mellom OBU og RBC må det etableres en ny KSMAC. KSMAC genereres via en funksjon som heter "Key Derivation Function" (KDF). KMAC er en del av inngangsdata i KDF og bare Euroradio enheter som deler samme KMAC kan generere en KSMAC som er lik. Som resultat av dette etableres en sikker forbindelse. Figuren under illustrerer dette.

3.1.1 Definisjon

I ERTMS arkitekturen finnes det et "Key Management Center" (KMC). KMC har ansvaret for nøkkelhåndteringen innen ERTMS, dvs. generering, lagring, distribusjon og fjerning av alle nøkler som trengts i et KM domene. Et KM domene består av en KMC med alle ERTMS enheter (RBC og OBU) som får sine nøkler fra KMC. Det vanligste er at KM domene er et land med alle RBC'er og OBU'er til alle togoperatørene i landet.

For å kunne kjøre et ERTMS utstyrt tog mellom ulike KM domener må en utveksle KMAC mellom ulike KMC'er. Prosedyrer for dette fins definert i SUBSET-038, men dette er ikke endel av vår analyse, siden slik type trafikk ikke er aktuelt for ØØL- prosjektet . Men etter hvert som det bygges ut med ERTMS vil dette bli en problemstilling senere. I SUBSET-038 defineres hvordan nøkler byttes eller distribueres mellom ulike KMC'er og hvordan nøkkelhåndtering utføres. Prosessen som beskrives er en off-line prosess, det vil si at det kreves manuelle prosedyrer for nøkkelhåndtering. Distribusjon, fjerning og oppdatering av nøkler må gjennomføres manuelt. Det er ikke blitt definert en prosedyre eller metode for on-line nøkkelhåndtering i ERTMS standarden, men Banedanmark holder på å utvikle en metode i samarbeid med ERA. Figuren under viser hvordan dette er tenkt gjennomført i Norge.



Fokus for denne analysen er nøkkelhåndteringen mellom KMC, RBC og OBU. Hvordan dette kan gjennomføres sikrest mulig og analysere hvilke farer som kan oppstå.

3.1.2 KMAC and KTRANS Keys in Operation

ETCS trains use a KMAC key to encrypt the checksum for the messages they exchange with the RBC during session establishment. The same KMAC key needs to be installed in the OBU and RBC. The KMS sends the KMAC keys using offline messages (computer files). The KMAC keys themselves are encrypted with KTRANS keys.

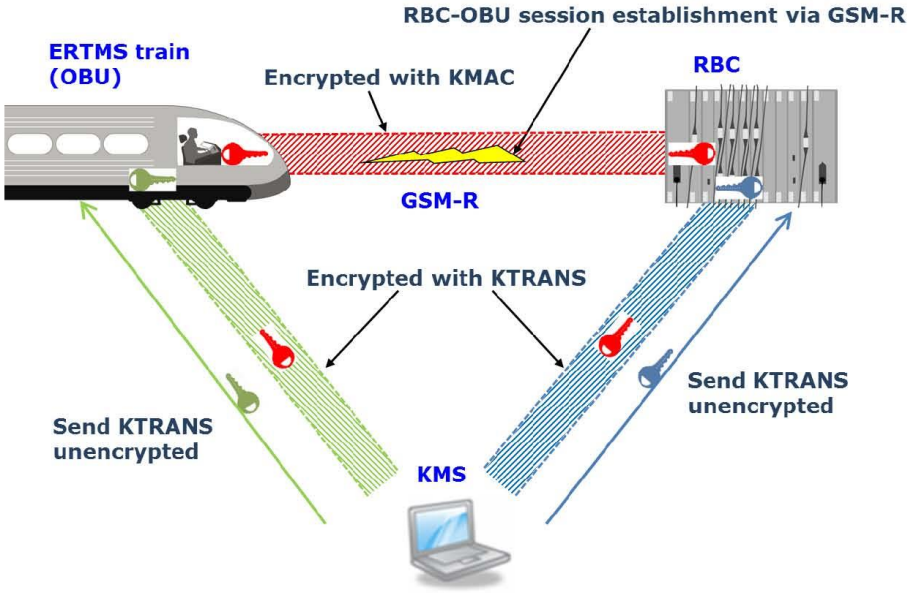


Figure 1

3.1.3 K-KMC Keys and the "Home KMC" Concept

Each OBU and RBC has a home KMC. The home KMC delivers all keys to the OBU and RBC in its domain. When a train needs to connect with an RBC that is not in the same domain as its home KMC (i.e. an RBC in another country), then the two KMCs need to exchange KMAC keys. As shown in the example below, when KMAC keys are exchanged between different KMCs, the KMAC keys are encrypted using K-KMC keys.

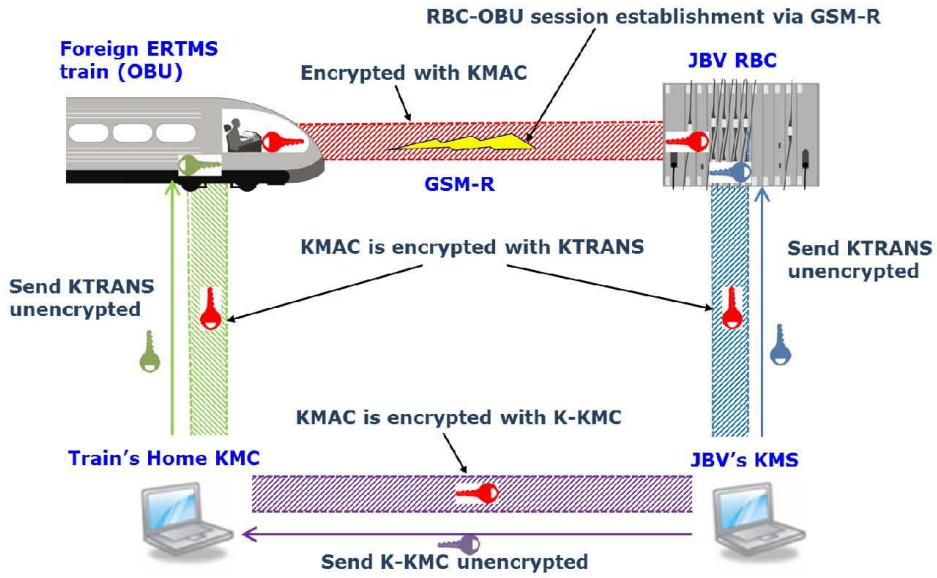


Figure 2

3.1.4 KTRANS and K-KMC are Not Encrypted

KTRANS and K-KMC are like the "passwords" that unlock an encrypted file. These keys need to be unencrypted for them to be used. That means that KTRANS and K-KMC key files need to be distributed by secure means. In this way, KTRANS and K-KMC messages are "more secret" than KMAC messages.

4 FAREIDENTIFISERING

Mulige konsekvenser (farlige situasjoner) av uautorisert tilgang til nøkler kan være at noen genererer og sender en falsk MA til et tog. Det ble i analysen konkludert med at dette er den eneste reelle faren ifm. uautorisert tilgang til nøkkel.

En falsk MA til et tog kan føre til at tog sendes inn på en strekning som ikke er «fri», dvs. det kan være andre tog der, sporveksel kan være ute av kontroll eller en planovergang kan være åpen for veifarende. Konsekvensen av dette kan være tog – tog kollisjon, avsporing eller påkjørsel personer/kjøretøy i planovergang.

Falsk MA kan sees på som en topphendelse i et feiltre. Den eneste måten å få til å sende en falsk MA er å kompromittere RBC-en eller ha tilgang til en falsk RBC, og samtidig ha tilgang til nøkkelen (KMAC).

Kompromittert RBC (eller falsk RBC) faller utenfor omfanget til denne analysen fordi det ikke har noe å gjøre med selve nøkkelhåndteringen. RBC-en må fysisk sikres så ikke uvedkommende kan få tilgang til den.

Basishendelser i feiltreet blir derfor forskjellige måter å få tilgang til riktig nøkkel.

Mulige systemer/områder for å kunne få tilgang til nøkler ble identifisert til å være:

- Nøkkel (KMAC)
- Kryptering
- Code security
- "Ser over skulder"
- Key Management Database
- RBC
- OBU
- Key Management Distribution Server
- Ansatte

Disse ble analysert iht. punktene 4 – 6 i metodebeskrivelsen (se kapittel 2.2). Analyseresultater er gjengitt som tabeller i kapittel 8.

5 VURDERING AV MULIGE TILTAK

Det ble i analysen identifisert en rekke mulige tiltak, enten i form av nye barrierer eller som en forbedring av eksisterende barrierer. Tiltakene er oppsummert i tabellen under:

Nr.	Mulige tiltak	Relatert til Id. i analysetabell (kapittel 8)	Anbefales (Ja/Nei)
1	Ikke bruk USB	1.1	Nei
2	Benytte security-USB	1.1	Ja
3	Sikkerhetsklarering av personell (også eksterne)	1.1, 1.2, 5.2, 6.2, 8.2	Ja
4	Årlig sikkerhetssamtale	1.1, 1.2, 5.2, 6.2, 8.2	Ja
5	Må være JBV/(NSB)-ansatt	1.1, 1.2, 5.2, 6.2, 8.2	Ja
6	Dedikerte PC-er (kan være under JBV-kontroll og eiendom)	1.1, 1.2	Ja
7	Egen USB med nødv. OS/programvare	1.2	Ja
8	Eget (JBV/NSB) teknisk utstyr benyttes	3.3	Ja
9	Vurdere å implementere checksum dersom dette ikke eksisterer (gjelder Bombardier)	3.3	Ja
10	Sjekk at prosedyrer for avslutning av rettigheter, tilganger, passord, osv. ved avslutning av arbeidsforhold er gode nok	9.1	Ja

Tiltakene vil bli videre vurdert og fulgt opp av ansvarlige for KMC (dvs. OPM). Siden KMS er et SIL0-system vil analysen, med farer og mulige tiltak, ikke bli registrert i prosjektets farelogg.

6 KONKLUSJON OG ANBEFALINGER

Basert på vurderingene av eksisterende barrierer som beskrevet i kapitel 8 har analysegruppen konkludert med at planlagt system for nøkkelhåndtering er tilstrekkelig sikkert. Analysegruppen forutsetter at de anbefalte forslag til tiltak blir vurdert iht. ALARP.

7 REFERANSER

[1] ERT-00-Q-00151, ØSTFOLDBANEN ØSTRE LINJE ERTMS ERFARINGSSTREKNING, Key Management System Development Process and Specification, Rev. 00E

Id	System/område	Fare	Hvordan/hvem?	Eksisterende barrierer	Vurdering av eksisterende barrierer	Mulige tiltak	Kommentar
					for session key		
2.2			"Long key exposure time"	Nøkkellengde sikrer stort antall kombinasjoner	Ingen reell risiko innenfor levetiden til systemet (maks 5 år)		
2.3			Key re-use	Bruker forskjellige nøkler til hvert tog	God nok forutsatt at GCD har true random generator		
3.1	Code security	Angriper får adgang til systemet (KMS)	Angriper får lurt virus inn i KMS via USB-pinne ("Stuxnet")	• Minnebrikker må være forhåndsgodkjent. • Fysisk sikring av lokasjon. • Adgangskontroll. • KMS-server er beskyttet av en aksess-ID for hver bruker.	Vurderes som god nok fordi barrierene består av flere kombinasjoner (både fysisk og teknisk tilgang)		
3.2		Angriper får tilgang til OBU	Får lastet inn ny SW i OBU via innlasting av nøkkel	Fysisk sikring av OBU med GCD	Vurderes ikke her da det er togoperatørens ansvar	Togoperatøren må ha god nok fysisk sikring og rutiner	
3.3			Får lastet inn SW med virus i GCD ifm. innlasting av nøkkel	• Ny SW er utstyrt med en checksum? (denne barrieren flyttes til tiltak hvis det ikke er tilfelle p.t.) • Testleder/sluttkontrollør vil sjekke installasjonen (uavhengig av installatør)	Vurderes som god nok forutsatt gode prosedyrer for testleder/sluttkontrollør	• Eget (JBV/NSB) teknisk utstyr benyttes. • Vurdere å implementere checksum dersom dette ikke eksisterer (gjelder Bombardier)	
4.1	"Ser over skulder"	Angriper får adgang til systemet eller nøkkel	Angriper ser nøkkel eller adgangs-informasjon over skulder på operatør	• Nøkkel vises ikke i klartekst • Tilgangskontroll • Instruks og opplæring	Vurderes som god nok fordi barrierene består av flere kombinasjoner (både fysisk og teknisk tilgang)		
5.1	Key Management Database	Angriper får adgang til systemet	Ekstern aktør	• KMD er ikke knyttet til internett • Adgangskontroll • Fysisk sikring	Vurderes som god nok fordi barrierene består av flere kombinasjoner (både fysisk og teknisk		

8 ANALYSETABELLER

Id	System/område	Fare	Hvordan/hvem?	Eksisterende barrierer	Vurdering av eksisterende barrierer	Mulige tiltak	Kommentar
0	**Falsk MA**	**Pirat-RBC sender farlig MA med en gyldig nøkkel**	**Se Id 1-9 under**	**Se Id 1-9 under**	**Se Id 1-9 under**	**Se Id 1-9 under**	**Dette er topphendelsen. Id. 1 – 9 under er mulige basishendelser som, i kombinasjon med en pirat-RBC, kan føre til topphendelsen.**
1.1	Nøkkel (KMAC)	Mister USB med nøkkel (USB brukt til overføring fra tekniker PC til RBC (pr. i dag ikke mulig til tog)	Tekniker mister nøkkel eller kontroll på den	• KTRANS kryptering av USB • Fysisk sikring av USB • Opplæring og godkjenning av personell	Vurderes som god, men security USB og sikkerhetssamtale bør vurderes	• Ikke bruk USB • Security USB • Sikkerhetsklarering av personell (også eksterne) • Årlig sikkerhetssamtale • Må være JBV/NSB-ansatt?	USB må kunne brukes, men den bør da være en security USB
1.2		Tekniker mister nøkkel fordi den ikke er slettet etter håndtering – funnet av angriper	Tekniker glemmer å slette nøkkel fra sin PC	Systemet er bygget opp slik at tekniker skal slette filen når den er lastet over (prosedyre)	Vurderes som god, men dedikerte JBV PC-er eller egen USB med nødvendig programvare og sikkerhetssamtale bør vurderes.	• Dedikerte PC-er (kan være under JBV-kontroll og eiendom) • Må være JBV/NSB-ansatt • Sikkerhetsklarering av personell (også eksterne). • Årlig sikkerhetssamtale • Egen USB med nødv. OS/programvare	Prosedyre krever at tekniker sletter nøkkel etter spørsmål fra systemet. Norsk sikkerhetsklarering kan være et problem fordi tekniker kan være fra utenlandsk leverandør. Sikker sletting av nøkkel på en vanlig PC anses som en utfordring i dag.
2.1	Kryptering	"Re-play attack" pga. utilstrekkelig tilfeldighet i generator eller dårlig implementasjon av algoritme	Pga. utilstrekkelig tilfeldighet kan angriper se at det kommer en lik melding som tidligere	• True random generator er implementert • Sertifisert implementasjon av FIPS	True random generator (sertifisert av FIPS) anses som en god nok barriere og at OBU med GCD forutsettes å ha true random generator		

Id	System/område	Fare	Hvordan/hvem?	Eksisterende barrierer	Vurdering av eksisterende barrierer	Mulige tiltak	Kommentar
				• Passordbeskyttelse • Kryptert innhold	tilgang)		
5.2			Intern: Utro tjener	• Passordbeskyttelse • Adgangskontroll	Vurderes som god, men mulige tiltak må vurderes	• Må være JBV-ansatt • Sikkerhetsklarering av personell (også eksterne) • Årlig sikkerhetssamtale	
6.1	RBC	Angriper får adgang til systemet	Ekstern aktør	• Adgangskontroll • Fysisk sikring • Passordbeskyttelse	Vurderes som god nok fordi barrierene består av flere kombinasjoner (både fysisk og teknisk tilgang)		Det forutsettes rutine for passordadministrasjon
6.2			Intern: Utro tjener	• Passordbeskyttelse Instruks og opplæring • Adgangskontroll med logg	Vurderes som god, men mulige tiltak må vurderes	• Må være JBV-ansatt • Sikkerhetsklarering av personell (også eksterne) • Årlig sikkerhetssamtale	
7.1	OBU	Angriper får adgang til systemet	Ekstern: Under hensetting	• Adgangskontroll • Vakthold • Fysisk sikring	Vurderes som god, men det er togoperatørens ansvar.	Alarmsystem	Ansvar til togoperatør. Utenfor scope til nøkkelhåndtering
7.2			Intern: Togpersonell	• Opplæring og godkjenning av personell • Ikke mulig å få nøkkel ut av GCD	Vurderes som god, men det er togoperatørens ansvar.		Ansvar til togoperatør. Utenfor scope til nøkkelhåndtering
8.1	Key Management Distribution Server	Angriper får adgang til systemet	Ekstern aktør	• Brukernavn/passord • Fysisk sikring • Adangskontroll • Fysisk plassering (annet sted enn KMS) • Tilknyttet DMZ • Tidsbegrensning for datalagring på server	Vurderes som god nok fordi barrierene består av flere kombinasjoner (både fysisk og teknisk tilgang)		
8.2			Intern: Utro tjener	• Passordbeskyttelse Instruks og opplæring	Vurderes som god, men mulige tiltak må	• Må være JBV-ansatt • Sikkerhetsklarering	

Id	System/område	Fare	Hvordan/hvem?	Eksisterende barrierer	Vurdering av eksisterende barrierer	Mulige tiltak	Kommentar
				• Adgangskontroll	vurderes	av personell (også eksterne) • Årlig sikkerhetssamtale	
9.1	Ansatte	Angrep fra ansatt som slutter	"Intern": Utro tjener		Vurderes som god nok forutsatt gode nok prosedyrer for avslutning av arbeidsforhold	Sjekk at prosedyrer for avslutning av rettigheter, tilganger, passord, osv. er gode nok	