| Skapat av (Efternamn, Förnamn, org) | DokumentID | Ev. ärendenummer |
|---|---|---|
| JG/NK/JO | KMS14-04 | |
| **Fastställt av** | **Dokumentdatum** | **Version** |
| | 2014-09-17 | 1.0 |

**Dokumenttitel**

# Information om Trafikverkets hantering av krypteringsnycklar för ERTMS

## Inledning

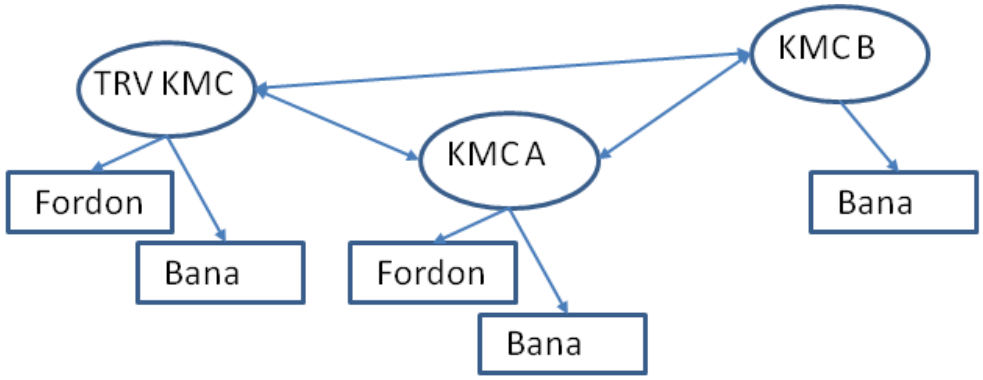
I ERTMS används radio för att överföra signalbesked mellan markutrustning och ett fordons ombordutrustning. Kryptonycklar används för att mottagaren ska kunna verifiera att meddelanden som tas emot kommer från rätt avsändare och att informationen är oförändrad.

## KMC

Den typ av kryptering som används är symmetrisk kryptering, vilket innebär att avsändare och mottagare använder samma kryptonyckel. Detta innebär att identiska kryptonycklar måste installeras på ett säkert sätt i förväg innan krypterad kommunikation kan etableras.

För att få tillgång till nycklar måste varje ERTMS-enhet tillhöra en KMC, denna KMC är ERTMS-enhetens hem-KMC. Det spelar ingen roll vilken KMC som är hem-KMC, eftersom alla KMC:er skall kunna tala med varandra och utbyta nycklar.

En KMC (Key Management Centre) ansvarar för all nyckelhanteringen inom en KM-domän. En KM-domän består av en KMC och alla de ERTMS-enheter som får sina kryptonycklar från denna KMC. Nyckelhantering innefattar generering, lagring, distribution och borttagning av alla kryptonycklar som behövs inom KM-domänen. För att möjliggöra gränsöverskridande järnvägstrafik utbyts kryptonycklar också mellan olika KMC:er.




*Figur 1.*

En ombordutrustning kan endast vara anslutet till en KMC och endast erhålla kryptonycklar från denna KMC. Ett fordon som tillhör en KMC och behöver trafikera en bana som tillhör en annan KMC, får tillgång till kryptonycklar genom ett utbyte av kryptonycklar mellan fordonets KMC och den KMC som banans marksystem tillhör.

| Skapat av (Efternamn, Förnamn, org) | DokumentID | Ev. ärendenummer |
|---|---|---|
| JG/NK/JO | KMS14-04 | |

# Alternativa KMC-lösningar

## Alternativ 1 – Egen KMC

Detta alternativ är en lösning som rekommenderas för de järnvägsföretag som trafikerar ERTMS-banor som förvaltas av både Trafikverket och av andra infrastrukturförvaltare.

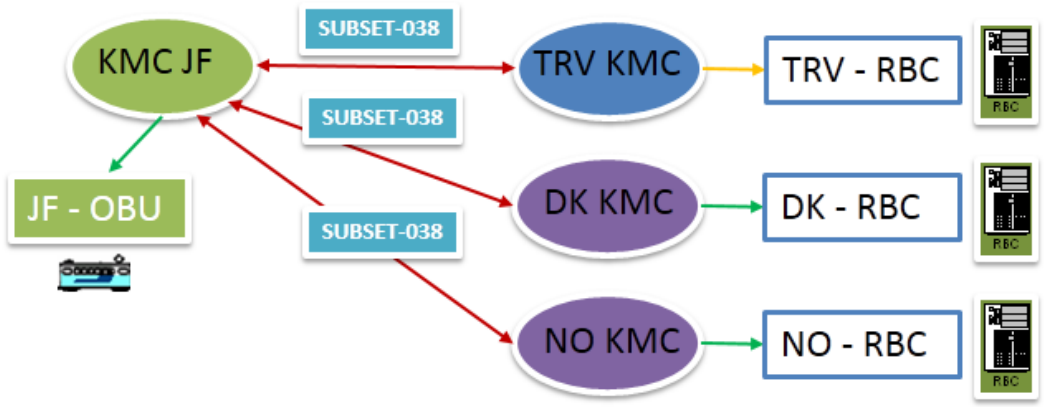
Detta alternativ är det mest flexibla alternativet och innebär att järnvägsföretag upprättar en egen KMC för distribution av kryptonycklar till ombordutrustningar. Denna KMC används för att utbyta erfoderliga kryptonycklar med alla berörda infrastrukturförvaltare med filstruktur enligt den europeiska specifikationen SUBSET-038.

Fördelar:

1. Direkt kontakt med berörda infrastrukturförvaltare utan Trafikverkets inblandning, ger färre parter, större frihet och bättre säkerhet.
2. Möjlighet att i egen regi införa nya gränssnitt mellan KMC och ombordutrustning, t.ex. SUBSET-114 och efterföljande standard för online kryptonyckeldistribution.

Nackdelar:

1. Det finns ingen KMC-lösning på marknaden som stöder Trafikverkets gränssnittsspecifikation som används i EOS ombordutrustning.




*Figur 2.*

## Alternativ 2 – Ansluta till Trafikverkets KMC

Detta alternativ är en enkel lösning som rekommenderas för de järnvägsföretag som trafikerar ERTMS-banor som Trafikverket förvaltar och som använder ombordutrustning som stöder Trafikverkets gränssnittsspecifikation.

Trafikverket har upprättat en KMC i första hand avsedd för att hantera kryptonycklar mot ERTMS markutrustningar som Trafikverket förvaltar. Trafikverket tillåter även järnvägsföretag att ansluta ombordutrustning till Trafikverkets KMC, förutsatt att de uppfyller Trafikverkets krav. Trafikverkets krav måste godkännas genom avtal mellan Trafikverket och järnvägsföretag innan kryptonycklar lämnas ut från Trafikverkets KMC.

Trafikverkets KMC har endast stöd för Trafikverkets egna gränssnitt för nyckeldistribution mellan KMC – OBU. Alla ERTMS-enheter inom Trafikverkets KM-domän måste därför stödja denna gränssnittsspecifikation.

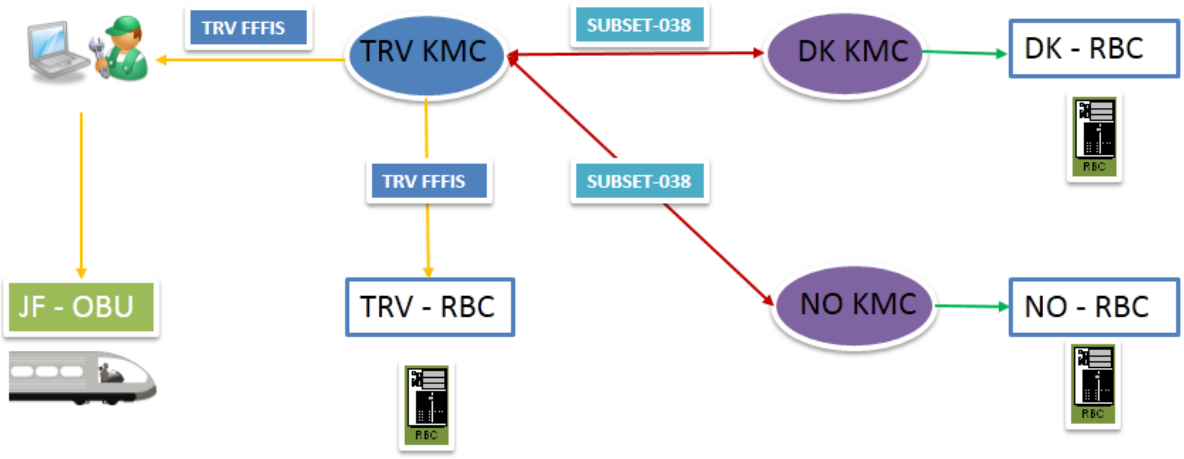
| Skapat av (Efternamn, Förnamn, org) | DokumentID | Ev. ärendenummer |
|---|---|---|
| JG/NK/JO | KMS14-04 | |

Fördelar:

1. Enkel lösning för mindre järnvägsföretag som bedriver trafik på enbart Trafikverkets ERTMS-banor och har stöd för Trafikverkets gränssnittsspecifikation (t.ex. EOS).
2. Kräver ingen egen KMC.

Nackdelar:

1. Trafikverkets KMC distribuerar endast kryptonycklar enligt Trafikverkets gränssnittsspecifikation. Kräver speciallösningar för stöd av andra gränssnittsspecifikationer.




*Figur 3.*

## ETCS-ID

Alla ombordutrustningar och KMC:er behöver en unik ETCS identitet. Ansvaret för hantering av ETCS-identiteter i Europa ligger hos European railway agency (ERA). ETCS identiteter för ombordutrustning ansöks av systemleverantörerna och medföljer utrustningen. Ansvaret för ETCS identiteter för KMC innehas av Transportstyrelsen som tilldelar dessa.

## För mer information

**Trafikverkets KMC**

Skicka gärna dina frågor till Trafikverkets KMC.

E-post: kmc@trafikverket.se.

| Skapat av (Efternamn, Förnamn, org) | DokumentID | Ev. ärendenummer |
|---|---|---|
| JG/NK/JO | KMS14-04 | |

## Definitioner och förkortningar

| | |
|---|---|
| ERTMS | European Rail Traffic Management System, europeiskt standardiserat trafikstyrningssystem för järnväg, som inkluderar ETCS och GSM-R. |
| ERTMS-enhet | I detta dokument avses ERTMS ombord- och markutrustning som är beroende av kryptonycklar för sin funktion. |
| KMC | Key Management Centre - Den funktionella enheten som ansvarar för generering, lagring och distribution av krypteringsnycklar i en KM domän och nyckelhantering mot andra domäner. Distribution av nycklar till enheter inom en domän sköts endast av domänens KMC. |
| KM-domän | Består av en KMC och alla ERTMS enheter som får sin nyckelhantering från denna KMC. |
| OBU | On Board Unit, den del av ERTMS-systemet som finns ombord på fordonet. En av uppgifterna som OBU:n sköter är att skicka och ta emot säkerhetsrelaterad information från RBC. |
| RBC | Radio Block Centre, den centraliserad säkerhetsenhet som tillsammans med förreglingssystemet skapar och upprätthåller separationen mellan fordon. RBC skickar och tar emot säkerhetsrelaterad information via radio (GSM-R) till ombordutrustning. |