

**Verksamhetssystemet
Föreskrift
BVF 1544.60101**

Diarienummer
TRV 2011/8848

Handläggare
Johan Olsson, Ttsisi

Gäller för
Trafikverket koncern

Giltigt från
2011-03-01

Giltigt till
Tills vidare

Ansvarig enhet
Teknik / Operativ teknik

Ersätter
-

Version
1.0

Antal bilagor
0

Fastställd av
Björn Svanberg, Tt

Trafikverkets KMS

Regler för hantering av ERTMS kryptonycklar

Innehållsförteckning

1	Syfte	4
2	Omfattning	4
3	Definitioner och förkortningar	4
3.1	Definitioner	4
3.2	Förkortningar	6
4	Ansvar	6
5	Krav	6
6	Trafikverkets KMS	7
6.1	Beskrivning	7
6.2	Roller	8
6.2.1	KMC-administratör	8
6.2.2	KMC-operatör	9
6.2.3	KMC-tekniker	9
6.3	Behörighet	9
6.3.1	Behörighetsnivåer i KMC-applikationen	10
7	Teknik	10
7.1	Teknisk miljö	10
7.2	Gränssnitt	11
7.2.1	Inom Trafikverkets KM-domän	11
7.2.2	Mot andra KM-domäner	11
7.3	Teknisk utrustning	11
8	KMS Drift och underhåll	12
8.1	Anslutning till KMC	13
8.1.1	Trafikverkets ERTMS-enheter	13
8.1.2	Icke Trafikverkets ERTMS-enheter	13
8.1.3	Lämna KMC	14
8.1.4	Ändring av registrerade uppgifter	14
8.2	Registrering av ERTMS-enhet	14
8.2.1	Registrering	14
8.2.2	Avregistrering	14
8.3	Hantering av kryptonycklar	15
8.3.1	Ombordutrustning	15

8.3.2	Markutrustning	15
8.4	Bekräftelse.....	16
9	Spårbarhet.....	16
9.1	Dokumentering.....	16
9.2	Personuppgifter	17
10	Säkerhet	17
10.1	Hantering av oskyddade nycklar	17
10.2	Röjda nycklar	17
10.3	Kontaktpersoner	17
11	Hjälpmedel och referenser.....	18
11.1	Hjälpmedel	18
11.2	Referenser	18

1 Syfte

ETCS-utrustade fordon och banor utrustade med ERTMS kräver kryptonycklar för säker radiokommunikationen enligt ERTMS-standard. ERTMS-standard definierar protokollet Euroradio för etableringen av säkra förbindelser mellan marksystem (RBC eller RIU) och ombordsystem (OBU) via GSM-R-nät. Protokollet använder kryptonycklar för att skydda informationsflöde (säkerhetskritisk information) mellan marksystem och ombordsystem. Kryptonycklarna måste hanteras på ett säkert sätt; skyddet av informationsflöde (säkerhetskritisk information) mellan marksystem och ombordsystem beror på att kryptonycklar verkligen är skyddade från obehöriga.

2 Omfattning

Detta dokument fastställer de grundläggande principer, rutiner och procedurer som Trafikverkets KMS ska uppfylla för att säkerställa att kraven som ligger till grund för den interoperabla järnvägstrafiken ska vara uppfyllda.

Utbyte av kryptonycklar med andra KMC:er och hantering av K-KMC nycklar sker efter vad som beskrivs i varje ERTMS Interoperability Contract.

3 Definitioner och förkortningar

3.1 Definitioner

3DES	Triple-DES, ett annat namn för krypteringsalgoritmen TDEA.
AES	Advanced Encryption Standard – erkänd amerikansk krypteringsstandard med utbredd användning. AES togs fram som en ersättare för DES.
Dekryptering	Metod som omvandlar oläsbar data (krypterad data) till läsbar data (klardata).
DEA	Data Encryption Algorithm – krypteringsalgoritm.
DES	Data Encryption Standard – En amerikansk krypteringsstandard från 70-talet. Standarden har fortfarande utbredd användning men ersätts successivt med AES. Standarden använder krypteringsalgoritmen DEA.
ERTMS	European Rail Traffic Management System, europeiskt standardiserat trafikstyrningssystem för järnväg, som inkluderar ETCS och GSM-R.
ERTMS Interoperability Contract	Avtal mellan olika KM-domäner som etablerar procedurer och överenskommelser om nyckelhantering mellan KM-domäner för att möjliggöra domänöverskridande trafik.
ETCS	European Train Control System, europeiskt standardiserat trafikstyrningssystem för järnväg, som inkluderar utrustning för fordon och markutrustning
Euroradio	Protokollet som används i ETCS för etablering av en säker förbindelse mellan två ERTMS-enheter (t.ex. RBC och OBU).

GSM-R	Standardiserat system för radiobaserad kommunikation av tal och data för järnvägen.
K-KMC	Transportnyckel som används för att säkra KMAC-utbyte mellan KMC:er. Transportnyckeln utgörs av K-KMC1 och K-KMC2 (samma funktion som KTRANS).
KM	Key Management – Alla aktiviteter som behöver utföras för att kunna hantera kryptonycklar, t.ex. generering, lagring, distribution och domänöverskridande nyckelutbyte mellan KMC:er.
KM-domän	Består av en KMC och alla ERTMS-enheter (RBC, RIU, OBU) som får sin hantering av kryptonycklar från domänens KMC.
KMAC	Autentiseringsnyckel i Euroradio-protokollet.
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.
KMAC-nycklar	för domänöverskridande trafik, distribueras till enheter tillhörande annan domän genom att nyckeln först skickas till den andra domänens KMC som sedan distribuerar ut den till enheten.
KMC-rum	Är ett rum med begränsad tillgänglighet, som är avsett att användas av operatörerna i KMC i deras arbete.
KMS	Key Management System – Det system som krävs för en säker nyckelhantering, inkluderande KMC och gällande regler och procedurer.
Kryptering	Metoden som omvandlar data i klartext till krypterad data (oläsbar).
Kryptonyckel	Ett initialt värde som kan bestå av godtyckliga kombinationer av siffror, bokstäver etc. som används tillsammans med en krypteringsalgoritm för kryptering och dekryptering av data.
KTRANS	Transportnyckel som används för att säkra KMAC-utbyte mellan KMC och ERTMS-enheter. Transportnyckeln utgörs av KTRANS1 och KTRANS2 (samma funktion som K-KMC).
Marksystem	I detta dokument avses marksystem anpassade för ERTMS-standard, om inget annat anges.
Nyckel	Det samma som kryptonycklar i detta dokument om inget annat anges.
Nyckeluthämtare	Ingår i rollen som KMC-tekniker.

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.
Ombordsystem	I detta dokument avses ombordsystem anpassade för ERTMS-standard, om inget annat anges.
RBC	Centraliserad säkerhetsenhet, som tillsammans med föreglingssystem skapar och upprätthåller separationen mellan fordonssätt. Kommunikerar med CTC/IL, lämnar och tar emot säkerhetsrelaterad information via radio åt ERTMS ombordutrustning.
Spårbarhet	Möjlighet att entydigt kunna härleda utförda aktiviteter i systemet till en identifierad användare.
Säker modul	Hårdvara, mjukvara eller både hårdvara/mjukvara modul där känslig information kan lagras (t.ex. kryptonycklar) på ett säkert sätt. En säker modul kan vara t.ex. ett USB-minne där information lagras krypterad eller ett kryptochip där information lagras i klartext och skyddas mot obehörigt intrång av olika mekanismer i kryptochip. Kryptochip används av OBU för lagring av KTRANS.
TDEA	Triple Data Encryption Algorithm – Krypteringsalgoritm som används i Euroradio protokollet. Algoritmen är en tre stegs process där DEA används i varje steg (3xDEA).

3.2 Förkortningar

ETCS-ID	ETCS identitet.
FFFIS	Form-Fit Functional Interface Specification.

4 Ansvar

Ansvar i Trafikverket för detta dokument och dess efterlevnad i styrs genom Trafikverkets arbetsordning.

5 Krav

Trafikverket ansvarar för hanteringen av nycklarna KTRANS och KMAC för alla ERTMS-enheter som ingår i Trafikverkets KM-domän. Trafikverket ansvarar också för hantering av nycklarna K-KMC enligt vad som beskrivs i varje ERTMS Interoperability Contract.

Det skydd som den kryptografiska säkerhetskoden, som definieras i Euroradio specifikationen, ger kan anses vara tillräcklig, förutsatt att organisationen som är ansvarig för systemdrift kan säkerställa att lämpliga åtgärder säkerställer sekretessen av kryptonycklarna [4].

Bilaga A i TSD Trafikstyrning och signalering anger obligatoriska och informativa tekniska specifikationer för driftkompatibilitet. Tillgängliga dokument från ERA har genomsköts och dokument som identifierats som kravställare för Trafikverkets KMS redovisas nedan.

Följande dokument är identifierade som kravställare för Trafikverkets KMS:

- TSD Trafikstyrning och signalering (höghastighet), direktiv 2006/860/EG.
- TSD Trafikstyrning och signalering (konventionell), direktiv 2006/679/EG.
- Bilaga A TSD Trafikstyrning och signalering, uppdaterad genom direktiv 2007/153/EG.
- Bilaga A TSD Trafikstyrning och signalering, uppdaterad genom direktiv 2008/386/EG.
- Bilaga A TSD Trafikstyrning och signalering, uppdaterad genom direktiv 2010/79/EG.
- UNISIG SUBSET-038, Off-line Key Management FIS, v2.1.9 (*informativt dokument*).
- UNISIG SUBSET-091, Safety Requirements for the Technical Interoperability of ETCS in Levels 1 & 2, v2.2.11.
- UNISIG SUBSET-091, Safety Requirements for the Technical Interoperability of ETCS in Levels 1 & 2, v2.5.0.

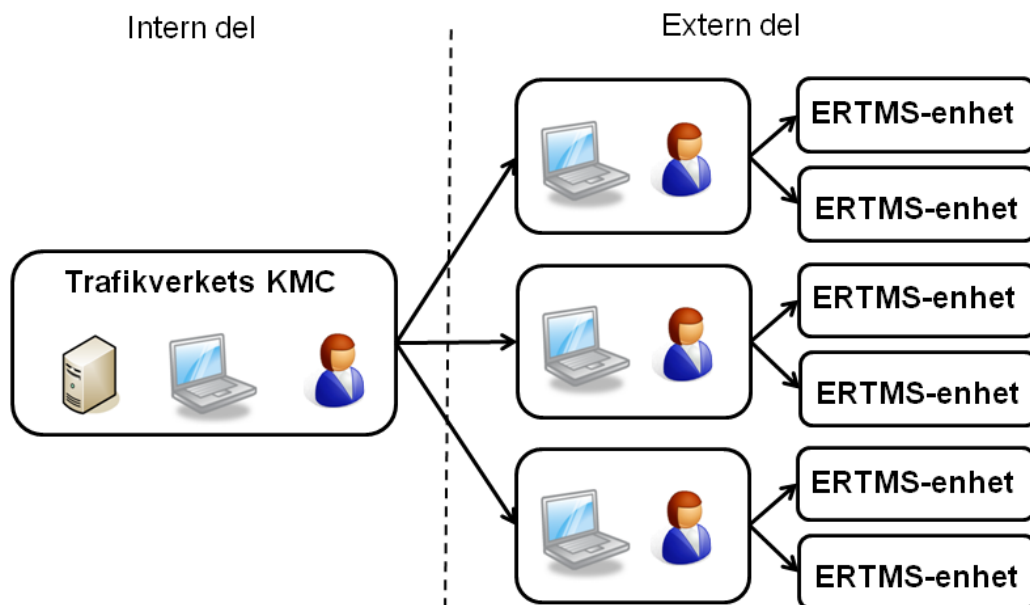
UNISIG SUBSET-098 behandlar kryptonycklar för säker kabeltransmission för exempelvis RBC-RBC, men endast informativt för KMS och är inte tillämpat i Trafikverkets KMS.

6 Trafikverkets KMS

6.1 Beskrivning

Nyckelhanteringsprocessen är uppdelad i en intern och en extern del, se figur 6.1. Syftet med att dela upp processen i separata delar är att underlätta och förenkla hanteringen av uppdateringar och godkännanden.

- Den interna delen omfattar Trafikverkets KMC. Den interna ställer gemensamma krav för KM-domänen och beskriver nyckelhanteringsprocessen från den externa uthämtningssidan.
- Den externa delen kan delas upp i ett flertal separata nyckelhanteringsprocesser, med det enda gemensamma att de är knutna till samma KMC. Varje extern del kan anpassas efter de lokala och organisatoriska förutsättningar som finns hos olika organisationer och dess ERTMS-enheter. Kravet är dock att den externa nyckelhanteringsprocessen är anpassad mot den interna nyckelhanteringsprocessen och följer de grundläggande krav som den interna delen ställer. Den externa delen ansvarar för att beskriva nyckelhanteringsprocessen från det att kryptonycklarna har laddats ner fram tills dess de kvitteras.



Figur 6.1: Nyckelhanteringsprocessen är uppdelad i två separata processer.

6.2 Roller

Det finns tre grundläggande roller som ska finnas inom en KM-domän [3]:

- KMC-administratör
- KMC-operatör
- KMC-tekniker

6.2.1 KMC-administratör

KMC-administratör ska:

- Ansvara för alla administrativa uppgifter i KMC.
- Ansvara för att hantera processen för nyckelhantering och därigenom möjliggöra för interoperabel trafik.
- Om det uppstår säkerhetsproblem med en kryptonyckel skall problemet lösas och eventuellt andra berörda KM-domäners administratörer informeras.
- Lösa eventuella problem som kan uppstå under nyckeldistribution till eller från en annan KM-domän.
- Begära att andra KMC administratörer ska radera kryptonycklar genererade i Trafikverkets KMC, eller på begäran av andra KMC administratörer raderar kryptonycklar skapade i deras KMC:er. KMC-administratören ska försäkra sig om att alla kopior av kryptonyckeln är

raderade och sedan skicka en bekräftelse tillbaka till den KMC-administratör som gick ut med begäran om radering.

Det är möjligt att utse flera administratörer, men vid ett och samma tillfälle får endast en KMC-administratör vara i aktiv tjänst.

6.2.2 KMC-operatör

KMC-operatör ska:

- Arbeta underordnat KMC-administratören med ansvar för de operativa uppgifterna i KMC.
- Hålla ordning på en förteckning över de ombordenheter som ingår i Trafikverkets KM-domän och som används i gränsöverskridande trafik till andra KM-domäner.
- Skapa, uppdatera, radera och distribuera kryptonycklar till ERTMS-enheter.
- Hålla loggar och kontaktuppgifter uppdaterade och aktuella.
- Ta emot och vidarebefordra inrapporterade säkerhetsavvikelser till KMC-administratören, t.ex. rapporter om misstänkt röjda kryptonycklar.

6.2.3 KMC-tekniker

KMC-tekniker ska:

- Ansvar för de uppgifter som finns utanför KMC.
- Hämta, installera och avinstallera kryptonycklar som används i KM-domänens ERTMS-enheter.
- Genomföra felsökningar och funktionstester för att säkerställa att en ombordenhet kan upprätta kontakt med radioblockcentral(er) i andra KM-domäner. Test ska om möjligt genomföras innan ett fordon ska passera gränsen mellan två KM-domäner, risk finns annars att ombordutrustningen inte får fortsatt körbesked vid gränsen och därmed skapas oönskade trafikstörningar.

6.3 Behörighet

Systemet är tillgängligt för behöriga användare via ett webbgränssnitt. Av säkerhetsskäl används två webbgränssnitt vilka är uppdelade för intern och extern åtkomst. Intern åtkomst ges till användare som ska arbeta i Trafikverkets KMC med att till exempel skapa, radera, lagra och distribuera kryptonycklar. Extern åtkomst är avsett för användare som behöver tillgång till att hämta och kvittera kryptonycklar.

Endast personer som för sin tjänsteutövning behöver tillgång till kryptonycklar ska tillåtas få behörighet. Om arbetsuppgifterna inte längre kräver behörighet ska behörigheten snarast dras tillbaka.

6.3.1 Behörighetsnivåer i KMC-applikationen

Det finns tre behörighetsnivåer i KMC-applikationen:

- Administratör, har fullständiga rättigheter.
- KMAC-uthämtare, har behörighet att hämta KMAC-nycklar.
- KTRANS-uthämtare, har behörighet att hämta KTRANS-nycklar

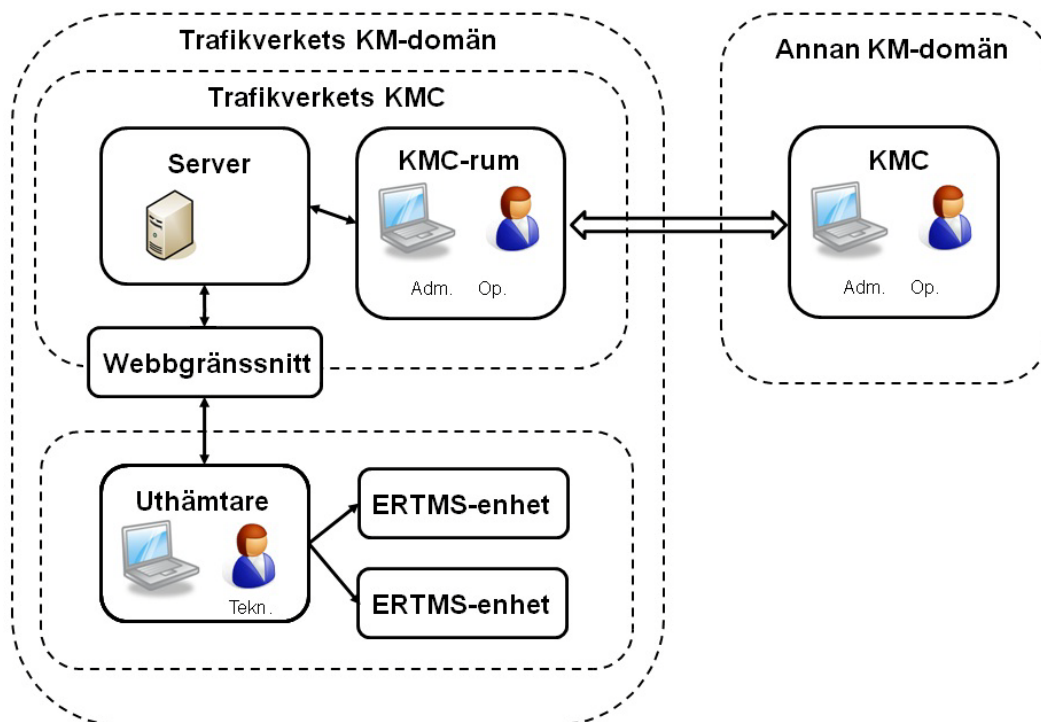
7 Teknik

7.1 Teknisk miljö

För att hantera kryptonycklar i Trafikverkets KMC har Trafikverket valt att utveckla ett eget system som i grova drag består av en KMC applikation som körs i en servermiljö och är tillgänglig via ett webbgränssnitt, se figur 7.1. Systemet är utvecklat för kryptonyckelhantering som uppfyller den europeiska gemensamma specifikationen subset-038 [3].

Servermiljön där KMC-applikationen kör ska ha begränsat tillträde, endast namngiven och säkerhetsklassad it-personal får arbeta med konfiguration, drift och underhåll av server som används för kmc-applikationen. Genom angränsade it-system ges sedan åtkomst till KMC för interna och externa användare.

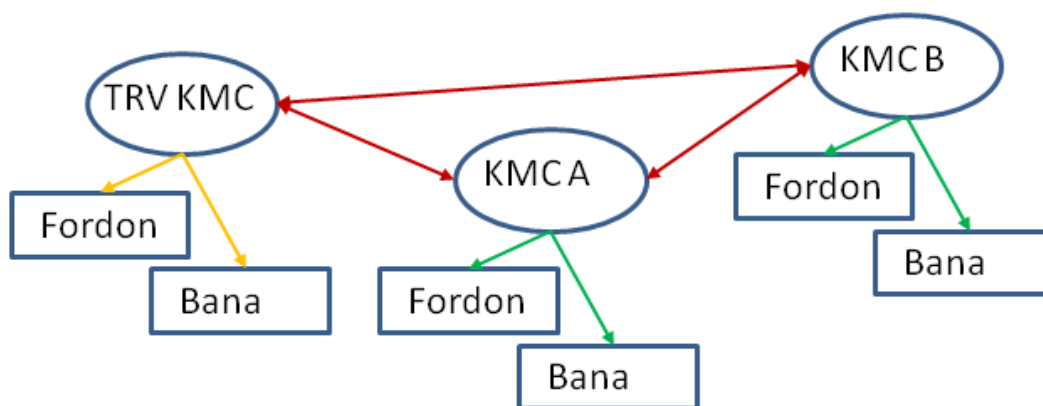
KMC-administratör och KMC-operatör ges tillgång till systemet från en klientdator i KMC-rummet. KMC-tekniker får tillgång till KMC via en internetansluten klientdator.



Figur 7.1: Den tekniska miljön och kopplingen till användarna.

7.2 Gränssnitt

Hantering av krypteringsnycklar förutsätter att det finns gränssnitt för nyckelhantering mellan alla inblandade parter [1][2]. I figur 7.2 visar med röda pilar det från Europeiskt håll specificerade gränssnittet för utbyten av kryptonycklar KMC till KMC. I gult representeras gränssnitt för distribution av kryptonycklar till de ERTMS-enheter som ingår i Trafikverkets KM-domän. De gröna pilarna representerar alla övriga gränssnitt som kan användas för att distribuera kryptonycklar mellan KMC och ERTMS-enheter.



Figur 7.2: Gränssnitt för överföring av kryptonycklar i ERTMS.

7.2.1 Inom Trafikverkets KM-domän

Trafikverket har tagit fram ett eget gränssnitt för att distribuera kryptonycklar från Trafikverkets KMC till alla ERTMS-enheter som är anslutna till Trafikverkets KMC.

Anm: Det finns inga krav på hur gränssnittet ska se ut mellan KMC och de ERTMS-enheter som ingår i en KM-domän. Trafikverkets gränssnittsspecifikation är det föredragna gränssnittet, men möjlighet finns att anpassa Trafikverkets KMC mot andra gränssnitt.

7.2.2 Mot andra KM-domäner

Gränssnitt för KMC till KMC nyckelutbyte följer Europeiska specifikationer för att möjliggöra utbyte av kryptonycklar med andra KM-domäner [3].

7.3 Teknisk utrustning

Teknisk utrustning avsedd att användas för nyckeluthämtning eller installation som kan innehålla oskyddade kryptonycklar från Trafikverkets KMC ska:

- Hållas under sådan kontroll att ingen obehörig kan få tillgång till kryptonycklarna.
- Underhållas och uppdateras på sådant sätt att sårbarheter som kan leda till att obehöriga får tillträde till utrustningen undviks.

Vid utbyte av utrustning eller lagringsmedia som innehåller oskyddade kryptonycklar, ska åtgärder vidtas så att kryptonycklarna förstörs eller förblir oåtkomliga för obehöriga.

8 KMS Drift och underhåll

För att få tillgång till kryptonycklar, finns en anslutningsprocess i två steg:

1. Den organisation som äger eller ansvarar för en ERTMS-enhet som behöver tillgång till kryptonycklar för sin funktion ska först registreras i Trafikverkets KMC. I processen ska den ansökande organisationen intyga att Trafikverkets krav kommer att följas, ange kontaktpersoner för organisationen och dess nyckeluthämtare. Nödvändiga behörigheter kommer därefter att ges till nyckeluthämtare. Detta är närmare beskrivet i avsnitt 8.1.
2. Registrera de ERTMS-enheter som behöver få kryptonycklar distribuerade från Trafikverkets KMC. En registrerad ERTMS-enhet kommer om inte annat är överenskommet att få tilldelat kryptonycklar. Detta är närmare beskrivet i avsnitt 8.2.

Har en organisation blivit registrerad i det första steget, kan samma organisation i fortsättningen registrera fler ERTMS-enheter enbart genom processen beskriven i det andra steget. När en ny ERTMS-enhet ska tas i bruk räcker det med att den vid registreringen kan kopplas mot en tidigare registrerad organisation i Trafikverkets KMC. På så sätt registreras enheten och kryptonycklarna kommer att distribueras till de nyckeluthämtare som har meddelats i det första steget.

ERTMS-enheter som är registrerade kommer att få kryptonycklar från KMC. Kryptonycklarna görs tillgängliga för den eller de nyckeluthämtare som är registrerade som mottagare av ERTMS-enhetens kryptonycklar, processen beskrivs närmare i avsnitt 8.3. Ett fordonsätt kan inte trafikera en ERTMS-utrustad bana innan kryptonycklarna har installerats i både ombordutrustningen och marksystemet.

Figurerna 8.1 och 8.2 ger en övergripande bild av nyckelhanteringsprocessen.



Figur 8.1: Övergripande bild av nyckelhanteringsprocessen för ombordutrustning.



Figur 8.2: Övergripande bild av nyckelhanteringsprocessen för markutrustning.

8.1 Anslutning till KMC

8.1.1 Trafikverkets ERTMS-enheter

Ansvariga avdelningar/enheter inom Trafikverket som ansvarar för driften av ERTMS-enheter som är beroende av kryptonycklar för sin funktion, ska för att få tillgång till kryptonycklar:

- Uppfylla de krav som ställs på hanteringen av kryptonycklar och tillse att eventuella underleverantörer också förbinder sig till att följa kraven.

Ingen behörighet får ges till icke Trafikverks personal innan det har säkerställts att kraven som Trafikverket ställer på hanteringen av kryptonycklar ska följas. Detta bör vara reglerat genom avtal.

- Ansökan om anslutning till Trafikverkets KMC, ska av den sökande lämnas personligen eller med rekommenderad post skickas till Trafikverkets KMC med uppgifter om:
 - o Kontaktperson för den avdelningar/enheter inom Trafikverket som ansvarar för markenheten.
 - o Mottagare av kryptonycklar, den eller de som ska ta emot kryptonycklar och behöver få den behörighet som krävs. Uppgifter som ska lämnas, är de uppgifter som Trafikverket behöver för att kunna ta kontakt, ge och administrera behörigheter och identifiera personen.
 - o E-post adress som ska användas av KMC för att informera när nya kryptonycklar finns att hämta.

8.1.2 Icke Trafikverkets ERTMS-enheter

Den organisation som äger eller ansvarar för ERTMS-utrustning (ombordutrustningen) ska:

- Uppfylla de krav som ställs på hanteringen av kryptonycklar och tillse att eventuella underleverantörer också förbinder sig till att följa kraven.

Ingen behörighet får ges till icke Trafikverks personal innan organisationen som äger eller ansvarar för ERTMS-enheten har förbundit sig att följa de krav som Trafikverket ställer på hanteringen av kryptonycklar. Detta bör vara reglerat genom avtal.

- Ansökan om anslutning till Trafikverkets KMC, ska av den sökande lämnas personligen eller med rekommenderad post skickas till Trafikverkets KMC med uppgifter om:
 - o Kontaktperson för den organisation som äger eller ansvarar för ombordenheten.
 - o Mottagare av kryptonycklar, den eller de som ska ta emot kryptonycklar och behöver få den behörighet som krävs. Uppgifter som ska lämnas, är de uppgifter som Trafikverket behöver för att kunna ta kontakt, ge och administrera behörigheter och identifiera personen.
 - o E-post adress som ska användas av KMC för att informera när nya kryptonycklar finns att hämta.

8.1.3 Lämna KMC

Anslutningen till KMC som genomförs i avsnitt 8.1.1 eller 8.1.2, kan avslutas genom att kontaktpersonen personligen eller med rekommenderad post skickar en underskriven begäran om utträde ur KMC. Vid utträde ska samtliga ERTMS-enheter avregistreras ur KMC.

När en ERTMS-enhet avregistreras skall alla kryptonycklar raderas och alla behörigheter till Trafikverkets KMC avslutas. Om det gäller ombordutrustning ska de kryptonycklar som lämnats ut även inaktiveras genom att de tas bort från markenheterna.

Om kryptonycklar raderas som berör andra KM-domäner, ska KMC-administratörerna i berörda KM-domäner informeras.

8.1.4 Ändring av registrerade uppgifter

Om någon av de uppgifter som har lämnats behöver ändras, ska detta göras genom att kontaktpersonen för den organisation som äger eller ansvarar för ERTMS-enhet skickar in en underskriven begäran om ändring av uppgifter.

8.2 Registrering av ERTMS-enhet

8.2.1 Registrering

Alla ERTMS-enheter som behöver tillgång till kryptonycklar måste registreras i Trafikverkets KMC. Den som äger eller ansvarar för ERTMS-enheter ska efter anslutningen till KMC i avsnitt 8.1 även registrera de ERTMS-enheter som ska anslutas.

Uppgifter som ska lämnas till KMC:

- Organisationsnamn.
- Kontaktperson (skall vara samma kontaktperson som anges i avsnitt 8.1).
- ERTMS-enhetens ETCS-ID.
- Placering (gäller endast markenhet).

8.2.2 Avregistrering

En ERTMS-enhet kan avregistreras från Trafikverkets KMC. Detta gör genom att kontaktpersonen för den organisation som äger eller ansvarar för ERTMS-enheter skickar in en begäran om avregistrering.

Uppgifter som ska lämnas till KMC:

- Organisationsnamn.
- Kontaktperson (skall vara samma kontaktperson som anges i avsnitt 8.1).
- ERTMS-enhetens ETCS-ID.

När en ERTMS-enhet avregistreras skall alla kryptonycklar raderas. Om kryptonycklar raderas som berör andra KM-domäner, ska KMC-administratörerna i berörda KM-domäner informeras.

8.3 Hantering av kryptonycklar

8.3.1 Ombordutrustning

1. Operatörer i KMC ska arbeta för att det finns aktuella och säkra kryptonycklar utgivna i god tid. För att underlätta planering av service och underhåll bör nya kryptonycklar finnas tillgängliga i god tid innan giltighetstiden för en tidigare kryptonyckel går ut.
2. När nya nycklar blir tillgängliga skickas automatisk ett meddelande till angiven e-postadress för ERTMS-enheten. Mottagaren av e-postmeddelandet ska se till att kryptonycklarna blir uthämtade och installerade.
3. Behörig nyckeluthämtare ska logga in på Trafikverket KMC och hämta ner de nya kryptonycklarna.

Amn: Om särskilda behov föreligger kan kryptonycklar distribueras på annat sätt. En förutsättning är att kryptonycklarnas sekretess inte äventyras. Kryptonycklarna får endast överlämnas till person som har rätt att hämta ut kryptonycklar från Trafikverkets KMC. Speciell hänsyn ska tas till kraven i avsnitt 10.

4. Kryptonycklarna ska installeras i avsedd ERTMS-enhet.
5. Kvittensfilen som genereras under installationen av kryptonycklarna ska av den behöriga nyckeluthämtaren laddas tillbaka till KMC, genom att åter logga in på KMC. På detta sätt bekräftar nyckeluthämtaren att kryptonycklarna är korrekt installerade.

Amn: Kvittensfil skapas endast i utrustning som stödjer Trafikverkets specificerade gränssnitt, FFFIS KMC – OBU. Används utrustning som inte stödjer Trafikverkets gränssnitt, ska en bekräftelse skickas till Trafikverkets KMC, som anger ETCS-ID på den ombordutrustning i vilken kryptonycklarna har installerats.

6. Om kryptonycklar till en annan KM-domän har installerats ska KMC-teknikern genomföra en funktionstest för att säkerställa att ombordutrustningen kan kontakta nödvändiga RBC:er i den andra KM-domänen.
7. Om kryptonycklar har installerats som ska användas för interoperabel trafik ska KMC-administratören informera KMC-administratören i den berörda KM-domänen om att kryptonycklarna är installerade i ombordutrustningen.

8.3.2 Markutrustning

1. När operatören i KMC genererar kryptonycklar till ombordutrustning eller tar emot kryptonycklar från annan KMC, ska dessa göras tillgängliga i god tid för ansvarig nyckeluthämtare/installatör i marksystemet. I det fall som kryptonycklar tas emot från annan KMC för installation.
2. När nya nycklar blir tillgängliga skickas automatisk ett e-postmeddelande till angiven kontaktperson för ERTMS-enheten. Mottagaren av e-postmeddelandet ska se till att kryptonycklarna blir uthämtade och installerade.

3. Behörig nyckeluthämtare ska logga in på Trafikverket KMC och hämta ner de nya kryptonycklarna.

Anm: Om särskilda behov föreligger kan kryptonycklar distribueras på annat sätt. En förutsättning är att kryptonycklarnas sekretess inte äventyras. Kryptonycklarna får endast överlämnas till person som har rätt att hämta ut kryptonycklar från Trafikverkets KMC. Speciell hänsyn ska tas till kraven i avsnitt 10.

4. Kryptonycklarna ska installeras i avsedd ERTMS-enhet.
5. Kvittensfilen som genereras under installationen av kryptonycklarna ska av den behöriga nyckeluthämtaren laddas tillbaka till Trafikverkets KMC, genom att åter logga in på KMC. När kvittensfilen laddas upp, bekräftar nyckeluthämtaren att kryptonycklarna är korrekt installerade.

Anm: Kvittensfil skapas endast i utrustning som stödjer Trafikverkets specificerade gränssnitt, FFFIS KMC – RBC. Används utrustning som inte stödjer Trafikverkets gränssnitt, ska en bekräftelse skickas till Trafikverkets KMC, som anger ETCS-ID för den markutrustning i vilken kryptonycklarna har installerats.

6. Om kryptonycklar har installerats som ska används i interoperabel trafik, ska KMC-administratören informera KMC-administratören i den berörda KM-domänen om att kryptonycklarna är installerade.

8.4 Bekräftelse

När Trafikverkets KMC har gjort en ändring av någon av de uppgifter som har lämnats under någon av punkterna i avsnitt 8, ska en bekräftelse skickas till kontaktpersonen för den organisationen som äger eller ansvarar för aktuell enhet. Om organisationens kontaktperson får en bekräftelse där uppgifter som inte stämmer, så skall denne snarast meddela detta till Trafikverkets KMC.

9 Spårbarhet

9.1 Dokumentering

Det är viktigt att händelser och åtgärder dokumenteras. I avsett säkerhetsskåpet ska en pärm förvaras tillsammans med klientdatorn. I pärmen ska aktiviteter i Trafikverkets KMC antecknas, så att det är möjligt att upprätthålla spårbarhet. Följande förteckningar ska finnas:

Aktivitetslogg: En kronologisk loggbok där dagliga aktiviteter händelser ska antecknas i form av datum och aktivitet.

Kontaktpersoner och nyckeluthämtare: Kontaktuppgifter ska hållas uppdaterade och aktuella. Den anslutande organisationen har i under anslutningsprocessen lämnat kontaktuppgifter till minst en kontaktperson och en e-postadress för information om att kryptonycklar finns att hämta. Uppgifterna får användas för ge behörighet samt ta kontakt och förmedla information som berör kryptonycklar eller Trafikverkets KMC.

Register över anslutna ERTMS-enheter: Uppgifterna ska hållas uppdaterade och aktuella.

9.2 Personuppgifter

Hantering av personuppgifter som i KMC-applikationen/databasen eller i pärmen ska följa svensk lagstiftning om personuppgifter, vilket bland annat innebär att uppgifterna endast får sparas under en begränsad tid.

Uppgifter i KMC-applikationens transaktionslogg får för närvarande inte sparas längre än 10 år. Det är möjligt att ta bort eller ändra användarnamn i transaktionsloggen, men detta får endast genomföras efter godkännande från KMC-administratören.

10 Säkerhet

10.1 Hantering av oskyddade nycklar

En kryptonyckel anses skyddad om den är krypterad med en krypteringsalgoritm som är minst lika stark som 3DES (TDEA med tre skilda nycklar) eller om den är lagrad i en säker modul som har godkänts av Trafikverket.

All teknisk utrustning som innehåller eller kan innehålla oskyddade kryptonycklar ska hållas under sådan kontroll att ingen obehörig kan få tillgång till kryptonycklarna.

Om utrustning eller lagringsmedia som har använts till att lagra oskyddade krypteringsnycklar ska bytas ut eller kasseras, ska informationen förstöras på ett sådant sätt att ingen information kan gå att återställa.

10.2 Rörda nycklar

Om utrustning eller lagringmedium har försvunnit eller att kryptonycklar har eller misstänks ha blivit exponerade för obehörig person ska detta snarast meddelas till Trafikverkets KMC. Den som lämnar en anmälan ska försäkra sig om att anmälan har tagits emot. Trafikverkets KMC ska snarast möjligt skicka en bekräftelse till den person som lämnat anmälan om att anmälan är mottagen.

Beslut om en nyckel är röjd och beslut av nödvändiga åtgärder ska fattas av Trafikverket. Om en nyckel anses vara röjd ska berörda kryptonycklar snarast ersättas med nya. KMC-administratören ska meddela beslutet till den som lämnat in anmälan.

Vid misstanke att krypteringsnycklar har röjts ska KMC-administratören informeras och därefter sammankalla till ett säkerhetsråd som ska ta beslut om nödvändiga åtgärder. Säkerhetsrådet ska protokollföra mötet och beslutet.

10.3 Kontaktpersoner

Vid anslutning till Trafikverkets KMC i avsnitt 8.1 ska kontaktperson anges. Endast den angivna kontaktpersonen tillåts:

- Lämna och ändra uppgifter som rör kontaktperson eller nyckeluthämtare.
- Registrera eller avregistrera ERTMS-enheter.
- Begära utträde ur Trafikverkets KMC.

11 Hjälpmedel och referenser

11.1 Hjälpmedel

Inga hjälpmedel finns för detta dokument.

11.2 Referenser

- [1] TSD Trafikstyrning och signalering (höghastighet), kommissionens beslut 2006/860/EG.
- [2] TSD Trafikstyrning och signalering (konventionell), kommissionens beslut 2006/679/EG.
- [3] SUBSET 038, Off-line Key Management FIS, UNISIG, v2.1.9
- [4] SUBSET-091, Safety Requirements for the Technical Interoperability of ETCS in Levels 1 & 2, UNISIG, v2.2.11 och v2.5.0