

Gebruiksvoorschrift

ETCS Key Management

Beherende instantie:
Inhoud verantwoordelijke:
Status:

IM Kwaliteitsmanagement
Manager Wim Griffioen
Concept/Definitief

Datum van kracht: 01-01-2010	Versie: 001	Documentnummer: GVS60560-1
---	------------------------------	---

INHOUD

1	Revisiegegevens	3
2	Algemeen	4
2.1	Scope	4
2.2	Van kracht verklaarde regelgeving	4
2.3	Definities en afkortingen	4
3	Beschrijving	6
3.1	Doel van de procedure	6
3.2	Toepassingsgebied	6
3.3	Algemene beschrijving	6
4	Werkwijze	8
4.1	Aanvraag van sleutel (KMAC) voor trein aan het KMC	8
4.2	Afspreken van transportsleutel (K-KMC)	8
4.3	Sleutelcapaciteit treinapparatuur (optie 1 /2)	8
4.4	KMC genereert en verstrekt de sleutel (KMAC)	9
4.5	Aanvraag door eigenaar i.p.v. spoorwegonderneming	9
4.6	Werkingstest	9
5	Vervanging van sleutels	11
5.1	Veiligheidsredenen	11
5.2	Vervaldatum	11
5.3	Verwijderen van sleutels	11
6	Bijlagen	13
6.1	Aanvraagformulier voor KMAC – 1 (Algemene informatie)	13
6.2	Aanvraagformulier voor KMAC –2 (Treinspecifieke informatie)	14
6.3	Leveringstijden	15
6.4	Contactgegevens KMC ProRail	15
7	Beheervoorwaarden	16
7.1	ProRail levert sleutels aan de aanvrager	16
7.2	De aanvrager implementeert sleutels in de trein	16
7.3	Het gebruik van de K-KMC transportsleutel	16
7.4	Uitvoeren van testen	16
7.5	Beveiligingsmaatregelen	17

1 Revisiegegevens

Datum	Versie	Hoofdstuk/ paragraaf	Wijziging
13-1-2010	1	Geheel	Dit document bestond voorheen als "GOR ERTMS Key management ten behoeve van materieeltoelating 1.0". Deze GVS is een inhoudelijk verbeterde versie van bovengenoemde GOR.

2 Algemeen

ProRail heeft op een aantal - in de Netverklaring aangegeven – baanvakken het ERTMS/ETCS beveiligingssysteem in gebruik. Het Gebruiksvoorschrift (GVS) heeft betrekking op een dienst uit het Basistoegangspakket. Dit gebruiksvoorschrift maakt deel uit van de toegangsovereenkomst tussen ProRail en de spoorwegonderneming die op ETCS level 2 baanvakken rijdt.

Krachtvoertuigen die op dergelijke baanvakken rijden dienen voorzien te zijn van apparatuur voor de datacommunicatie ten behoeve van ERTMS. In dit GVS wordt de procesgang beschreven voor de aanvraag en het beheer van sleutels die nodig zijn om te rijden op ETCS Level 2 baanvakken.

ProRail stelt in de Algemene Voorwaarden bij de Toegangsovereenkomst o.a. voorwaarden aan de geheimhouding van gevoelige informatie. Die voorwaarden beogen een zorgvuldig beheer van de verstrekte sleutels teneinde:

- storingen en niet-beschikbaarheid te voorkomen;
- misbruik van het systeem door onbevoegden te voorkomen;

In dit GVS worden de genoemde voorwaarden verbijzonderd.

2.1 Scope

In dit GVS wordt de procesgang beschreven voor het aanvragen en beheer van sleutels die nodig zijn om te rijden op ETCS Level 2 baanvakken.

Het proces start bij het aanvragen van een sleutel middels een aanvraagformulier.

Dit GVS beschrijft het aanvraagproces en het beheer van sleutels die noodzakelijk zijn om te kunnen rijden op baanvakken die zijn voorzien van ETCS Level 2. Dit is een invulling van TSI CCS [1] paragraaf 4.2.8 “Beheer”, voor zover van toepassing voor de infrabeheerder.

Doelgroep

- Alle spoorwegondernemingen die in de Toegangsovereenkomst het Basistoegangspakket afnemen van ProRail en rijden onder Level 2 op ERTMS baanvakken.

2.2 Van kracht verklaarde regelgeving

Ref. nr.	Naam document	Nummer	Status
[1]	TSI Command Control Signalling Conventional Rail en High Speed		
[2]	Subset-038 Off Line Key management FIS (dit is onderdeel van [1], hier expliciet genoemd vanwege de relevantie voor dit GVS)	V2.1.9	

2.3 Definities en afkortingen

Term	Verklaring
Aanvrager	Degene die de aanvraag voor sleutels voor een voertuig indient dat op een ERTMS Level 2 baanvak dient te gaan rijden.
ETCS_ID (NID_Engine)	Unieke identificatie van treinapparatuur. Het beheer van deze

ETCS Key Management

	identificatie verloopt conform Subset-054 [1].
ETCS_ID (NID_KMC)	Unieke identificatie van een KMC. Het beheer van deze identificatie verloopt conform Subset-054 [1].
ETCS Level 2	European Train Control System; Europees gestandaardiseerd treinbeïnvloedingssysteem. Level 2 maakt gebruik van GSM-R datacommunicatie om rijtoestemmingen aan de trein te geven.
ETCS-voertuig	Een spoorvoertuig dat voorzien is van ETCS-apparatuur.
EVC	European Vital Computer; Treingebonden ETCS apparatuur
RBC	Radio Block Center; Baangebonden ETCS apparatuur
Home-KMC	Alle ETCS apparatuur (RBC of EVC) is gerelateerd aan één KMC dat zorg draagt voor daadwerkelijke installatie van sleutels in de apparatuur. Dit KMC wordt het Home-KMC genoemd.
Home-KMC EVC	Het KMC dat zorg draagt voor het sleutelbeheer in de treinapparatuur
Home-KMC RBC (=ProRail KMC)	Het KMC dat zorg draagt voor het sleutelbeheer in de baanapparatuur. Het ProRail KMC is het Home-KMC voor de Nederlandse baanvakken waar onder Level 2 gereden kan worden.
KMAC	Sleutel waarmee berichten tussen trein (EVC) en baan (RBC) wordt beveiligd
KMC	Key Management Center: organisatie die sleutels genereert, uitgeeft en plaatst in ETCS apparatuur. Een KMC kan zich toespitsen op treinapparatuur, baanapparatuur of beide.
K-KMC	Transportsleutel waarmee het transport van KMAC tussen twee KMC's wordt beveiligd. (Technisch gelijk aan KTRANS)
KTRANS	Transportsleutel waarmee het transport van KMAC vanuit het KMC naar de ETCS apparatuur wordt beveiligd. (Technisch gelijk aan K-KMC)
Triviale versleuteling	Een ongewenste versleuteling die zwakker is dan het 3DES-algoritme dat in Subset-037 en Subset-038 van de TSI-CCS [1] beschreven wordt.
TSI CCS	Technical Specification for Interoperability Command Control and Signalling (zowel de HighSpeed als de ConventionalRail-versies)

3 Beschrijving

3.1 Doel van de procedure

Het gebruik van ETCS Level 2 betekent dat het beveiligingssysteem aan baanzijde via radio communicatie rijtoestemmingen verleent aan treinen die willen rijden op een traject beveiligd met ETCS. Deze berichten zijn veiligheidsrelevant waardoor ze volgens de TSI CCS [1] moeten worden beveiligd met een encryptiesleutel. Zonder de sleutel kan er geen veilige radio communicatie tot stand komen met als gevolg dat de ETCS trein niet kan rijden onder Level 2.

3.2 Toepassingsgebied

Deze procedure is van toepassing op alle krachtvoertuigen voorzien van ETCS die onder Level 2 moeten kunnen rijden op baanvakken voorzien van ETCS Level 2 waarvoor ProRail optreedt als KMC. De sleutels worden uitgegeven voor zowel commercieel gebruik als voor testdoeleinden.

3.3 Algemene beschrijving

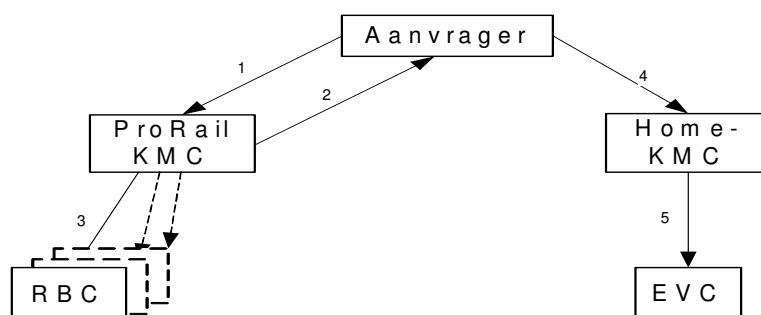
Alle ETCS krachtvoertuigen krijgen een unieke sleutel die wordt opgenomen in de ETCS treinapparatuur. De overeenkomstige sleutel wordt ook aan de baanzijde in de Radio Block Centers (RBC's) van het baanvak opgenomen. Deze sleutel wordt voor Nederlandse ETCS baanvakken gegenereerd door het Key Management Center (KMC) van ProRail. Bij het genereren van de sleutel wordt een koppeling gelegd met de ETCS ID (NID_Engine) van het krachtvoertuig. De NID_Engine krijgt volgens Europese afspraken een unieke waarde, zie hiervoor Subset-054, ([1] Bijlage A, Index23). Daardoor is de gegenereerde sleutel ook uniek.

Voor sleutelbeheer dient er voor elk ETCS apparaat (EVC en RBC) een zgn "Home-KMC" aangewezen te worden. Een Home-KMC draagt er zorg voor dat sleutels in de bijbehorende apparatuur geplaatst worden. Het ProRail KMC is Home-KMC van alle RBC's in Nederland.

De spoorwegonderneming dient bij de aanvraag aan te geven welke partij het Home-KMC van het krachtvoertuig is die de sleutel in de treinapparatuur zal opnemen. Het verzenden van de sleutel van het KMC aan deze partij wordt beveiligd met een transportsleutel (K-KMC). Deze transportsleutel wordt gegenereerd door het KMC.

De transportsleutel kan voor verzending van meerdere sleutels worden gebruikt.

In Figuur 1 is schematisch weergegeven hoe de sleutelaanvraag en implementatie verlopen, er van uit gaande dat er met het Home-KMC-EVC een transportsleutel is uitgewisseld. De verschillende stappen kunnen gedeeltelijk parallel verlopen.



Figuur 1: Stappen sleutelaanvraag en implementatie

- 1) Aanvraag van nieuwe sleutel
- 2) Aanvrager ontvangt (gecodeerde) sleutel
- 3) ProRail implementeert sleutel aan de baanzijde
- 4) Aanvrager stuurt sleutel naar Home-KMC-EVC van het krachtvoertuig
- 5) Home-KMC-EVC decodeert sleutel en implementeert deze in de EVC van het krachtvoertuig

Het is de taak van de aanvrager om de invloed van de verkregen sleutels op het inzetcertificaat van het materieel te beoordelen. Bij materieel dat niet eerder onder Level 2 op het aangevraagde baanvak gereden heeft zal na plaatsing van de sleutel in het krachtvoertuig het inzetcertificaat doorgaans herzien moeten worden voordat de trein ingezet mag worden op dat ETCS-baanvak. De aanvraag en levering van ETCS sleutels voorziet in de technische middelen noodzakelijk voor toelating d.m.v. het inzetcertificaat.

4 Werkwijze

4.1 Aanvraag van sleutel (KMAC) voor trein aan het KMC

De aanvrager downloadt via de ProRail website het formulier “Aanvraag formulier voor KMAC”, dit is tevens als bijlage aan dit document toegevoegd. Op dit formulier moet onder andere de volgende gegevens worden ingevuld:

- Identificatie van het krachtvoertuig zoals de spoorwegonderneming het krachtvoertuig aanduidt;
- ETCS ID (NID_Engine);
- Type treinapparatuur mbt sleutelcapaciteit (optie 1 of optie 2) (zie paragraaf 4.3);
- het Home-KMC-EVC dat de sleutel in het krachtvoertuig implementeert;
- baanvak(ken) waarvoor een sleutel aangevraagd wordt;
- beoogde ingangsdatum.

Het volledig ingevulde aanvraagformulier wordt gestuurd aan: kmc@prorail.nl.

Opmerking: Indien er een groot aantal krachtvoertuigen tegelijk aangevraagd wordt kan - in overleg met het ProRail KMC - de benodigde informatie ook in een ander formaat dan het genoemde formulier aangeleverd worden.

4.2 Afspreken van transportsleutel (K-KMC)

Op het “Aanvraagformulier KMAC” wordt gevraagd naar het Home-KMC-EVC dat de sleutel (KMAC) in de ETCS treinapparatuur zal implementeren. Het beheer en gebruik van de sleutels is onderhevig aan de voorwaarden zoals beschreven in Hoofdstuk 7 van dit document. In het geval dat de spoorwegonderneming de aanvrager is, is deze GVS, inclusief de voorwaarden onderdeel van de Toegangsovereenkomst. Voor de gevallen dat er geen Toegangsovereenkomst is met de aanvrager (zie ook 4.5) zullen de voorwaarden middels een aparte overeenkomst tussen ProRail –KMC en aanvrager vastgelegd worden.

De transportsleutel (K-KMC) wordt op veilige wijze overhandigd door het ProRail KMC aan de aanvrager of eventueel direct aan een contactpersoon van het Home-KMC-EVC.

In het voorkomende geval dat de aanvrager en Home-KMC-EVC niet dezelfde partij zijn, zal de aanvrager moeten borgen dat de verplichtingen door het Home-KMC-EVC uitgevoerd worden. Een aanvrager kan verschillende Home-KMC-EVC's gebruiken (bijvoorbeeld voor verschillende materieeltypes). Elk Home-KMC-EVC wordt gekenmerkt door een uniek ETCS-ID (NID_KMC).

4.3 Sleutelcapaciteit treinapparatuur (optie 1 /2)

Met betrekking tot sleutelcapaciteit zijn er twee typen treinapparatuur in omloop, aangeduid met optie 1 of optie 2:

- 1) De ETCS treinapparatuur kan slechts één enkele sleutel bevatten, deze sleutel dient opgenomen te worden in alle baanapparatuur waarmee deze trein verbinding wil maken
- 2) De ETCS treinapparatuur kan voor elk baanvak een andere sleutel bevatten.

Bij beide opties hoort een verschillend proces voor het genereren en uitwisselen van de sleutels. Bij de optie 1) apparatuur is het gangbaar dat het Home-KMC-EVC de sleutel genereert en deze aan alle relevante Home-KMC-RBC's levert. Bij optie 2) is dit precies

andersom en genereert het Home-KMC-RBC een sleutel voor het desbetreffende baanvak die vervolgens aan het Home-KMC-EVC geleverd wordt.

Opmerking: Momenteel zijn beide opties nog in gebruik, in een toekomstige versie van de ERTMS/ETCS-specificatie zal alleen optie 2) blijven bestaan.

4.4 KMC genereert en verstrekt de sleutel (KMAC)

Er van uitgaande dat er een K-KMC (zie paragraaf 4.2) is afgesproken, zal het ProRail KMC zich inspannen om binnen maximaal vijf werkdagen na binnenkomst van de aanvraag een sleutel (KMAC) te genereren en na bewerking met de transportsleutel (K-KMC) te verzenden aan de aanvrager. Het ProRail KMC zal er tevens voor zorgdragen dat de sleutel (KMAC) wordt toegevoegd aan de RBCs behorende bij de ETCS infrastructuur waar de aanvrager toegang toe heeft gevraagd. Het door de aanvrager aangewezen Home-KMC-EVC is verantwoordelijk voor het implementeren van de sleutel (KMAC) in het krachtvoertuig.

In het voorkomende geval dat het krachtvoertuig optie-1 treinapparatuur bevat, zal het Home-KMC-EVC van het krachtvoertuig de sleutel na bewerking met de transportsleutel (K-KMC) verzenden aan het ProRail KMC. Het ProRail KMC zal er zorg voor dragen dat de sleutel (KMAC) wordt toegevoegd aan de RBCs behorende bij de ETCS Level 2 infrastructuur waar de aanvrager toegang toe heeft gevraagd.

In beginsel worden de KMAC sleutels opgeleverd in het formaat zoals gedefinieerd in TSI CCS Subset-038 v2.1.9/05E537 Off line key management FIS [2]. In overleg met het ProRail KMC kan in uitzonderlijke gevallen een toegespitst formaat afgesproken worden.

4.5 Aanvraag door eigenaar i.p.v. spoorwegonderneming.

In het voorkomende geval dat de spoorwegonderneming een krachtvoertuig via lease of huur in bruikleen heeft kunnen de spoorwegonderneming en de eigenaar overeenkomen dat de eigenaar het sleutelbeheer van dit krachtvoertuig regelt. In dat geval is de eigenaar de aanvrager van de sleutels en zal dan ook het beheer van de sleutels in de treinapparatuur uitvoeren in de periode dat het krachtvoertuig in gebruik is door een spoorwegonderneming.

4.6 Werkingstest

Na implementatie van de sleutel (KMAC) in de ETCS treinapparatuur en de baan (RBC) dient onder verantwoordelijkheid van de aanvrager middels een werkingstest vastgesteld te worden of de ETCS treinapparatuur in staat is een veilige radio verbinding op te zetten met de betreffende baan (één of meer RBC's).

Bij het verstrekken van de sleutel (KMAC) aan de aanvrager geeft het KMC aan vanaf wanneer de sleutel (KMAC) in de betreffende baan (RBC's) aanwezig is.

Voor deze test is het niet noodzakelijk dat het krachtvoertuig zich op het betreffende ETCS Level 2 traject bevindt. Wel moet het krachtvoertuig zich in een gebied met voldoende GSM-R-dekking bevinden. Deze test maakt formeel onderdeel uit van de toelatingstesten van de betreffende krachtvoertuig op de betreffende infra. Een Notified Body¹ zal het testresultaat (conform de eisen in de TSI CCS) van een positief oordeel moeten voorzien.

¹ Als het gaat om een type certificering, kan de Notified Body besluiten niet elke individueel krachtvoertuig te beoordelen, maar zich beperken tot alleen een kenmerkend type-exemplaar.

Het is de taak van de aanvrager om de invloed van de verkregen sleutels op het inzetcertificaat te beoordelen en te borgen dat een krachtvoertuig met een verkregen sleutel niet ingezet wordt zonder geldig inzetcertificaat. De aanvraag en levering van ETCS sleutels voorziet slechts in de technische middelen noodzakelijk voor rijden onder ETCS Level 2.

5 Vervanging van sleutels

Er kunnen zich 2 soorten situaties voordoen waardoor sleutels vervangen moeten worden:

- om veiligheidsredenen (paragraaf 5.1)
- bij overschrijding van de vervaldatum (paragraaf 5.2).

5.1 Veiligheidsredenen

Er zijn twee mogelijke (veiligheids)redenen waardoor een sleutel vervangen moet worden:

1. de K-KMC-sleutel van een KMC is openbaar geworden.
2. de KMAC-sleutel is openbaar geworden of werkt niet meer.

Ad 1. Als de transportsleutel niet meer veilig is, moeten alle sleutels van het betreffende KMC worden vervangen. De werkwijze in dit geval staat beschreven in 7.5.

Ad 2. Als de KMAC-sleutel niet meer veilig is moet deze vervangen worden. Ook als de KMAC-sleutel niet meer werkt, moet dit aan het KMC worden gemeld. Als de oorzaak niet duidelijk is, dan kan het KMC een nieuwe sleutel genereren en ervoor zorgen dat deze in het RBC geïmplementeerd wordt.

Het kan ook voorkomen dat de KTRANS openbaar geworden is die een KMC gebruikt om de KMAC te beschermen bij transport naar de baan- of trein apparatuur. In dat geval moet de KMAC die met deze KTRANS beschermd was ook als openbaar worden beschouwd.

Omdat het krachtvoertuig al toegelaten is, hoeft er dan geen nieuwe werkingstest uitgevoerd te worden. Vanzelfsprekend is een werkingstest wel verstandig om te zien of de KMAC juist is geïmplementeerd in de ETCS treinapparatuur én in de RBC.

5.2 Vervaldatum

Indien een sleutel een vervaldatum heeft, zal het KMC, minimaal een maand voor het einde van de vervaldatum, een nieuwe sleutel genereren en deze verzenden aan de aanvrager en ervoor zorgen dat deze in het RBC geïmplementeerd wordt.

Omdat het krachtvoertuig al toegelaten is, hoeft er geen nieuwe werkingstest uitgevoerd te worden. Vanzelfsprekend is een werkingstest wel verstandig om te zien of de KMAC juist is geïmplementeerd in de ETCS treinapparatuur én in de RBC.

Opmerking: Vanwege technische beperkingen omtrent het uitwisselen van sleutels kan het voorkomen dat de werkelijke vervaldatum van de sleutels niet overeenkomt met de vervaldatum zoals deze in de uitgewisselde berichten opgenomen is.

5.3 Verwijderen van sleutels

Als de ETCS treinapparatuur van een krachtvoertuig met een geïmplementeerde KMAC uit dienst genomen wordt, worden de relevante sleutels ook uit de betrokken RBC's verwijderd. De spoorwegonderneming dient dit aan het ProRail-KMC te melden.

Ook in het geval de ETCS treinapparatuur een andere eigenaar krijgt, dient de spoorwegonderneming dit aan het ProRail-KMC te melden. Vervolgens zal in overleg besloten worden of er een nieuwe sleutel gemaakt dient te worden of dat de sleutel bruikbaar blijft.

6 Bijlagen**6.1 Aanvraagformulier voor KMAC – 1 (Algemene informatie)**

Aan: ProRail Key Management Center
Afdeling Treinbeveiligingssystemen
Postbus 2038
3500 GA Utrecht
kmc@prorail.nl

Betreft: aanvraag KMAC

Contact informatie*

Home-KMC-EVC van het materieel

Organisatie:
ETCS-ID:
Contactpersoon:
Telefoonnummer:
E-mail:

Aanvrager KMAC

Organisatie:
Contactpersoon:
Telefoonnummer:
E-mail:

Naam aanvrager:

Datum:

Plaats:

* mocht de informatie wijzigen, dient u het KMC hiervan op de hoogte te stellen.

6.2 Aanvraagformulier voor KMAC –2 (Treinspecifieke informatie)

Aan: ProRail Key Management Center
Afdeling Treinbeveiligingssystemen
Postbus 2038
3500 GA Utrecht
kmc@prorail.nl

Betreft: aanvraag KMAC

Treinspecifieke informatie

ETCS ID (NID_engine):
Identificatie zoals gebruikt door de aanvrager (naam/nummer):
Type treinapparatuur (optie 1/2):
Home-KMC-EVC trein:
Traject: Amsterdam-Utrecht / BetuweRoute/ HSL-Zuid /
Gewenste ingangsdatum:

Treinspecifieke informatie

ETCS ID (NID_engine):
Identificatie zoals gebruikt door de aanvrager (naam/nummer):
Type treinapparatuur (optie 1/2):
Home-KMC-EVC trein:
Traject: Amsterdam-Utrecht / BetuweRoute/ HSL-Zuid /
Gewenste ingangsdatum:

Treinspecifieke informatie

ETCS ID (NID_engine):
Identificatie zoals gebruikt door de aanvrager (naam/nummer):
Type treinapparatuur (optie 1/2):
Home-KMC-EVC trein:
Traject: Amsterdam-Utrecht / BetuweRoute/ HSL-Zuid /
Gewenste ingangsdatum:

Treinspecifieke informatie

ETCS ID (NID_engine):
Identificatie zoals gebruikt door de aanvrager (naam/nummer):
Type treinapparatuur (optie 1/2):
Home-KMC-EVC trein:
Traject: Amsterdam-Utrecht / BetuweRoute/ HSL-Zuid /
Gewenste ingangsdatum:

6.3 Leveringstijden

Het ProRail-KMC zal zich inspannen om een aanvraag voor een KMAC-sleutel in maximaal 5 werkdagen te verwerken. Deze termijn is alleen geldig indien er reeds een transportsleutel K-KMC tussen ProRail KMC en aanvrager overeengekomen is (zie ook 4.4)

Afhankelijk van het baanvak is er een andere doorlooptijd voor de implementatie van de sleutel in de RBC. Doorgaans worden een aantal sleutelaanvragen verzameld en periodiek in de RBC geïmplementeerd.

De aanvrager krijgt een terugmelding van de datum waarop de aangevraagde sleutels in de RBC geïmplementeerd zijn.

6.4 Contactgegevens KMC ProRail

ProRail Key Management Center

Afdeling Treinbeveiligingssystemen

Postbus 2038

3500 GA Utrecht

E-mail: kmc@prorail.nl

7 Beheervoorwaarden

7.1 ProRail levert sleutels aan de aanvrager

- Het KMC beheert de Masterdatabase met KMAC-sleutels voor de Nederlandse RBC's. Deze database is leidend voor alle (uitgegeven) sleutels.
- Het KMC levert sleutels aan de aanvrager in een technisch formaat zoals beschreven in [2]
- Het KMC bewaart kopieën van de laatste en voorlaatst geleverde sleutels die aan de aanvrager worden aangeboden om de versies te vervangen die op een bepaald moment door de aanvrager actief worden gebruikt.
- Indien een KMAC sleutel van de aanvrager, of de K-KMC transportsleutel die is overeengekomen tussen het KMC en de aanvrager, onverhoopt toch openbaar wordt, of dreigt te worden, zal het KMC daar de aanvrager binnen één werkdag nadat dat is vastgesteld, over informeren.

7.2 De aanvrager implementeert sleutels in de trein

- De aanvrager is niet bevoegd om een door ProRail opgeleverd bestand met sleutels inhoudelijk te wijzigen; indien een bestand misvormt blijkt, dan dient de aanvrager aan het KMC een nieuwe kopie van de betreffende bestand met geleverde sleutels (of van een door het KMC gewijzigd bestand) te vragen.
- Indien een KMAC sleutel van de aanvrager, of de K-KMC transportsleutel die is overeengekomen tussen het KMC en de aanvrager, onverhoopt toch openbaar wordt, of dreigt te worden, zal de aanvrager het KMC daar binnen één werkdag nadat dat is vastgesteld, schriftelijk over informeren.

7.3 Het gebruik van de K-KMC transportsleutel

- Het KMC en de aanvrager komen een 'Transportsleutel' (de zg 'K-KMC' sleutel) overeen waarmee sleutels bedoeld om de communicatie trein-wal te beschermen (de zg 'KMAC' sleutels) tijdens transport worden versleuteld.
- In beginsel genereert het KMC de K-KMC transportsleutel en levert de K-KMC op veilige wijze aan de aanvrager. Andere mogelijkheden om een K-KMC te genereren en uit te wisselen zijn bespreekbaar.
- Het KMC codeert iedere KMAC key voor transport vanuit het KMC aan de aanvrager met behulp van de Transportsleutel "K-KMC", die tussen het KMC en de aanvrager is afgesproken.
- Zowel het KMC als de aanvrager dragen er zorg voor dat de transportsleutel K-KMC niet in handen van onbevoegden kan komen. Mocht dat onverhoopt toch gebeuren, dan zal de partij die dat als eerste ontdekt de andere partij daar binnen één werkdag schriftelijk over informeren en kan besloten worden een nieuwe K-KMC sleutel te gaan gebruiken. Ook dient besloten te worden of alle KMAC sleutels die met de K-KMC waren beveiligd die openbaar is geworden, moeten worden vervangen door nieuwe sleutels.

7.4 Uitvoeren van testen

- Voorafgaand aan een eerste uitwisseling tussen KMC en aanvrager moeten testen worden uitgevoerd om de succesvolle uitwisseling en verwerking van de sleutels te toetsen. Beide partijen werken hieraan mee.

7.5 Beveiligingsmaatregelen

- Zowel het KMC als ook de aanvrager zal zodanig worden beveiligd dat gevoelige informatie niet toegankelijk is voor onbevoegden:
 - Sleutels (KMAC en K-KMC) dienen niet opgeslagen of getransporteerd te worden in ongecodeerde of triviaal versleutelde vorm tenzij dit vooraf geautoriseerd is door zowel KMC als aanvrager.
 - Sleutels (KMAC en K-KMC) in ongecodeerde of triviaal versleutelde vorm dienen beschermd te worden tegen ongeautoriseerde toegang.
 - Sleutels (KMAC en K-KMC) zijn onderhevig aan bovenstaande regels gedurende de gehele levensduur van de sleutel.
- In situaties waarin sleutels openbaar toegankelijk zijn geworden waardoor de veiligheid van het treinverkeer in het geding is, dient een noodprocedure te worden gevolgd met als doel misbruik te voorkomen door bestaande sleutels in RBC en treinen of te vervangen.
- Afhankelijk van de verwachte impact voor de spoorwegonderneming (“stilleggen van treinverkeer”) enerzijds en de veiligheid van treinen en infra anderzijds, dient het besluit om de noodprocedure van kracht te verklaren bij ProRail en aanvrager te worden genomen op het juiste managementniveau.
- Het verwerken van sleutels zal bij zowel KMC als de aanvrager uitsluitend gebeuren door geautoriseerd personeel.
- Zowel het KMC als de aanvrager leggen iedere activiteit die zij uitvoeren in het kader van het genereren, uitwisselen en verwijderen van sleutels vast in een logboek waarbij ten minste de volgende aspecten worden vastgelegd:
 1. datum
 2. persoon die de handeling verricht
 3. aard van handeling
 4. relevante bijzonderheden indien van normale procedures wordt afgeweken
- Zowel bij het KMC als bij de aanvrager kunnen audits worden uitgevoerd door ProRail of de aanvrager ter controle van de veiligheidsmaatregelen. Beide partijen werken hier volledig aan mee.