(1) Einleitung

Um Fahrzeugen Fahrten im ETCS Level 2 zu ermöglichen, müssen ETCS-Fahrzeuggeräte (OBU) und ETCS-Zentralen (RBC) verschlüsselt kommunizieren können. Hierzu werden entsprechende kryptografische Schlüssel (KMAC) sowie eine eindeutige ETCS-Kennung (NID-ENGINE) des Fahrzeugs benötigt, die auf der OBU und auf dem RBC installiert werden müssen. Die DB InfraGO AG betreibt hierzu ein Key Management Center (KMC DB) bei dem EVU-Unternehmen die Schlüssel für DB InfraGO AG Strecken beantragen können. Für den Datenaustausch mit dem KMC DB ist die E-Mail-Adresse

DB.KMC.ETCS@deutschebahn.com

zu verwenden.

Unter einem Key Management Center (KMC) versteht man eine technische Datenbank, die geeignet ist, alle funktionalen und kryptografischen Anforderungen des UNISIG SUBSET-038 (aus Beschluss der Kommission vom 27.05.2016 (2016/919/EU) zur Änderung des Beschlusses 2012/696/EU über die Technische Spezifikation für die Interoperabilität der Teilsysteme „Zugsteuerung, Zugsicherung und Signalgebung“ des transeuropäischen Eisenbahnsystems) sowie der dort genannten normativen Referenzen, zu erfüllen. Daraus folgt, dass das KMC insbesondere folgenden weiteren Anforderungen genügen muss:

- UNISIG EURORADIO FIS Subset-037 (aus Beschluss 2016/919/EU)
- ANSI X9.52 – 1998 Triple Data Encryption Algorithm Modes of Operation
- ANSI X3.92 – 1981 Data Encryption Standard (DES) Algorithm

Sofern das KMC die Spezifikationen der ETCS Baseline 3 Release 2 und GSM-R Baseline 1 erfüllt, ist auch

- UNISIG Online Key Management FFFIS Subset-137 (aus Beschluss 2016/919/EU)

erforderlich.

Das KMC dient der sicheren Aufbewahrung und Verwaltung der an das Eisenbahnverkehrsunternehmen (EVU) übergebenen Fahrzeugschlüssel, so dass diese im Bedarfsfall (zum Beispiel nach Wartungsarbeiten) wieder im Fahrzeug installiert werden können, sowie der standardisierten Kommunikation mit anderen KMCs über eine festgelegte E-Mail Adresse bzw. über die Onlineschnittstelle gemäß Subset-137.

Unter EVU wird in diesem Anhang auch ein Fahrzeughalter ohne Zulassung als EVU verstanden, da er bezüglich der Inhalte dieses Anhangs gleichgestellt ist.

Steht dem EVU kein eigenes KMC zur Verfügung, kann dieses seine Fahrzeuge über ein KMC Dritter verwalten lassen. In diesem Fall muss dieses KMC bei dem KMC DB registriert werden. Es besteht ebenfalls die Möglichkeit die Verwaltung der Fahrzeuge gegen Entgelt durch die DB InfraGO AG durchführen zu lassen, siehe hierzu Kapitel 4 - Ablauf „Verwaltung von ETCS-Fahrzeuggeräten“. Dabei muss das beauftragte KMC die Offlineschnittstelle nach Subset-038 unterstützen. Das Onlineverfahren zum Schlüsselaustausch kann alternativ verwendet werden, wenn dies von allen beteiligten KMC unterstützt wird, eine Public Key Infrastructure (PKI) gegeben ist und diese den Vorgaben des Subset-137 entspricht.
Damit die DB InfraGO AG ETCS-Störfälle analysieren und bewerten kann, sind neben den streckenseitigen technischen Daten ggf. auch Fahrzeugdaten notwendig. Diese werden dann entspre-

chend §12 durch die DB InfraGO AG angefordert. Die DB InfraGO AG wird ihrerseits ebenfalls Infrastrukturdaten zur Analyse von Fahrzeugstörungen entsprechend §13 bereitstellen.
Die Mitwirkung aller Beteiligten ist in solchen Fällen unbedingt erforderlich.
Die entsprechenden Verfahrensweisen werden in diesem Anhang festgelegt und dienen dem geregelten Austausch der Informationen zwischen den EVU und dem Infrastrukturbetreiber.

(2) Ablauf „KMC registrieren“

Mit dem Antrag „KMC registrieren“ kann ein EVU oder ein Infrastrukturbetreiber (EIU) sein KMC beim KMC DB registrieren. Nur wenn dies erfolgt ist, können Schlüssel für die Kommunikation zwischen OBUs und RBCs der DB InfraGO AG beantragt werden.

In diesem Antrag sind die Daten des KMC wie Name und E-Mail-Adresse sowie die Daten des Antragstellers anzugeben. Alle folgenden Schlüsselanträge müssen dem hier angegebenen KMC zugeordnet werden und werden nur von der angegebenen E-Mail-Adresse akzeptiert. Für die Kommunikation bzw. den Austausch der Subset-038 Nachrichten zwischen dem KMC DB und dem KMC des Kunden wird ein kryptografischer Schlüssel (K-KMC) benötigt. Dieser wird mit der Antragsbearbeitung generiert und verteilt. Dieser Schlüssel darf nicht unverschlüsselt versendet werden und muss sicher auf dem KMC des Kunden gespeichert werden (weitere Informationen siehe Kapitel 4).

Wird das Onlineverfahren verwendet, so sind Angaben zur genutzten Certificate Authority (CA) und der Adressierung des KMC anzugeben.

Der Antrag ist an die im Abschnitt 1 genannte E-Mail-Adresse zu senden. Die Anträge werden in der Reihenfolge des Eingangs bearbeitet. Die DB InfraGO AG verpflichtet sich den Antrag innerhalb von 4 Wochen zu bearbeiten.

(3) Verteilung der Schlüssel (K-KMC)

Bei Verwendung des Offlineverfahrens dürfen die K-KMC nicht unverschlüsselt verteilt werden. Zur Verteilung der K-KMC wird openSSL eingesetzt. Beide Teilnehmer generieren hierzu mit openSSL einen privaten und einen öffentlichen Schlüssel und senden den öffentlichen Schlüssel dem Kommunikationspartner zu. Der K-KMC wird mit diesem Schlüssel verschlüsselt und ausschließlich an die KMC-E-Mail-Adresse gesendet. Der K-KMC kann nur mit dem privaten Schlüssel wieder entschlüsselt werden.

Steht eine asymmetrische E-Mail-Verschlüsselung (z.B. PGP) zur Verfügung, kann auch diese verwendet werden.

Das zu verwendende Verfahren ist mit der DB InfraGO AG abzustimmen.
Wird die Onlineschnittstelle genutzt, so dürfen die genutzten Schnittstellenzertifikate eine Gültigkeit von 4 Jahren nicht überschreiten.

(4) Ablauf „Verwaltung von ETCS-Fahrzeuggeräten“

Die DB InfraGO AG bietet die Verwaltung von kryptografischen ETCS-Schlüsseln in Form eines Key Management Center gemäß INB Ziffer 5.5.8 an, wenn das EVU kein eigenes KMC besitzt. Dieser Service wird aktuell nur mit der Offlineschnittstelle realisiert.

Um OBUs bei der DB InfraGO AG zu registrieren, kann, nach der Beauftragung, der Antrag „OBU zuweisen“ verwendet werden. Sobald diese Zuweisung erfolgt ist, können die gewünschten Schlüssel beantragt werden.

Für weitere Informationen wenden Sie sich bitte an DB.KMC.ETCS@deutschebahn.com.

(5) Ablauf „Schlüssel beantragen“

Ist das KMC des Kunden registriert, können Schlüssel für die Kommunikation zwischen OBU und RBC über den Antrag „Schlüssel beantragen“ beantragt werden. Sollen für eine Strecke mehrere Fahrzeuge eingetragen werden, so kann im Antrag eine Liste der OBUs eingetragen werden. Zusätzlich sind die Strecken, auf der die OBU fahren sollen, sowie die gewünschte Gültigkeitsdauer anzugeben. Es werden ausschließlich Schlüssel für DB InfraGO AG Strecken generiert und ausgestellt.

Sofern die DB InfraGO AG nicht mit der Führung des KMCs durch das EVU beauftragt wurde, müssen Schlüssel für Strecken von anderen EIUs im Ausland direkt dort beantragt werden. Die notwendigen Schritte zum Austausch der Schlüssel sind bilateral zu vereinbaren und liegen außerhalb des Zuständigkeitsbereichs der DB InfraGO AG.

Werden die OBUs von der DB InfraGO AG verwaltet, werden die Schlüsselanträge an die jeweiligen KMCs weitergeleitet. Liegt eine Strecke dabei außerhalb des DB InfraGO AG-Bereichs, sind mit dem Antrag die betroffenen Länder anzugeben.

Sind die RBCs bekannt, können diese zusätzlich zur Strecke eingetragen werden. Sind diese nicht bekannt, ermittelt das KMC DB die notwendigen RBCs aus den Streckenangaben und erstellt die entsprechenden Schlüssel.

Die Gültigkeitsdauer eines Schlüssels ist im Antrag anzugeben, darf jedoch nicht länger als 5 Jahre sein. Wird ein längerer Zeitraum angegeben wird die Gültigkeitsdauer auf 5 Jahre reduziert. Wird kein Zeitraum angegeben, beginnt die Gültigkeitsdauer von 5 Jahren mit dem Ausstellen des Schlüssels.

Läuft die Gültigkeitsdauer ab, muss der Kunde rechtzeitig einen neuen Schlüssel beantragen. Der Schlüssel wird nicht automatisch ersetzt.
Der Antrag ist an die o.g. E-Mail-Adresse zu senden. Die Anträge werden in der Reihenfolge des Eingangs bearbeitet. Die DB InfraGO AG verpflichtet sich die beantragten Schlüssel innerhalb von 8 Wochen zur Verfügung zu stellen.

Ist ein Schlüssel an die KMC E-Mail-Adresse des Kunden im Offlineverfahren gesendet worden, ist der Empfang innerhalb 1 Woche durch den Kunden über die KMC E-Mail-Adresse zu bestätigen, wenn möglich mit einer Subset-konformen „Confirmation Message“. Liegt nach einer Woche keine Bestätigung vor, wird der Schlüssel automatisch zurückgezogen und kann nicht mehr verwendet werden. In diesem Fall wird der Antragsteller über diesen Vorgang via E-Mail informiert.
Werden die Schlüssel online übertragen, so erfolgt die Quitierung unmittelbar entsprechend der Schnittstellenspezifikation.

(6) Ablauf „Schlüssel zurückziehen“

Soll ein Schlüssel zurückgezogen werden, ist die entsprechende Subset-Nachricht („Delete Key Request“) an die o.g. E-Mail-Adresse zu senden. Das KMC DB löscht daraufhin unwiderruflich den Schlüssel im RBC und im KMC und sendet die Subset konforme „Confirmation Message“.
Bei der Nutzung der Onlineschnittstelle wird die entsprechende Quittung unmittelbar gesendet.

(7) Ablauf „OBU löschen“

Sofern das DB KMC als EVU KMC fungiert, kann das EVU auch die Löschung einer ganzen OBU mit dem Antrag “OBU löschen” beantragen. Dabei werden dann alle vergebenen Schlüssel gelöscht und die OBU sebst aus der Datenbank entfernt. Wurden Schlüssel von ausländischen EIUs bereitgestellt, werden diese umgehend informiert, dass die Schlüssel nicht weiter verwendet werden. Soll eine solche OBU später wieder in Betrieb genommen werden, wird diese wie ein Neufahrzeug behandelt (siehe Ablauf 4).

(8) Datensicherheit beim Kunden

Nach Erhalt der Schlüssel auf dem KMC ist jeder Zugangsberechtigte des Kunden verpflichtet, die Datensicherheit durch Sicherstellen der ausschließlichen Nutzung nur durch befugte Mitarbeiter zu gewährleisten. Schlüssel dürfen nur als Anhang zwischen den bekannten KMC-E-Mails verteilt und, außer zur OBU bzw. zum RBC, nicht weitergeleitet und nicht in Kopie gesendet werden.

Das EVU bzw. EIU bestätigt, dass das gewählte KMC die folgenden Anforderungen zugesichert hat:

- Unverschlüsselte Schlüssel werden nur von einer begrenzten Anzahl (in der Regel < 5) vertrauenswürdiger Personen bearbeitet.
- Diese vertrauenswürdigen Personen müssen innerhalb ihrer Organisation explizit benannt werden.
- Die Bearbeitung von Schlüsseln muss unter Nennung des Bearbeiters dokumentiert werden.
- Nicht autorisierter Zugang zu Schlüsseln muss durch geeignete Betriebsprozesse und technische Umgebungen verhindert werden.
- Außerhalb der geschützten Umgebung müssen die Schlüssel mit Verfahren verschlüsselt werden, die mindestens vergleichbar mit der 3DES Verschlüsselung der KMC-KMC-Kommunikation sind.
- Alle Schlüssel müssen auf ausfallsicheren elektronischen Speichermedien abgelegt werden, die kryptografische gesichert sind. Die dazu verwendeten Verfahren müssen dem aktuellen Stand der Verschlüsselungstechnik entsprechen.
- Wird die Onlineschnittstelle nach Subset-137 verwendet, so ist eine PKI mit den dort definierten Verfahren und Standards zu verwenden.

Der Kunde verpflichtet sich den Verlust oder die Kompromittierung eines Schlüssels umgehend an die o.g. E-Mail Adresse zu melden und den Schlüssel zurückziehen zu lassen. Der Schlüssel ist umgehend und unwiderruflich auf der OBU zu löschen. Die DB InfraGO AG zieht nach

Meldungseingang umgehend den Schlüssel zurück und fordert den Kunden auf, die Einhaltung der oben genannten Vorgaben zu überprüfen.

Meldet ein Kunde mehrfach den Verlust von Schlüsselmaterial oder zeigt mehrfach die Kompromittierung von Schlüsseln an, so geht die DB InfraGO AG davon aus, dass die oben genannten Vorgaben nicht eingehalten werden. Der Kunde wird dann aufgefordert, einen Audit zur Schwachstellenanalyse durch die DB InfraGO AG oder durch ein anderes zertifiziertes Unternehmen für den Security Bereich durchführen zu lassen, um diese Abweichungen aufzudecken und zu beseitigen. Einsteht durch den Verlust oder die Kompromittierung des Schlüssels eine unmitterlbare Gefahr für den Betriebsablauf auf dem Streckennetz der DB InfraGO AG, so ist diese, auch ohne Zustimmung bzw. Information des betroffenen EVU, berechtigt, alle notwendigen Maßnahmen zur Gefahrenabwehr zu ergreifen. Eine Gefahr entsteht dann, wenn ein Schlüssel nicht autorisierten Dritten bekannt ist und damit dann dieser Dritte auf die ETCS-Führung des Fahrzeuges, für das der Schlüssel bereitgestellt wurde, Einfluss nehmen kann. Befindet sich das so gefährdete Fahrzeug in Einsatz, so wird von einer unmittelbaren Betriebsgefahr ausgegangen. Die Betriebsführung der DB InfraGO AG wird dieses Fahrzeug sofort zum Halten bringen oder an der Weiterfahrt hindern.

Befindet sich das Fahrzeug noch nicht in Benutzung, so wird über die Betriebsführung der DB InfraGO AG eine Betriebsaufnahme innerhalb der DB Infrastruktur verweigert (keine Fahrerlaubnis durch Fahrdienstleitung oder ETCS-Zentrale) oder die Überführung des Fahrzeuges in die DB Infrastruktur wird verwehrt. In solch einem Fall erfolgt dann auch eine unmittelbare Information des EVUs über die Gründe der verwehrten Betriebsaufnahme.

Neben diesen betrieblichen Maßnahmen kann auch durch die Löschung der betroffenen Schlüssel auf den RBCs eine Betriebsaufnahme technisch verhindert werden.

(9)Zuweisung der ETCS-Kennung (NID-ENGINE)

Jede OBU benötigt eine eindeutige ETCS-Kennung (NID-ENGINE), die nur einmal vergeben werden darf. Diese wird bei der Anmeldung an den RBC als Identifikation des Fahrzeugs verwendet. Für die Beschaffung dieser Identifikation ist das EVU des Fahrzeugs verantwortlich. Im Regelfall wird der Hersteller der OBU oder des Fahrzeugs die ETCS-Kennung aus dem zugewiesenen Nummernbereich entnehmen und diese dann mit der OBU bzw. dem Fahrzeug an das EVU übergeben.

Falls dem Hersteller kein eigener Nummernbereich zugewiesen wurde oder dieser bereits vollständig vergeben wurde oder andere Gründe eine Zuweisung nicht zulassen, kann ein EVU mit Hauptsitz in der Bundesrepublik Deutschland eine Zuweisung einer ETCS-Kennung durch die DB InfraGO AG beantragen. Dazu ist ein begründeter Antrag zu richten an: DB.KMC.ETCS@deutschebahn.com

Sofern das EVU die Notwendigkeit einer Vergabe der ETCS-Kennung durch die DB InfraGO AG plausibel machen kann, wird dem EVU die benötigte Kennung innerhalb eines Monats nach Beantragung zugewiesen. Das EVU ist verpflichtet alle für die Vergabe und Verwaltung der ETCS-Kennungen notwendigen Daten des jeweiligen Fahrzeugs der DB InfraGO AG mitzuteilen. Die zugewiesene Kennung darf nur auf der entsprechenden OBU verwendet werden.

Missbräuchliche Verwendung der Kennungen, insbesondere Mehrfachverwendung, Verwendung auf anderen Fahrzeugen oder OBU als hinterlegt oder Weitergabe an Dritte, sind durch das nutzende EVU zu verhindern.

Die DB InfraGO AG ist berechtigt im Falle eines solchen Missbrauch die ETCS-Kennung zurück zu ziehen oder allen betroffenen Fahrzeugen die Nutzung ihrer Infrastruktur zu untersagen.

Spätestens nach 12 Monaten muss das EVU eine erteilte Inbetriebnahmegenehmigung in einem Mitgliedsstaat der EU als Nachweis der realen Verwendung der ETCS-Kennung vorlegen oder die ETCS-Kennung zurückgeben. Dazu kann ein formloser elektronischer Nachweis per E-Mail an DB.KMC.ETCS@deutschebahn.com gesandt werden.

(10) Verpflichtungen des EVU zum Schlüsselmanagement

Die verteilten Schlüssel dienen zur kryptographischen Verschlüsselung zwischen RBC und EVC und schützen vor allem vor einen unberechtigten Zugriff Dritter auf die Kommunikation. Es wird hierüber nicht geregelt, ob ein Fahrzeug bezüglich seines Zulassungsstands, Eignung und Berechtigung usw. zum sicheren Befahren einer bestimmten Strecke geeignet ist. Dies zu bewerten und im Bedarfsfall sicherzustellen, fällt in die Verantwortung des EVU.

Deshalb sind kryptographischen Schlüssel, welche von der DB InfraGO AG erstellt und verteilt wurden, nur in Fahrzeugen uneingeschränkt nutzbar, die eine Streckenzulassung für ETCS in Deutschland besitzen.

Wurden die Schlüssel vom EVU für Fahrzeuge ohne entsprechende Streckenzulassung für ETCS im Zuständigkeitsbereich der DB InfraGO AG beantragt, so ist folgendes zu beachten:

- Bei eingelegten ETCS SIM-Karten ist die Nutzung von ETCS (mit Ausnahme von Test-, Versuchs-, oder Erprobungsfahrten) technisch zu unterbinden.
- Die Aktivierung für den Betrieb unter ETCS darf erst zeitnah vor Aufnahme der Test-, Versuchs-, oder Erprobungsfahrten bzw. mit Erteilung der ETCS-Zulassung erfolgen. Ist dies nicht umsetzbar bzw. der zeitliche Vorlauf nicht einschränkbar, muss der Tf gesondert darüber informiert werden, dass mit dem Tfz keine in Betrieb befindlichen ETCS Strecken der DB InfraGO AG befahren/gekreuzt werden dürfen, für die bereits Schlüssel ausgehändigt wurden.
- Das EVU ist für die Handlungssicherheit des Tf für den Fall eines unvorhergesehenen Wechsels (Anbieten einer Betriebsart) nach ETCS verantwortlich. Er darf einen Wechsel nach ETCS Level 0, 1, 2 und 3 auf dem DMI nicht bestätigen und muss das Tfz gefahrenfrei unmittelbar zum Halten bringen. Danach setzt er sich unverzüglich mit dem Fdl in Verbindung.
- Auf Fahrzeugen, auf denen Schlüssel nur für Test- oder Zulassungsfahrten aktiviert wurden, sind diese nach den Fahrten bis zum Erhalt der letztendlichen Zulassung für ETCS in Deutschland zu löschen. Alternativ oder zusätzlich kann für ein solches Fahrzeug der Wechsel in die ETCS Überwachung mittels Software- oder Hardwaresperren verhindert werden.

Mit dem Erhalt der ETCS Schlüssel werden diese Verpflichtungen des EVU anerkannt.

(11) Haftung

1) Die DB InfraGO AG haftet unbeschränkt für Vorsatz und grober Fahrlässigkeit.

2) Für einfache Fahrlässigkeit haftet die DB InfraGO AG - außer im Falle der Verletzung des Lebens, des Körpers oder der Gesundheit - nur, sofern wesentliche Pflichten aus den Bestimmungen dieses Anhanges (Kardinalpflichten) verletzt werden. Die Haftung ist begrenzt auf den vertragstypischen und vorhersehbaren Schaden.

3) Die Haftung für mittelbare und unvorhersehbare Schäden, Produktions- und Nutzungsausfall, entgangenen Gewinn, ausgebliebene Einsparungen und Vermögensschäden wegen Ansprüchen Dritter, ist im Falle einfacher Fahrlässigkeit - außer im Falle der Verletzung des Lebens, des Körpers oder der Gesundheit - ausgeschlossen.

4) Eine weitergehende Haftung als in den Bestimmungen dieses Anhanges sind - ohne Rücksicht auf die Rechtsnatur des geltend gemachten Anspruchs - ausgeschlossen. Vorstehende Haftungsbeschränkungen bzw. -ausschlüsse gelten jedoch nicht für eine gesetzlich zwingend vorgeschriebene verschuldensabhängige Haftung oder die Haftung aus einer verschuldensabhängigen Garantie.

5) Soweit die Haftung nach Ziffern 2 und 3 ausgeschlossen oder beschränkt ist, gilt dies auch für die persönliche Haftung der Angestellten, Vertreter, Organe und Erfüllungsgehilfen der DB InfraGO AG.

6) Das EVU haftet nach § 278 BGB für Schäden, die von ihm im Rahmen der Schlüsselverwaltung (Home-KMC) eingesetzte Auftragnehmer verursachen.

(12) Allgemeine Mitwirkungsverpflichtung des EVU (gültig für alle ETCS-Level)

ETCS als Zugbeeinflussungssystem besteht aus verschiedenen Komponenten, deren komplexes Zusammenwirken erst den Eisenbahnbetrieb ermöglicht. Hierzu ist auch die korrekte Funktion von Komponenten erforderlich, auf die die DB InfraGO AG als Infrastrukturbetreiber keinen direkten Einfluss hat. Hierbei sind im Wesentlichen alle ETCS-Anteile auf den Fahrzeugen der Eisenbahnverkehrsunternehmen gemeint.

Treten Beeinflussungen im Bahnbetrieb (z. B. Störungen auf den Tfz) auf, so ist das EIU verpflichtet deren Ursache zu analysieren, deren Sicherheitsrelevanz für den Eisenbahnbetrieb zu bewerten und ggf. alle notwendigen Maßnahmen zu ergreifen, um Gefahren abzuwenden und den sicheren Eisenbahnbetrieb weiter zu gewährleisten.

Werden zur Analyse Informationen der beteiligten EVU oder technische Daten aus den beteiligten Fahrzeugen (insbesondere JRU-Daten oder andere fahrzeugspezifische Fehleranalysedaten) benötigt, so sind die EVU verpflichtet, diese an die DB InfraGO AG zu übergeben und bei der Fehleranalyse mitzuwirken, damit die Analyse und Ermittlung der Ursachen der Störung erfolgen kann. Hierzu benennt das EVU auf Nachfrage ggü. der ETCS Bauartverantwortung der DB InfraGO AG einen fachlich kompetenten Ansprechpartner und stellt dessen Kontaktdaten zur Verfügung.

Diese Verpflichtungen gelten nicht nur bei sicherheitsrelevanten Vorfällen, sondern auch bei Vorfällen, die die Verfügbarkeit der Strecke einschränken oder den Bahnbetrieb behindern. Des Weiteren gelten die Verpflichtungen auch dann, wenn es sich bei dem eingesetzten Tfz um ein seitens des EVU angemietetes Fahrzeug handelt.

Die Daten müssen in elektronisch lesbarer Form innerhalb von 15 Werktagen nach der Anforderung durch die zuständige Bauartverantwortung ETCS unter Angabe des entsprechenden Störfalles bereitgestellt werden. Sofern erforderlich, muss auch eine Hilfestellung bei der Interpretation der Da-

ten durch das EVU bzw. den Fahrzeughersteller erfolgen. Alle Informationen sind an folgende Adresse zu übermitteln:

ETCS-Monitoring@deutschebahn.com

Sofern die Datenmenge einen Transfer per E-Mail nicht zulässt, wird eine andere individuelle Austauschmethode (z. B. ftp) zwischen dem EVU und der DB InfraGO AG vereinbart.

Die DB InfraGO AG verpflichtet sich, alle Informationen vertraulich zu behandeln und diese nur im Rahmen der Störungsanalyse zu verwenden. Müssen Informationen an Dritte (z. B Infrastrukturhersteller) weitergegeben werden, so wird zuvor das EVU informiert und für den jeweiligen Störfall dessen Einwilligung eingeholt.

Den genauen Verfahrensablauf kann dem Ablaufdiagramm unter (17) entnommen werden.

(13) Allgemeine Mitwirkungsverpflichtung der DB InfraGO AG (gültig für alle ETCS-Level)

Sofern ein EVU zur Störungsanalyse auf seinen Fahrzeugen Daten der Infrastrukturkomponenten der DB InfraGO AG benötigt, so können diese über die Adresse der Bauartverantwortung ETCS

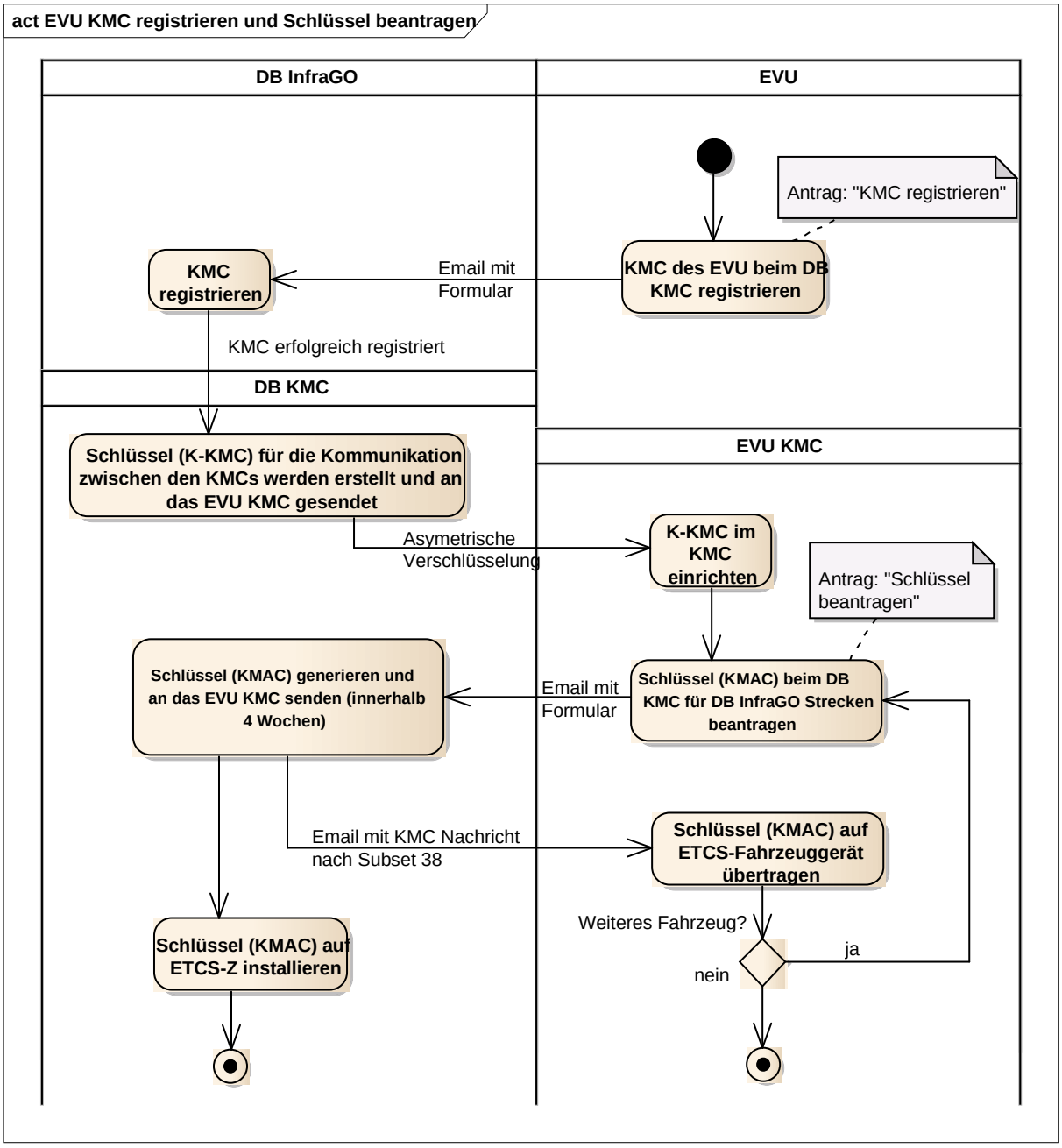
ETCS-Monitoring@deutschebahn.com

unter Angabe von Zeitpunkt und Ort der Betriebsbeeinflussung, sowie der Fahrzeugidentifikation (ETCS-ID, MSISDN der beiden EDOR) angefordert werden. Für Daten aus einer ETCS-Zentrale muss diese ebenfalls mit angegeben werden. Die DB InfraGO AG kann ERTMS-Tracedaten sowie interne Tracedaten der ETCS-Zentralen bereitstellen. Die Interpretationstiefe der Daten sowie deren Umfang ist abhängig vom Hersteller der ETCS-Zentrale und kann sich daher unterscheiden. Hilfestellung zur Interpretation der Informationen können durch die DB InfraGO AG nur im Umfang der Instandhaltungsschulungen des jeweiligen Herstellers geben.

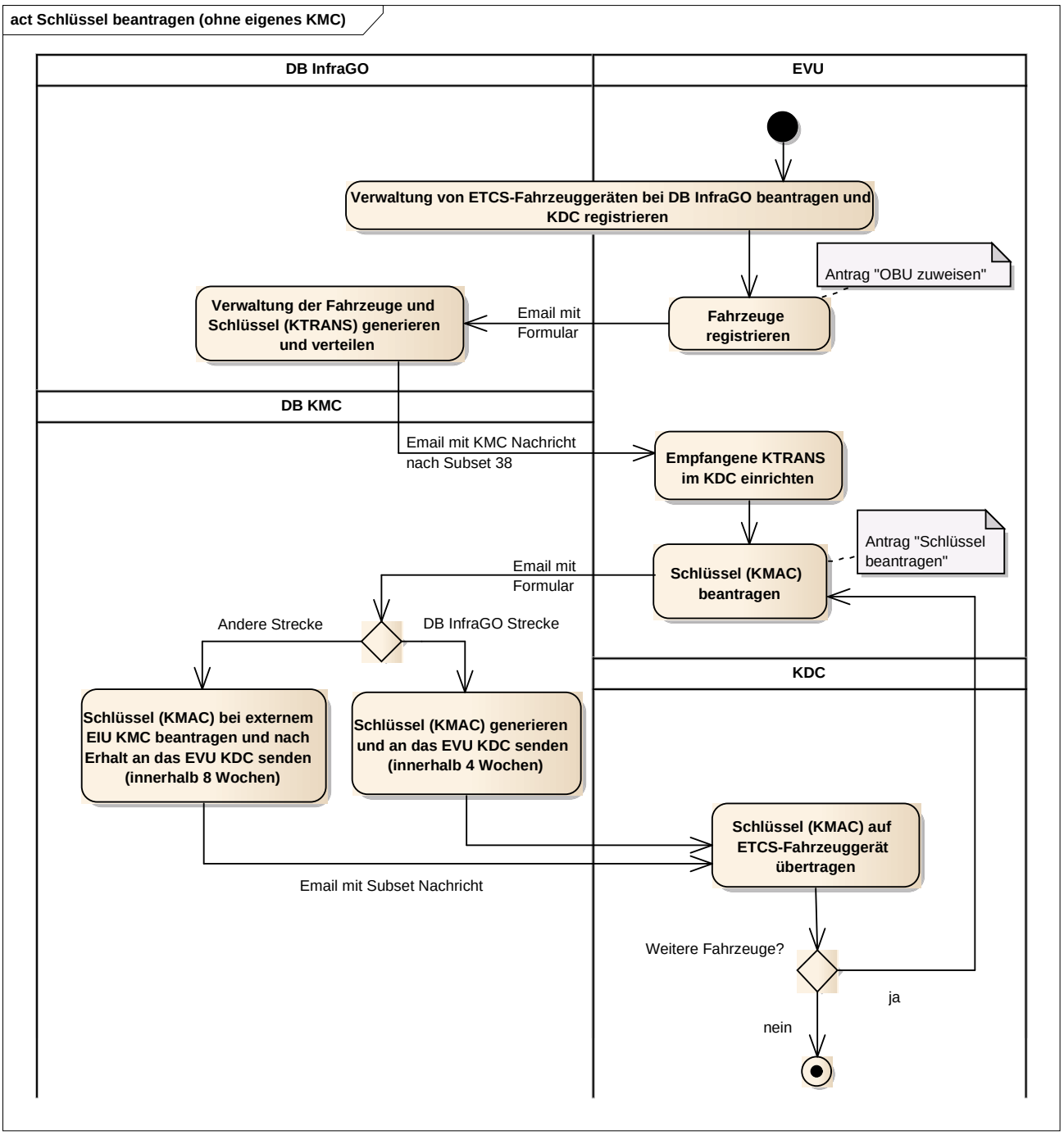
Die gelieferten Daten sind vertraulich zu behandeln, dürfen an keinen Dritten weitergegeben werden und sind nur im Rahmen der Störungsanalyse zu verwenden.

Die Bauartverantwortung ETCS wird die Anfragen innerhalb von 15 Werktagen beantworten und die angeforderten Daten in elektronischer Form bereitstellen.

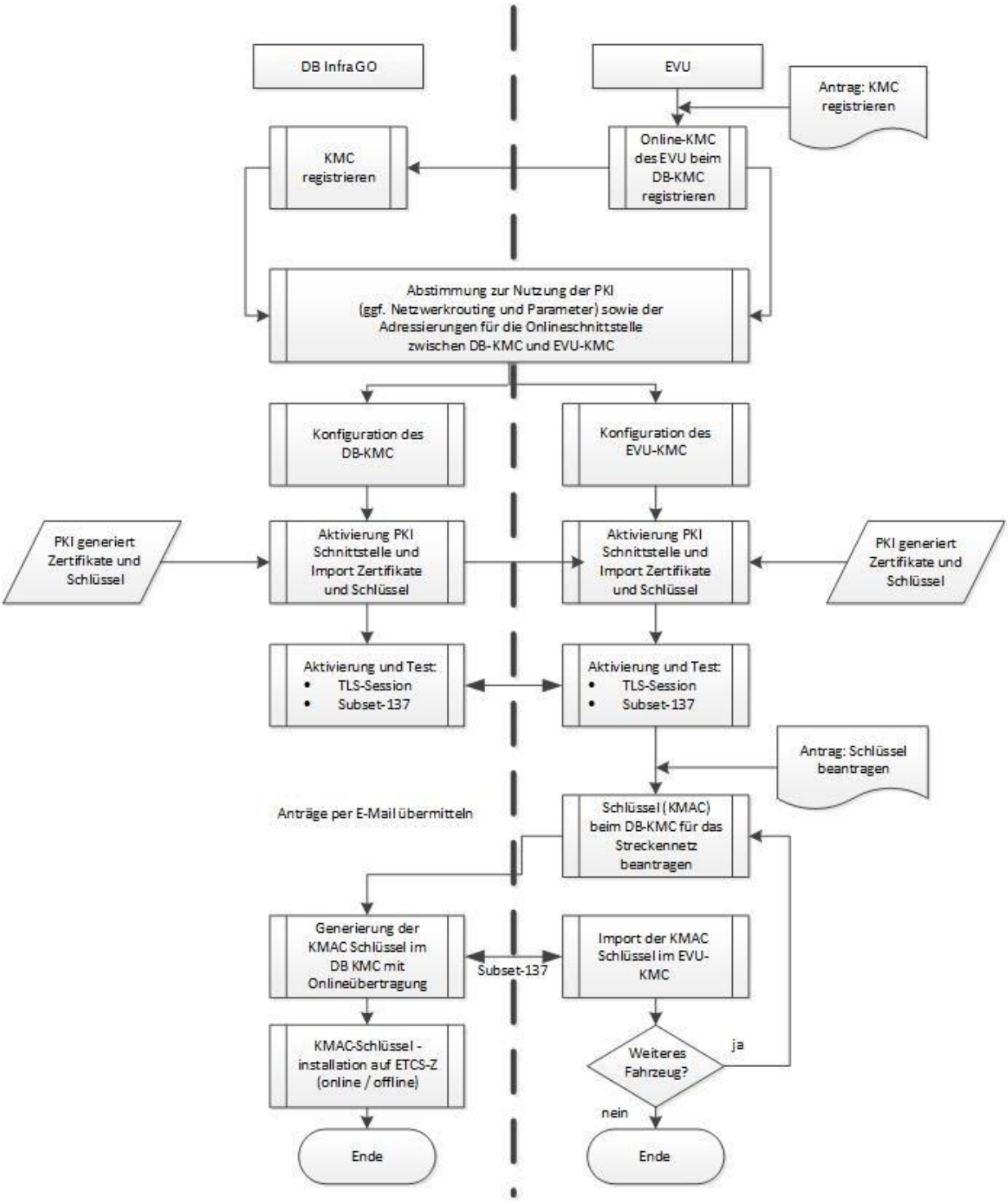
(14) Ablauf 1: EVU registriert eigenes KMC bei der DB und beantragt Schlüssel für DB InfraGO AG Strecken (Offlineverfahren)



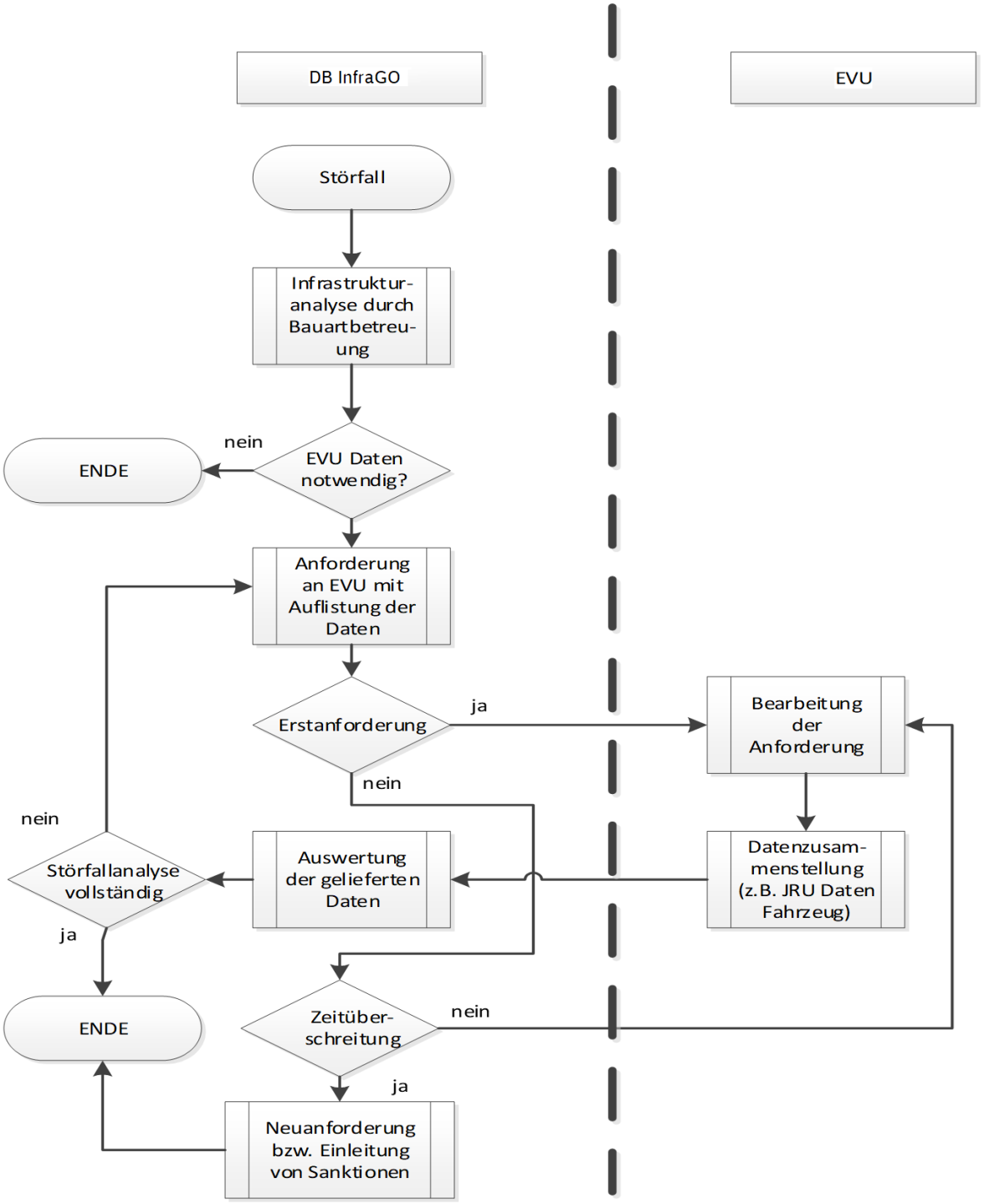
(15) Ablauf 2: EVU lässt seine Fahrzeuge von der DB InfraGO AG verwalten und beantragt Schlüssel für beliebige Strecken (Offlineverfahren)



(16) Ablauf 3: EVU registriert eigenes KMC bei der DB und beantragt Schlüssel für DB InfraGO AG Strecken (Onlineverfahren)



(17) Ablauf 4: Mitwirkungspflicht EVU: Lieferung von ETCS Fahrzeugdaten



Dokumentenübersicht

- **Anträge**
  - **„KMC registrieren“**
  - **„Schlüssel beantragen bzw. löschen“**
  - **„OBU zuweisen“**
  - **„OBU löschen“**
  - **„ETCS-Kennung beantragen“**

❑