

Geschäftseinheit I-AT-SAZ

Systemführerschaft ETCS CH

CKM Leitfaden

Version V1.0

Vom: 02.07.2018
Dokumenten-ID: L2_CH_Eng_12

	Erstellt	Q-geprüft	Freigegeben
Datum, Visum	02/07/18 	02/07/2018 	2.7.2018 
Name	Bettina Wilhelm	Alfred Essig	Frank Pulfer
Stelle / Funktion	System Engineer I-AT-SAZ	Qualitätsmanager I-AT-SAZ	Leiter Systemführerschaft ETCS CH

Dokumenten-Kontrollblatt

Inhalt	Das vorliegende Dokument beschreibt in Form eines Leitfadens für die Besteller von Schlüsseln die notwendigen Schritte aus Sicht Key Management, bevor Fahrzeuge auf ETCS Level 2 Strecken verkehren können.
Ersteller	Bettina Wilhelm
Wordprozessor	Microsoft Word 2016
Filename	18_CKM_Leitfaden_v10.docx
Status des Dokuments	In Bearbeitung / in Review / <u>Freigegeben</u>
Gelenktes Dokument	Nein
Verteiler	Systemführerschaft ETCS CH, BAV
Dokumenteigner	Systemführerschaft ETCS CH
Gültigkeit	Bis zum Vorliegen einer neueren Version dieses Dokuments oder Ausserkraftsetzung.
Sicherheit	Dieses Dokument muss nicht durch eine unabhängige Stelle begutachtet werden.
Periodische Überwachung	Prüfung des Dokuments auf Aktualität spätestens nach 5 Jahren.
Aufbewahrung/Archivierung	Elektronisch. Nach Vorliegen einer neuen Version oder Ausserkraftsetzung erfolgt Aufbewahrung > 5 Jahre; danach Archivierung bei Erfordernis.
Hinweis	<p>Das Originaldokument ist elektronisch gespeichert. Falls das Dokument in einer Papierversion benutzt wird, muss der Benutzer die Gültigkeit der aktuellen Dokumentversion überprüfen.</p> <p>Dieses Dokument wird in weitere Sprachen übersetzt. Bei inhaltlichen Zweifelsfällen gilt ausschliesslich das vorliegende, deutsche Originaldokument.</p>

Urheberrecht (Auszug aus Schutzvermerk ISO 16016)

Das Urheberrecht für das durch das BAV veröffentlichte Dokument der Systemführerschaft ETCS CH ist so zu verstehen, dass die Weitergabe und die Vervielfältigung ausdrücklich gestattet sind.

Aktualitätsprüfung

Nächste Prüfung:	Datum	Prüfer / Visum
Spätestens Juli 2023		

Änderungsnachweise

Version	Datum	Ersteller	Änderungshinweise
X0.1	20.06.18	B. Wilhelm	Erstellung des Dokuments
X0.2	28.06.18	B. Wilhelm	Einarbeiten der Review Kommentare gemäss rv_18_CKM_Leitfaden_x01_all.docx
V1.0	02.07.18	B. Wilhelm	Freigabe

Inhaltsverzeichnis

1	Einleitung	6
1.1	Hintergrund des Key Managements	6
1.2	Ziel des Dokuments	6
1.3	Abgrenzung	6
2	Allgemeine Aspekte	7
2.1	Termine und Ablauf	7
2.2	Auszutauschende Daten	7
2.2.1	Allgemein	7
2.2.2	UIC Nummer, Fahrzeugbezeichnung, Fahrzeugnummer	7
2.2.3	NID_ENGINE	7
2.2.4	Home KMC resp. KDC	8
2.2.5	Ausländisches KMC und Strecken	8
2.3	Schlüsselvergabe durch das KMC-CH	8
3	Schweizer Fahrzeuge auf Schweizer Strecken	9
4	Schweizer Fahrzeuge auf ausländischen Strecken	10
5	Ausländische Fahrzeuge auf Schweizer Strecken	11

Abbildungsverzeichnis

Abbildung 1: Schweizer Fahrzeuge auf Schweizer Strecken	9
Abbildung 2: Schweizer Fahrzeuge auf ausländischen Strecken	10
Abbildung 3: Ausländische Fahrzeuge auf Schweizer Strecken	11

Tabellenverzeichnis

Tabelle 1: Schlüsselupgrade: Termine und Ablauf	7
---	---

Referenzen

- [1] SBB: KMC-CH Security Policy; KMC_CH_Sec_Pol
- [2] SBB: Crypto Key Management (CKM), Vorgaben an Fahrzeuge und Strecken;
08_SF_CKM_Vorgaben_SF
- [3] SBB: List of all NID_ENGINE, NID_RBC und NID_KMC used in Switzerland;
ETCS_IDs_CH

Hinweis: Bei sämtlichen Referenzen sind keine Versionen angegeben. Es gilt jeweils die zum Zeitpunkt des Gebrauchs aktuelle Version.

Abkürzungen und Begriffe

BAV	Bundesamt für Verkehr
Besteller	Hier ist der Besteller von Schlüsseln beim KMC-CH gemeint. Je nach Fall kann es sich dabei um den Fahrzeughalter, den OBU Lieferanten oder ein ausländisches KMC handeln.
CKM	Crypto Key Management
Crypto Key	Alternative Bezeichnung für Schlüssel
ETCS	European Train Control System; europäisches Zugbeeinflussungssystem
Home KMC	Jede OBU (und jedes RBC) ist einem KMC, seinem Home-KMC, zugeordnet. Schlüsselupgrades dürfen nur über das Home-KMC erfolgen.
KDC	Key Distribution Center; Schlüsselverteilzentrum Ein KDC kann Meldungen und Schlüssel empfangen und versenden, jedoch keine Schlüssel generieren.
KMC	Key Management Center; Schlüsselverwaltungszentrum Ein KMC kann Meldungen und Schlüssel empfangen und versenden und auch Schlüssel generieren. Ausserdem kann ein KMC Home-KMC sein.
KMC-CH	Key Management Center Schweiz
NID_ENGINE	ETCS Variable, Identifikationsnummer einer OBU
OBU	On-Board Unit; ETCS Fahrzeugausrüstung
OBU ID	Umgangssprachliche Bezeichnung für die NID_ENGINE
RBC	Radio Block Center; Streckenzentrale
SBB	Schweizerische Bundesbahnen
SW	Software
UIC	Union Internationale des Chemins de Fer

1 Einleitung

1.1 Hintergrund des Key Managements

- 1.1.1.1 ETCS Level 2 verwendet Schlüssel, sog. „Crypto Keys“, zur Authentifizierung der Fahrzeuge (OBU) und Streckenzentralen (RBC) beim Verbindungsaufbau.
- 1.1.1.2 Da es sich bei diesen „Crypto Keys“ um symmetrische Schlüssel handelt, müssen sie vor Beginn des Betriebs mit ETCS Level 2 sowohl strecken- wie auch fahrzeugseitig installiert werden.
- 1.1.1.3 Als Key Management werden sämtliche Tätigkeiten im Zusammenhang mit den Schlüsseln bezeichnet.

1.2 Ziel des Dokuments

- 1.2.1.1 Dieses Dokument beschreibt in Form eines Leitfadens für die Besteller von Schlüsseln beim KMC-CH die notwendigen Schritte aus Sicht Key Management, bevor Fahrzeuge auf ETCS Level 2 Strecken verkehren können.
- 1.2.1.2 Besteller von Schlüsseln können je nach Situation sein:
 - Fahrzeughalter
 - OBU Lieferanten
 - Ausländische KMC
- 1.2.1.3 Kapitel 2 behandelt die allgemeinen Aspekte des Key Managements, während sich die nachfolgenden Kapitel den jeweiligen Prozessen widmen:
 - Schweizer Fahrzeuge auf Schweizer ETCS Level 2 Strecken (Kapitel 3)
 - Schweizer Fahrzeuge auf ausländischen ETCS Level 2 Strecken (Kapitel 4)
 - Ausländische Fahrzeuge auf Schweizer ETCS Level 2 Strecken (Kapitel 5)

1.3 Abgrenzung

- 1.3.1.1 Dieses Dokument macht keine Aussagen zu den einzuhaltenden Vorgaben der Systemführerschaft ETCS CH im Zusammenhang mit dem Key Management, welche sich in den Dokumenten „KMC-CH Security Policy“ [1] und „Crypto Key Management (CKM) Vorgaben an Fahrzeuge und Strecken“ [2] finden.
- 1.3.1.2 Das vorliegende Dokument betrachtet lediglich das Key Management und macht keine Aussagen zu weiteren Aspekten des Netzzugangs oder den dabei relevanten Vorschriften und Prozessen.
- 1.3.1.3 Der Netzzugang für die Fahrzeuge wird in der Schweiz nicht über die Schlüssel geregelt, da periodische, u.U. wöchentliche, Schlüsselinstallationen auf den diversen RBC unverhältnismässig aufwendig und teuer oder technisch gar nicht möglich sind.
- 1.3.1.4 Es wird stattdessen durch den Abgleich der NID_ENGINE mit einer in der Bahnleittechnik hinterlegten Liste sichergestellt, dass nur Fahrzeuge mit gültiger Betriebsbewilligung auf der jeweiligen ETCS Level 2 Strecke verkehren.
- 1.3.1.5 Weiter sind die eigentlichen Schlüsselinstallationen auf den OBU und RBC nicht Teil dieses Dokuments, sondern erfolgen in der Verantwortung der jeweiligen Fahrzeughalter oder Infrastrukturunternehmen.

2 Allgemeine Aspekte

2.1 Termine und Ablauf

2.1.1.1 Ein Schlüsselupgrade findet halbjährlich im Frühling und im Herbst für alle Schweizer ETCS Level 2 Strecken statt, so dass neue Fahrzeuge jeweils ab dem darauffolgenden Fahrplanwechsel verkehren können.

2.1.1.2 Die genauen Termine können Tabelle 1 entnommen werden:

Frühling	Herbst	Aktivität
20. Januar	20. Juli	Der Besteller informiert das KMC-CH, kmc-ch@sbb.ch , über neue Fahrzeuge und liefert die notwendigen Daten
27. Januar	27. Juli	KMC-CH liefert die Schlüssel aus
31. Mai	30. November	Schlüssel auf Schweizer ETCS Level 2 Strecken installiert

Tabelle 1: Schlüsselupgrade: Termine und Ablauf

2.1.1.3 Fahrzeuge, welche nicht mehr auf ETCS Level 2 Strecken verkehren, können dem KMC-CH jederzeit gemeldet werden.

2.2 Auszutauschende Daten

2.2.1 Allgemein

2.2.1.1 Das KMC-CH benötigt zur Erstellung von Schlüsseln die folgenden Daten, Details s. folgende Kapitel:

- UIC Nummer und Fahrzeugbezeichnung oder Fahrzeugnummer
- NID_ENGINE, falls nicht vom KMC-CH vergeben
- Home KMC resp. KDC inkl. Kontaktangaben
- Ausländisches KMC inkl. Kontaktangaben und Strecken, falls relevant

2.2.1.2 Bei im Ausland immatrikulierten Fahrzeugen müssen allfällig notwendige Schlüssel rechtzeitig durch das ausländische KMC zur Verfügung gestellt werden.

2.2.2 UIC Nummer, Fahrzeugbezeichnung, Fahrzeugnummer

2.2.2.1 Die UIC Nummer erlaubt es, ein Fahrzeug eindeutig zu identifizieren.

2.2.2.2 Im Alltag wird anstelle der UIC Nummer oft eine kürzere und prägnantere Fahrzeugbezeichnung oder Fahrzeugnummer verwendet, z.B. Re460 001 anstatt 91 85 4460 001-1.

2.2.2.3 Bei mehrteiligen Fahrzeugen, z.B. Triebzügen, ist anzugeben, welche „Wagen“ mit einer OBU ausgerüstet sind.

2.2.2.4 Sämtliche in der Schweiz verwendeten UIC Nummern und Fahrzeugbezeichnungen werden zusammen mit weiteren Angaben in einer Liste publiziert [3].

2.2.3 NID_ENGINE

2.2.3.1 Die NID_ENGINE, auch als OBU ID bezeichnet, erlaubt es, eine OBU eindeutig zu identifizieren.

- 2.2.3.2 Für in der Schweiz immatrikulierte Fahrzeuge wird die NID_ENGINE normalerweise vom KMC-CH vergeben.
- 2.2.3.3 Für im Ausland immatrikulierte Fahrzeuge wird die NID_ENGINE vom jeweiligen Home KMC oder vom Lieferanten der OBU vergeben.
- 2.2.3.4 Sämtliche in der Schweiz verwendeten NID_ENGINE werden zusammen mit weiteren Angaben in einer Liste publiziert [3].

2.2.4 Home KMC resp. KDC

- 2.2.4.1 Als Home KMC wird dasjenige KMC bezeichnet, welches die Schlüsselupgrades an einer OBU vornehmen darf.
- 2.2.4.2 Dies bedeutet nicht, dass das Home KMC effektiv die Schlüssel auf der OBU installiert, sondern dass das Home KMC die dazu notwendigen Daten bereitstellt.
- 2.2.4.3 Zusätzlich zum Home KMC kann ein Key Distribution Center (KDC) verwendet werden, etwa wenn die vom Home KMC gelieferten Schlüssel durch den OBU Lieferanten in die Fahrzeug SW eingebracht werden.
- 2.2.4.4 Für alle in der Schweiz immatrikulierten Fahrzeuge ist das KMC-CH das Home KMC.
- 2.2.4.5 Es ist deshalb nur das KDC, inkl. Kontaktperson, E-Mail Adresse und, falls vorhanden, Telefonnummer, anzugeben, falls ein KDC verwendet wird.
- 2.2.4.6 Für im Ausland immatrikulierte Fahrzeuge ist das Home KMC, inkl. Kontaktperson, E-Mail Adresse und, falls vorhanden, Telefonnummer, anzugeben.

2.2.5 Ausländisches KMC und Strecken

- 2.2.5.1 Das ausländische KMC wird benötigt, um die Schlüssel auszutauschen, wenn in der Schweiz immatrikulierte Fahrzeuge auf ausländischen ETCS Level 2 Strecken verkehren werden.
- 2.2.5.2 Das ausländische KMC, inkl. Kontaktperson, E-Mail Adresse und, falls vorhanden, Telefonnummer, ist deshalb nur in diesem Fall anzugeben.
- 2.2.5.3 Falls mehrere ausländische ETCS Level 2 Strecken in Frage kommen, ist auch anzugeben, für welche Strecken (oder RBC) Schlüssel benötigt werden.

2.3 Schlüsselvergabe durch das KMC-CH

- 2.3.1.1 Das KMC-CH vergibt i.d.R. einen Schlüssel pro OBU, welcher für alle ETCS Level 2 Strecken in der Schweiz gilt und eine zeitlich unbeschränkte Gültigkeitsdauer hat.
- 2.3.1.2 Dadurch ist sichergestellt, dass nach der Erstinstallation keine weiteren Schlüsselupgrades auf den Fahrzeugen notwendig sind, solange sich das Einsatzgebiet des Fahrzeugs nicht ändert.
- 2.3.1.3 Es gibt jedoch folgende Ausnahmen:
- Fahrzeuge, welche auf ausländischen ETCS Level 2 Strecken verkehren, wenn diese Strecken Schlüssel mit begrenzter Gültigkeitsdauer verwenden.
 - Neue, aktuell nicht geplante, Schweizer ETCS Level 2 Strecken.
- 2.3.1.4 Für weitere Informationen oder bei Fragen ist das KMC-CH, kmc-ch@sbb.ch, zu kontaktieren.

3 Schweizer Fahrzeuge auf Schweizer Strecken

3.1.1.1 In diesem Fall sind folgende Daten ans KMC-CH zu liefern:

- UIC Nummer
- Fahrzeugbezeichnung oder Fahrzeugnummer
- KDC inkl. Kontaktangaben, falls ein KDC verwendet wird

3.1.1.2 Abbildung 1 zeigt den Schlüsselupgrade Prozess in diesem Fall:

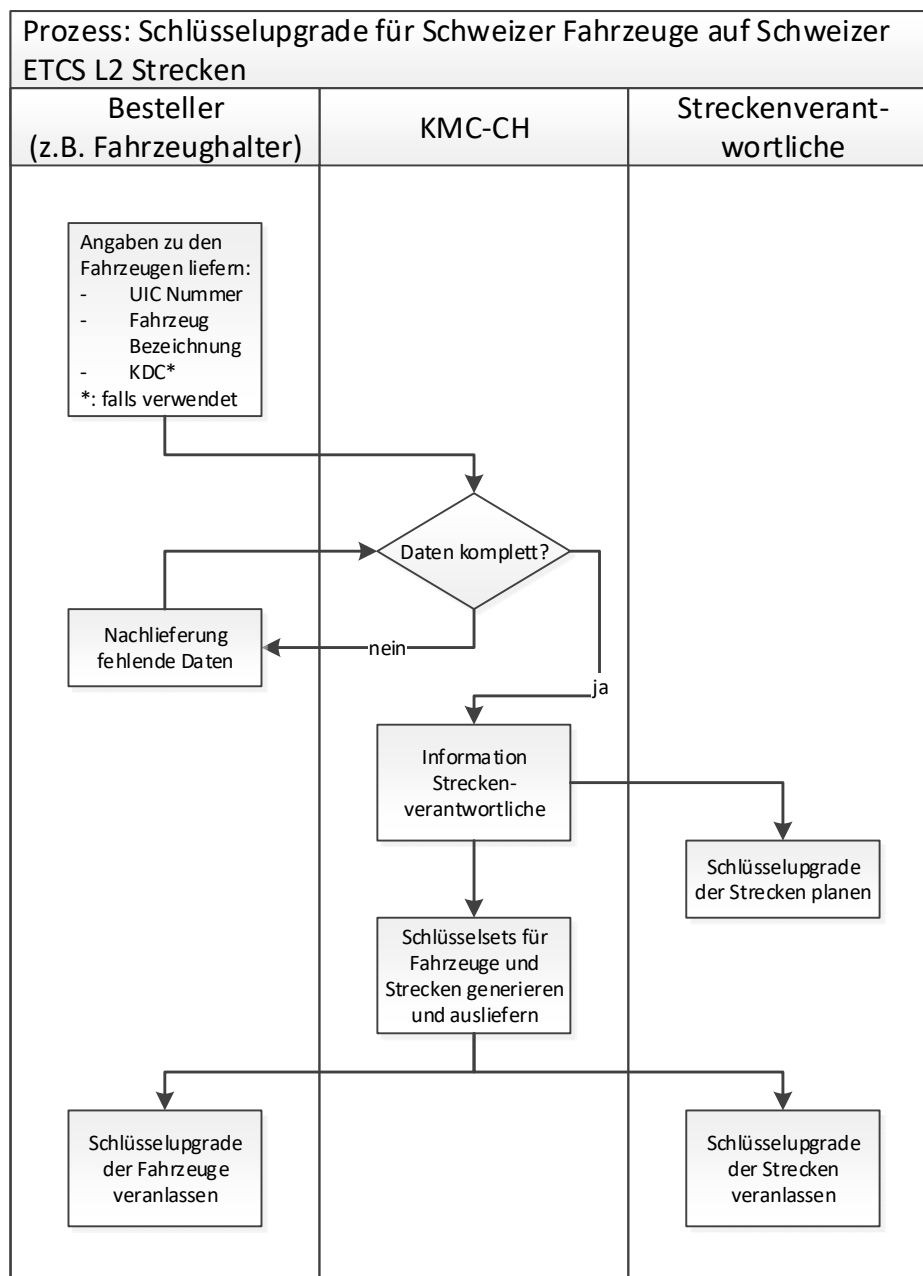


Abbildung 1: Schweizer Fahrzeuge auf Schweizer Strecken

4 Schweizer Fahrzeuge auf ausländischen Strecken

4.1.1.1 In diesem Fall sind folgende Daten ans KMC-CH zu liefern:

- UIC Nummer
- Fahrzeugbezeichnung oder Fahrzeugnummer
- Ausländisches KMC inkl. Kontaktangaben und zu befahrende Strecken (oder RBC)
- KDC inkl. Kontaktangaben, falls ein KDC verwendet wird

4.1.1.2 Abbildung 2 zeigt den Schlüsselupgrade Prozess in diesem Fall:

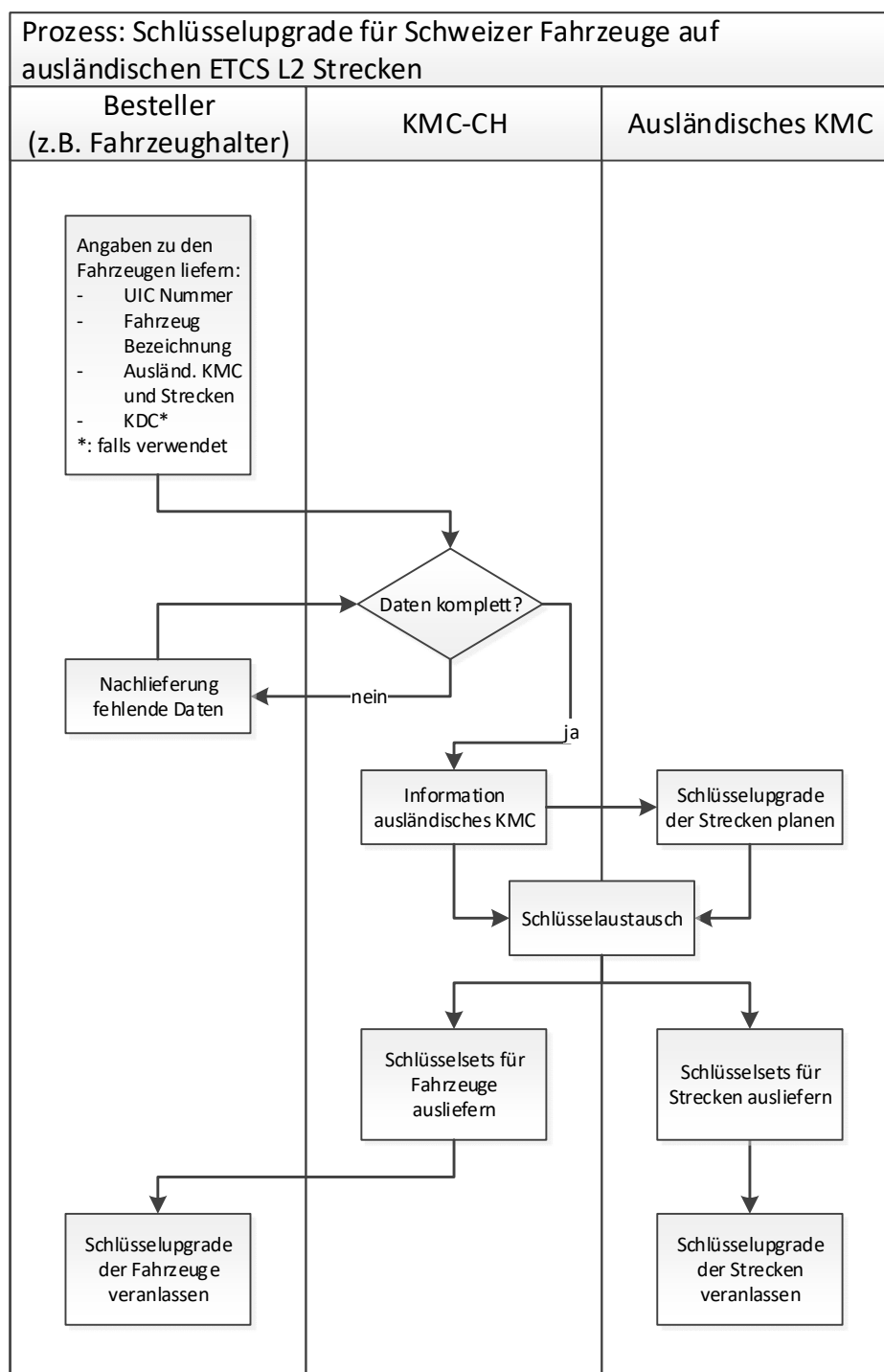


Abbildung 2: Schweizer Fahrzeuge auf ausländischen Strecken

5 Ausländische Fahrzeuge auf Schweizer Strecken

5.1.1.1 In diesem Fall sind folgende Daten ans KMC-CH zu liefern:

- UIC Nummer
- Fahrzeugbezeichnung oder Fahrzeugnummer
- NID_ENGINE
- Home KMC inkl. Kontaktangaben, falls das Home KMC nicht der Besteller ist

5.1.1.2 Abbildung 3 zeigt den Schlüsselupgrade Prozess in diesem Fall:

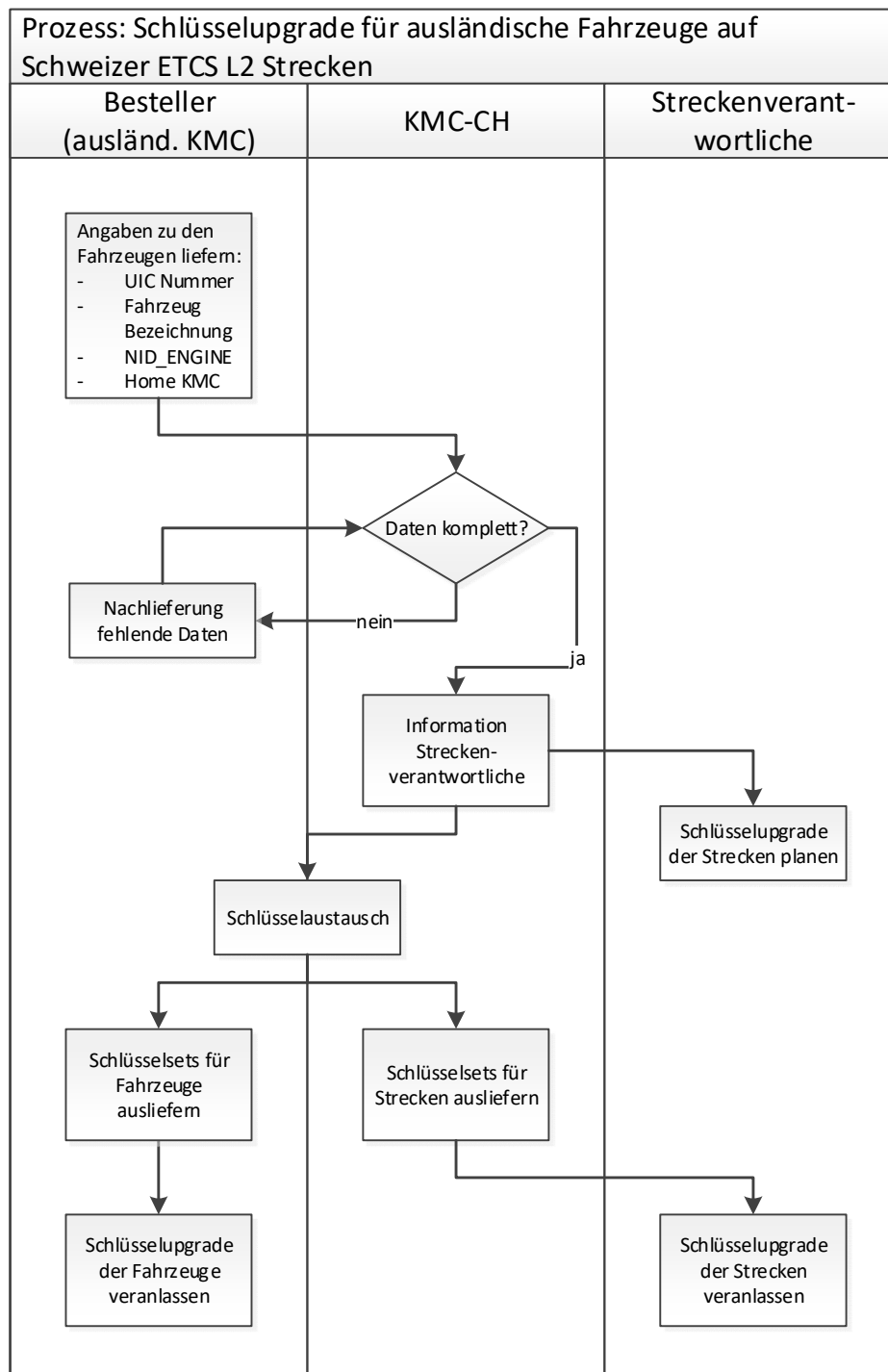


Abbildung 3: Ausländische Fahrzeuge auf Schweizer Strecken