

# Business Unit I-AT-SAZ

## System Management ETCS CH

### **CKM Guide**

### Version V1.0

Date: 02.07.2018  
Document ID: L2\_CH\_Eng\_13

	Written by	QA by	Approved by
Date, Signature	02.07.2018 / WB	02.07.2018 / EA	02.07.2018 / pu
Name	Bettina Wilhelm	Alfred Essig	Frank Pulfer
Function	System Engineer, I-AT-SAZ	Quality Manager, I-AT-SAZ	System Manager ETCS CH

This document is a translation. The signatures are on the original document.

## Document control sheet

Contents	This document serves as a guide for parties ordering keys and describes the steps that need to be taken from a key management point of view before vehicles can run on ETCS Level 2 lines.
Author	Bettina Wilhelm
Word processor	Microsoft Word 2016
File name	18_CKM_Leitfaden_v10_EN.docx
Document status	working / in review / <b><u>approved</u></b>
Controlled document	No
Distribution list	System Manager ETCS CH, FOT
Document owner	System Manager ETCS CH
Validity	Valid until a newer version of this document is produced or this document is withdrawn.
Safety	This document does not need to be reviewed by an independent body.
Periodic monitoring	The document is to be checked for relevancy after a maximum of five years.
Storage/archiving	Electronic. The document will be stored for five years after it is withdrawn or after a new version is produced; it may then be archived if required.
Note	<p>The original document is stored electronically. If a hard copy version of the document is used, the users must check the validity of the current document version.</p> <p>In the event of any doubt regarding content, the original document specified below shall apply exclusively.</p>
Original document	CKM Leitfaden, V1.0, 02.07.2018
Language of the original document	German
Translated by	SBB translation service

## Copyright (extract from protection notice ISO 16016)

The copyright notice for the System Management ETCS CH document, published by the FOT, should be understood as meaning that its further dissemination and reproduction are expressly permitted.

## Relevancy check

Next check:	Date	Checked by
July 2023 at the latest		

## Amendment record

Version	Date	Author	Amendments
X0.1	20.06.18	B. Wilhelm	Document created
X0.2	28.06.18	B. Wilhelm	Review comments incorporated in accordance with rv_18_CKM_Leitfaden_x01_alle.docx
V1.0	02.07.18	B. Wilhelm	Approval

## Contents

<b>1</b>	<b>Introduction</b>	<b>6</b>
1.1	Background information about key management	6
1.2	Purpose of the document	6
1.3	Scope	6
<b>2</b>	<b>General aspects</b>	<b>7</b>
2.1	Time frame and process	7
2.2	Data to be exchanged	7
2.2.1	General	7
2.2.2	UIC number, vehicle designation, vehicle number	7
2.2.3	NID_ENGINE	7
2.2.4	Home KMC or KDC	8
2.2.5	Foreign KMC and lines	8
2.3	Assignment of keys by the KMC-CH	8
<b>3</b>	<b>Swiss vehicles on Swiss lines</b>	<b>9</b>
<b>4</b>	<b>Swiss vehicles on foreign lines</b>	<b>10</b>
<b>5</b>	<b>Foreign vehicles on Swiss lines</b>	<b>11</b>

## List of figures

Figure 1: Swiss vehicles on Swiss lines	9
Figure 2: Swiss vehicles on foreign lines	10
Figure 3: Foreign vehicles on Swiss lines	11

## List of tables

Table 1: Key upgrades: time frame and process	7
---	---

## References

- [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 and NID\_KMC used in Switzerland; ETCS\_IDs\_CH

Note: No version is specified for any of the references. The version which is valid at the time of use is the applicable version in each case.

## Abbreviations and glossary

CKM	Crypto key management
Crypto key	Alternative name for key
ETCS	European Train Control System
FOT	Federal Office of Transport
Home KMC	Each OBU (and each RBC) is assigned to a KMC, which is its home KMC. Keys may only be upgraded by the home KMC.
KDC	Key distribution centre A KDC can send and receive messages and keys, but cannot generate keys itself.
KMC	Key management centre A KMC can send and receive messages and keys and also generate keys itself. A KMC can also be a home KMC.
KMC-CH	Key management centre for Switzerland
NID_ENGINE	ETCS variable, OBU identification number
OBU	On-board unit
OBU ID	Colloquial term for the NID_ENGINE
Ordering party	This refers to the party ordering keys from the KMC-CH. This may be the vehicle keeper, the OBU supplier or a foreign KMC, depending on the situation.
RBC	Radio block centre
SBB	Swiss Federal Railways
SW	Software
UIC	Union Internationale des Chemins de Fer

# 1 Introduction

## 1.1 Background information about key management

- 1.1.1.1 ETCS Level 2 uses keys known as “crypto keys” to authenticate vehicles (OBU) and radio block centres (RBC) when establishing connections.
- 1.1.1.2 These crypto keys are symmetric keys, meaning they need to be installed on the trackside and on the vehicle prior to operations with ETCS Level 2.
- 1.1.1.3 The term “key management” encompasses all activities relating to these keys.

## 1.2 Purpose of the document

- 1.2.1.1 This document serves as a guide for parties ordering keys from the KMC-CH and describes the steps that need to be taken from a key management point of view before vehicles can run on ETCS Level 2 lines.
- 1.2.1.2 Depending on the situation, the party ordering the keys may be:
  - the vehicle keeper
  - the OBU supplier
  - a foreign KMC
- 1.2.1.3 Section 2 deals with the general aspects of key management, while the subsequent sections focus on the various processes involved:
  - Swiss vehicles on Swiss ETCS Level 2 lines (Section 3)
  - Swiss vehicles on foreign ETCS Level 2 lines (Section 4)
  - Foreign vehicles on Swiss ETCS Level 2 lines (Section 5)

## 1.3 Scope

- 1.3.1.1 This document does not make any statements about the requirements from System Management ETCS CH with regard to key management, which can be found in the documents “KMC-CH Security Policy” [1] and “Crypto key management (CKM), Vorgaben an Fahrzeuge und Strecken” [2].
- 1.3.1.2 This document focuses exclusively on key management and does not make any statements about other aspects regarding network access or the regulations and processes relevant to this.
- 1.3.1.3 In Switzerland, network access for vehicles is not regulated via the keys, as periodic (potentially weekly) key installations at the various RBC would be unreasonably time-consuming and expensive or absolutely impossible from a technical perspective.
- 1.3.1.4 Instead, the NID\_ENGINE is checked against a list stored in the traffic control system to ensure that only vehicles with a valid operating licence are running on the ETCS Level 2 line in question.
- 1.3.1.5 Moreover, the actual key installations on the OBU and at the RBC are not covered by this document. These are the responsibility of the relevant vehicle keeper or infrastructure manager.

## 2 General aspects

### 2.1 Time frame and process

- 2.1.1.1 Key upgrades are carried out every six months (in the spring and in the autumn) for all Swiss ETCS Level 2 lines, thus ensuring that new vehicles can start operating when each timetable change comes into effect.
- 2.1.1.2 The precise dates are shown in Table 1:

Spring	Autumn	Activity
20 January	20 July	The ordering party notifies the KMC-CH, <a href="mailto:kmc-ch@sbb.ch">kmc-ch@sbb.ch</a> , of any new vehicles and provides the necessary data
27 January	27 July	The KMC-CH supplies the keys
31 May	30 November	The keys are installed on Swiss ETCS Level 2 lines

Table 1: Key upgrades: time frame and process

- 2.1.1.3 Vehicles no longer running on ETCS Level 2 lines can be reported to the KMC-CH at any time.

### 2.2 Data to be exchanged

#### 2.2.1 General

- 2.2.1.1 In order to issue keys, the KMC-CH needs the following data (see next section for details):
- UIC number and vehicle designation or vehicle number
  - NID\_ENGINE, if not assigned by the KMC-CH
  - Home KMC or KDC, including contact details
  - Foreign KMC including contact details and lines, if relevant
- 2.2.1.2 In the case of vehicles registered abroad, any keys required must be provided by the foreign KMC in good time.

#### 2.2.2 UIC number, vehicle designation, vehicle number

- 2.2.2.1 The UIC number makes it possible to clearly identify a vehicle.
- 2.2.2.2 In day-to-day operations, a shorter and more concise vehicle designation or vehicle number is often used instead of the UIC number, e.g. Re460 001 instead of 91 85 4460 001-1.
- 2.2.2.3 In the case of vehicles such as multiple units, which consist of several parts, it is necessary to specify which “coaches” are equipped with an OBU.
- 2.2.2.4 All UIC numbers and vehicle designations used in Switzerland are published in a list along with further details [3].

#### 2.2.3 NID\_ENGINE

- 2.2.3.1 The NID\_ENGINE, also known as the OBU ID, makes it possible to clearly identify an OBU.

- 2.2.3.2 For vehicles registered in Switzerland, the NID\_ENGINE is usually assigned by the KMC-CH.
- 2.2.3.3 For vehicles registered abroad, the NID\_ENGINE is assigned by the relevant home KMC or the OBU supplier.
- 2.2.3.4 All NID\_ENGINES used in Switzerland are published in a list along with further details [3].

#### **2.2.4 Home KMC or KDC**

- 2.2.4.1 “Home KMC” is the term used to refer to the KMC which is authorised to carry out key upgrades on an OBU.
- 2.2.4.2 This does not mean that the home KMC actually installs the keys on the OBU, but it does provide the data required for this.
- 2.2.4.3 In addition to the home KMC, a key distribution centre (KDC) may be used, for example if the keys supplied by the home KMC are incorporated into the vehicle SW by the OBU supplier.
- 2.2.4.4 The KMC-CH is the home KMC for all vehicles registered in Switzerland.
- 2.2.4.5 Therefore only details of the KDC (including contact person, e-mail address and telephone number, if available) need to be provided, if a KDC is being used.
- 2.2.4.6 For vehicles registered abroad, the home KMC needs to be specified (including contact person, e-mail address and telephone number, if available).

#### **2.2.5 Foreign KMC and lines**

- 2.2.5.1 The foreign KMC is required for the purpose of exchanging keys if vehicles registered in Switzerland are to run on foreign ETCS Level 2 lines.
- 2.2.5.2 Details of the foreign KDC (including contact person, e-mail address and telephone number, if available) therefore only need to be provided in such cases.
- 2.2.5.3 If several foreign ETCS Level 2 lines are involved, it is also essential to indicate which lines (or RBC) keys are needed for.

### **2.3 Assignment of keys by the KMC-CH**

- 2.3.1.1 The KMC-CH normally assigns one key per OBU, which is valid for all ETCS Level 2 lines in Switzerland for an unlimited period of time.
- 2.3.1.2 This ensures that no further key upgrades are required on the vehicles after the initial installation, unless the vehicle’s area of operation changes.
- 2.3.1.3 However, the following exceptions apply:
- Vehicles running on foreign ETCS Level 2 lines, if these lines use keys that are valid for a limited period.
  - New, not yet planned ETCS Level 2 lines in Switzerland.
- 2.3.1.4 If you would like more information or have any questions, please contact the KMC-CH, [kmc-ch@sbb.ch](mailto:kmc-ch@sbb.ch).



### 3 Swiss vehicles on Swiss lines

3.1.1.1 In this case, the following data needs to be supplied to the KMC-CH:

- UIC number
- Vehicle designation or vehicle number
- KDC, including contact details, if a KDC is being used

3.1.1.2 Figure 1 shows the key upgrade process in this case:

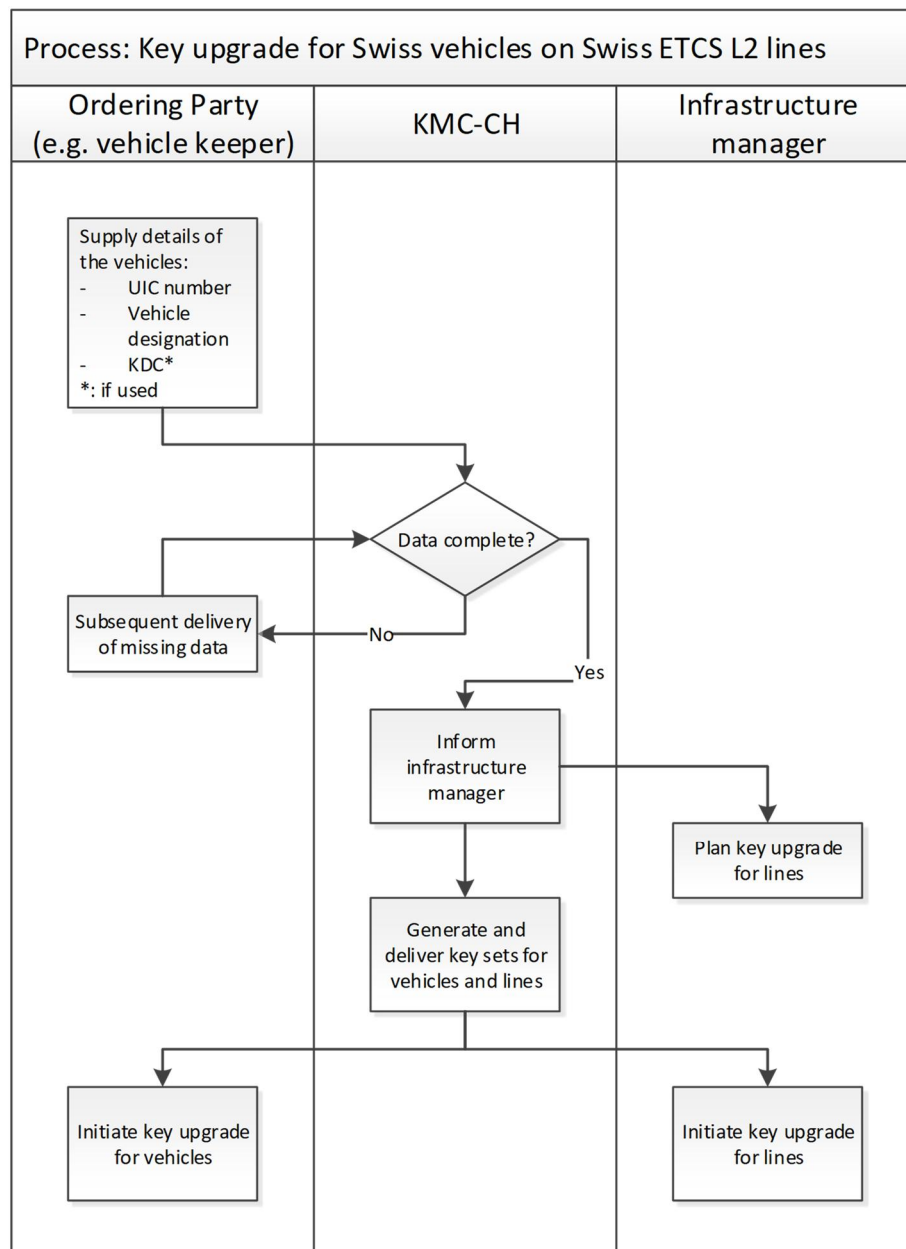


Figure 1: Swiss vehicles on Swiss lines

## 4 Swiss vehicles on foreign lines

4.1.1.1 In this case, the following data needs to be supplied to the KMC-CH:

- UIC number
- Vehicle designation or vehicle number
- Foreign KMC, including contact details and lines to be travelled (or RBC)
- KDC, including contact details, if a KDC is being used

4.1.1.2 Figure 2 shows the key upgrade process in this case:

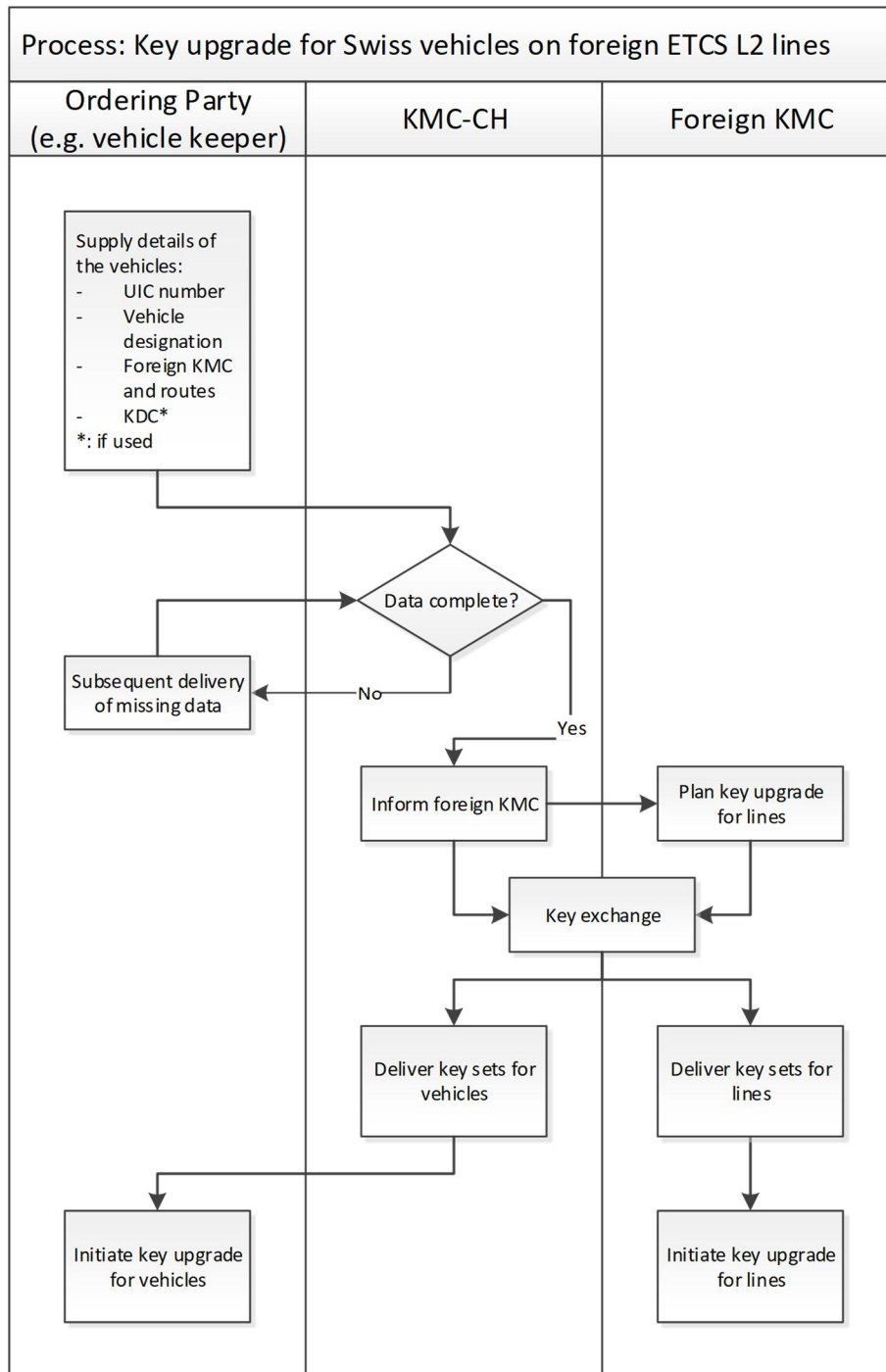


Figure 2: Swiss vehicles on foreign lines

## 5 Foreign vehicles on Swiss lines

5.1.1.1 In this case, the following data needs to be supplied to the KMC-CH:

- UIC number
- Vehicle designation or vehicle number
- NID\_ENGINE
- Home KMC, including contact details, if the home KMC is not the ordering party

5.1.1.2 Figure 3 shows the key upgrade process in this case:

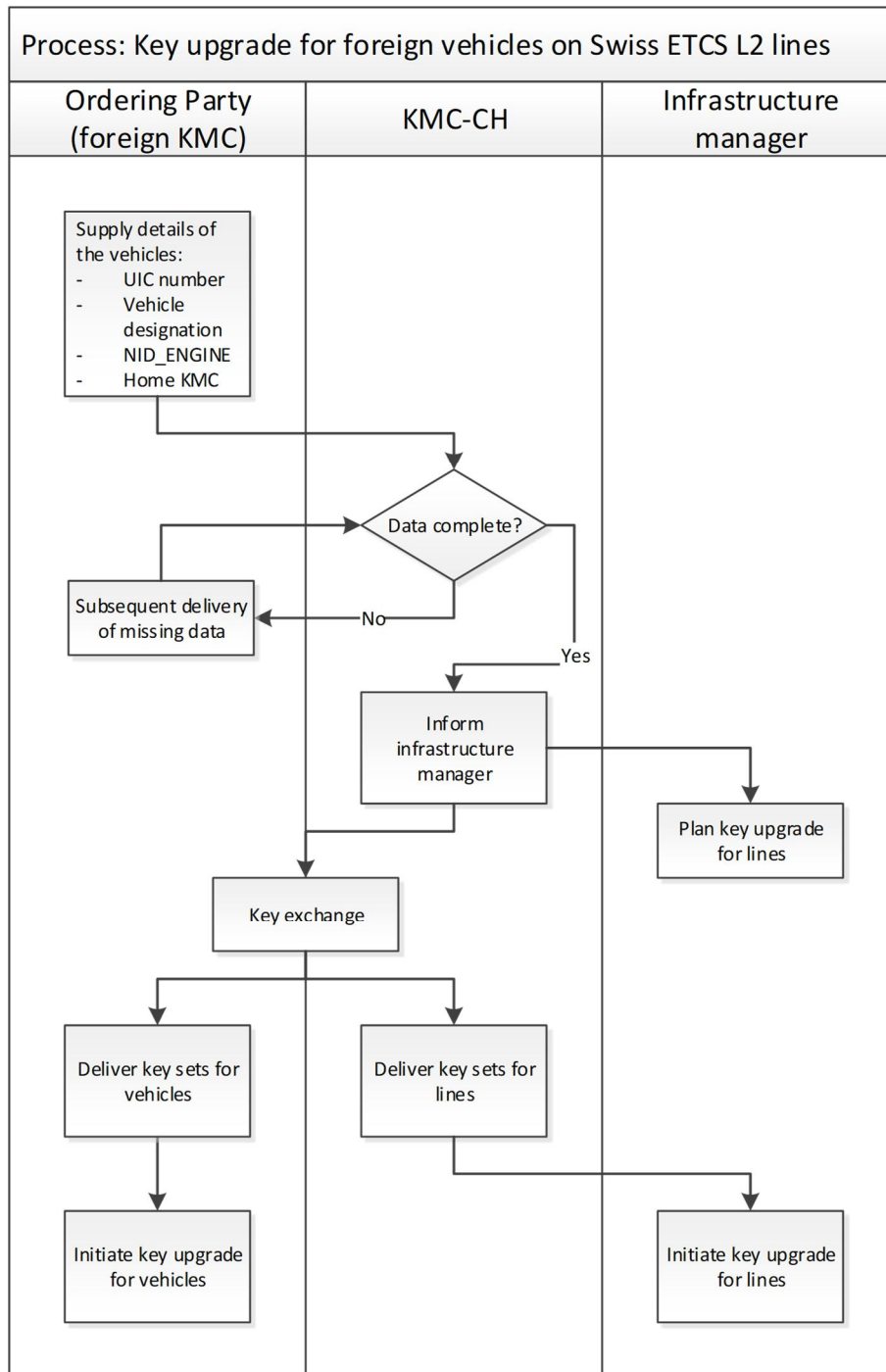


Figure 3: Foreign vehicles on Swiss lines