

Geschäftseinheit I-AT-SAZ

Systemführerschaft ETCS CH

Crypto Key Management (CKM)

Vorgaben an Fahrzeuge und

Strecken

Version V1.8

Vom: 01.05.2019
SF Dokumenten-ID: L2_CH_Eng_05

	Erstellt	Q-geprüft	Freigegeben
Datum, Visum	01/05/19 	06.05.2019 	6.5/2019 
Name	Bettina Wilhelm	Alfred Essig	Frank Pulfer
Stelle / Funktion	System Engineer I-AT-SAZ	Qualitätsmanager I-AT-SAZ	Leiter Systemführerschaft ETCS CH I-AT-SAZ

Dokumenten-Kontrollblatt

Inhalt	Crypto Key Management (CKM) Vorgaben an Fahrzeuge und Strecken
Ersteller	Bettina Wilhelm
Wordprozessor	Microsoft Word 2016
Filename	08_SF_CKM_Vorgaben_SF_V1.8.docx
Status des Dokuments	In Bearbeitung / in Review / <u>freigegeben</u>
Gelenktes Dokument	Nein
Verteiler	SF ETCS CH, BAV
Dokumenteigner	Systemführerschaft ETCS CH
Gültigkeit	Bis zum Vorliegen einer neueren Version dieses Dokuments oder eines Nachfolgedokuments.
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 erfolgt Aufbewahrung > 5 Jahre; danach Archivierung bei Erfordernis.
Hinweis	Das Originaldokument ist elektronisch gespeichert. Falls das Dokument in einer Papierversion benutzt wird, muss der Benutzer die Gültigkeit der aktuellen Dokumentversion überprüfen.

Urheberrecht (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 Mai 2024		

Änderungsnachweise

Version	Datum	Ersteller	Änderungshinweise
X1.0	29.05.08	N. Cedraschi	Erstellung Dokument
X1.1	13.06.08	M. Meier	Übernahme des Dokuments und Einarbeitung weiterer Aspekte
X 1.2	29.06.11	R. Allemann	Überarbeitung des Dokuments
X 1.3	14.07.11	R. Allemann	Einarbeitung Reviewkommentare gemäss rv_08_SF_CKM_Vorgaben_SF_X1 2_all.doc
V 1.4	17.08.11	R. Allemann	Freigabe
V1.5	12.12.14	B. Wilhelm	Kapitel 3: 3.1.1.4 ergänzt Kapitel 4: Anf. CKM-13 und CKM-14 ergänzt Kapitel 5: Anf. CKM-15 ergänzt Neues Kapitel 6 eingefügt
V1.6	17.12.14	B. Wilhelm	Anpassungen gemäss rv_08_SF_CKM_Vorgaben_SF_V1.5_alle.docx, Freigabe
V1.7	08.04.19	B. Wilhelm	Ganzes Dokument: Anpassung des Layouts an die aktuelle Vorlage von I-AT-SAZ Kapitel 1-3: redaktionelle Überarbeitung Kapitel 4: Anf. CKM-17 ergänzt Kapitel 6: Anf. CKM-16 präzisiert
V1.8	01.05.19	B. Wilhelm	Anpassungen gemäss rv_08_SF_CKM_Vorgaben_SF_V1.7_alle.docx Freigabe

Inhaltsverzeichnis

1	Einleitung	6
2	Begriffserklärungen	7
2.1	KM – Key Management	7
2.2	KMC – Key Management Center	7
2.3	KMC-CH – Key Management Center Schweiz	7
2.4	Home-KMC	7
2.5	KDC – Key Distribution Center	8
3	Rahmenbedingungen	9
4	Vorgaben an die Fahrzeughalter	10
4.1	Vorgaben an Fahrzeughalter mit KMC-CH als Home-KMC	10
4.2	Vorgaben an Fahrzeughalter mit KMC-CH als nicht Home-KMC	12
5	Vorgaben an die Streckenbetreiber	14
6	Vorgaben im Zusammenhang mit Tests	16
7	Kontakt	17

Referenzen

- [1] SBB: KMC-CH Security Policy; V1.1; 24.01.2008
- [2] UNISIG: Off-line Key Management FIS, Subset-038; Version 2.1.9; 12.09.2005
- [3] SBB: Sicherheitsnachweiskonzept für die Erlangung einer ETCS-Zulassung in der Schweiz (Fahrzeuge und Infrastruktur-Anlagen); V2.02; 22.11.2014
- [4] UNISIG: Subset-114, KMC-ETCS Entity Off-line KM FIS, Subset-114; Version 1.1.0; 17.12.2015

Abkürzungen und Begriffe

BAV	Bundesamt für Verkehr
CKM	Crypto Key Management
ERA	European Railway Agency (http://www.era.europa.eu); neu auch als EUAR (European Union Agency for Railways) bezeichnet.
ETCS	European Train Control System
EVU	Eisenbahnverkehrsunternehmen (Netzbenutzer)
I-AT-SAZ	Infrastruktur – Anlagen und Technologie – Sicherungsanlagen und Zugbeeinflussung (SBB Organisationseinheit)
IM	Infrastrukturmanager (entspricht der juristischen Person eines Infrastrukturunternehmers)
IOP	Interoperabilität
KDC	Key Distribution Center
KM	Key Management
KMC	Key Management Center
KMC-CH	Key Management Center Schweiz
KTRANS	Transportschlüssel; wird benötigt, um die eigentlichen Schlüssel während dem Transport zu verschlüsseln.
NID_ENGINE	ETCS-Identifikationsnummer einer OBU
OBU	Onboard Unit; ETCS-Fahrzeugausrüstung
RBC	Radio Block Center; Streckenzentrale
SBB	Schweizerische Bundesbahnen
Schlüsselvereinbarung	Eine Schlüsselvereinbarung besteht aus dem eigentlichen Schlüssel (Crypto Key) und weiteren Daten, z.B. für welche OBU und RBC der Schlüssel gültig ist.
SF	Systemführerschaft ETCS CH
UNISIG	Gemeinschaft der europäischen Signalindustrie

1 Einleitung

- 1.1.1.1 In diesem Dokument sind die Anforderungen aus Sicht CKM des Systemführers ETCS CH zusammengestellt.
- 1.1.1.2 Dabei wird unterschieden zwischen:
- Vorgaben für Fahrzeughalter mit Fahrzeugen, die in der Schweiz auf ETCS-Level-2-Strecken verkehren (s. Kapitel 4),
 - Vorgaben für Infrastrukturmanager von Schweizer ETCS-Level-2-Strecken (s. Kapitel 5) und
 - Vorgaben im Zusammenhang mit Tests (s. Kapitel 6).
- 1.1.1.3 Zusätzlich enthält das Dokument in Kapitel 2 Begriffserklärungen und im Kapitel 3 Rahmenbedingungen im Zusammenhang mit dem CKM.
- 1.1.1.4 Weitere Definitionen von verwendeten Begriffen wie Fahrzeughalter sind im Dokument [3] aufgeführt.

2 Begriffserklärungen

2.1 KM – Key Management

- 2.1.1.1 Für den Betrieb auf ETCS-Level-2-Strecken wird ein System benötigt, welches bei der Übermittlung von Informationen zwischen einem Fahrzeug und der Strecke gegenseitig sicherstellt, dass beide Entitäten zur Kommunikation berechtigt sind.
- 2.1.1.2 Zu diesem Zweck werden Schlüssel (Zertifikate) verwendet, welche vorgängig sowohl auf dem Fahrzeug als auch auf der Strecke installiert bzw. hinterlegt werden müssen.
- 2.1.1.3 Mit «Schlüsseln» sind in diesem Dokument generell Crypto-Schlüssel gemeint.
- 2.1.1.4 Unter Key Management ist die Gesamtheit der Prozesse zu verstehen, welche mit dem Lebenszyklus dieser Schlüssel verbunden sind.
- 2.1.1.5 Beispielprozesse sind:
 - Schlüsselgenerierung
 - Schlüsselverwaltung
 - Schlüsseltransport
 - Schlüssellöschung

2.2 KMC – Key Management Center

- 2.2.1.1 Ein Key Management Center (KMC) verfügt über die Berechtigung neue Schlüssel für die Netzbenutzung innerhalb seiner Key Management Domäne zu generieren.
- 2.2.1.2 Die Key Management Domäne eines KMC umfasst sowohl die ihm zugeordneten Fahrzeuge (OBU) als auch die ihm zugeordneten Strecken (RBC).
- 2.2.1.3 Diese Zuordnung erfolgt aus einer rein Key-Management-spezifischen Sicht und ist vollständig entkoppelt von den Eigentumsrechten an den entsprechenden Anlagen.
- 2.2.1.4 Dasjenige KMC, welches einen bestimmten Schlüssel generiert hat, bleibt der Eigner dieses Schlüssels über den ganzen Lebenszyklus dieses Schlüssels hinweg.
- 2.2.1.5 Schlüssel werden den Fahrzeughaltern und Infrastrukturmanagern (IM) durch ein KMC nur leihweise zur Nutzung zur Verfügung gestellt.
- 2.2.1.6 Der Besitzer eines Schlüssel ist dasjenige KMC, welches den Schlüssel generiert hat.
- 2.2.1.7 Schlüssel können durch ein KMC mit Validitätsdaten versehen werden, welche die Gültigkeitsdauer von Schlüsseln definieren.

2.3 KMC-CH – Key Management Center Schweiz

- 2.3.1.1 Die Aufgaben des KMC-CH sind hoheitlicher Natur, d.h. sie werden für alle IM in der Schweiz wahrgenommen.
- 2.3.1.2 In der Schweiz werden die Aufgaben des KMC durch die SBB-Infrastruktur im Auftrag des BAV im Rahmen der Systemführerschaft ETCS CH wahrgenommen.

2.4 Home-KMC

- 2.4.1.1 Home-KMC eines Fahrzeughalters ist dasjenige KMC, welches die Schlüssel für die Fahrzeuge eines Fahrzeughalters verwaltet.

- 2.4.1.2 Home-KMC eines IM ist dasjenige KMC, welches die Schlüssel für die ETCS-Level-2-Strecken dieses IM verwaltet.
- 2.4.1.3 Jeder Fahrzeughalter und Streckenbetreiber hat genau ein Home-KMC, somit ist jedes Fahrzeug und jede Strecke einem Home-KMC zugeordnet.

2.5 KDC – Key Distribution Center

- 2.5.1.1 Für jede ETCS-Komponente mit Schlüsseln kann es genau ein KDC geben, welches für die Installation bzw. Hinterlegung und Deinstallation bzw. Entfernung von Schlüsseln verantwortlich ist.
- 2.5.1.2 Die Verwendung eines KDC ist optional und abhängig von der betroffenen ETCS-Komponente (Fahrzeug oder Strecke).

3 Rahmenbedingungen

- 3.1.1.1 Das Home-KMC ist verantwortlich für die Verwaltung der Schlüssel.
- 3.1.1.2 Für den Austausch von Schlüsselmaterial sind nur folgende Wege zulässig:
- Home-KMC \leftrightarrow KMC
 - Home-KMC \rightarrow Betreiber (Fahrzeughalter/Strecke) (\rightarrow KDC)
- 3.1.1.3 Die ETCS-Identifikationsnummer (NID_ENGINE) wird durch das Home-KMC des Fahrzeughalters, durch die Industrie oder durch die ERA vergeben.
- 3.1.1.4 Die ETCS-Identifikationsnummer (NID_ENGINE) identifiziert eine ETCS-Fahrzeugausrüstung zu jedem Zeitpunkt eindeutig.

4 Vorgaben an die Fahrzeughalter

4.1 Vorgaben an Fahrzeughalter mit KMC-CH als Home-KMC

Identifikation	Anf. CKM-01
Titel	Security Policy
Beschreibung	Der Fahrzeughalter ist dafür verantwortlich, dass die KMC-CH Security Policy [1] von allen durch den Fahrzeughalter in den gesamten Prozess der Schlüsselverwaltung, resp. -vereinbarung und -installation involvierten Stellen eingehalten wird. Insbesondere muss der Fahrzeughalter sicherstellen, dass die KMC-CH Security Policy [1] auch durch sein(e) KDC eingehalten wird.
Anmerkung	
Querverweis	Keiner
Prüfhinweis	Nachweis

Identifikation	Anf. CKM-02
Titel	Übertragbarkeit Schlüsselvereinbarung
Beschreibung	Der Fahrzeughalter muss sicherstellen, dass eine Schlüsselvereinbarung nicht von einem Fahrzeug auf ein anderes Fahrzeug übertragen wird, auch wenn es sich um baugleiche Fahrzeuge handelt. Das KMC-CH kann Ausnahmen von dieser Regel zulassen.
Anmerkung	
Querverweis	Keiner
Prüfhinweis	Nachweis

Identifikation	Anf. CKM-03
Titel	Unveränderbarkeit der Schlüsselvereinbarung
Beschreibung	Der Fahrzeughalter darf ohne Einverständnis des KMC-CH Schlüsselvereinbarungen, welche für ETCS-Level-2-Strecken gültig sind, nicht ändern.
Anmerkung	
Querverweis	Keiner
Prüfhinweis	Nachweis

Identifikation	Anf. CKM-04
Titel	Einsatz Fahrzeuge im Ausland
Beschreibung	Möchte ein Fahrzeughalter seine Fahrzeuge auf ETCS-Level-2-Strecken ausserhalb der Schweiz verkehren lassen, so ist zwecks Organisation und Installation der notwendigen Schlüssel eine Anfrage an das KMC-CH zu richten.
Anmerkung	
Querverweis	Keiner
Prüfhinweis	Nachweis

Identifikation	Anf. CKM-13
Titel	Löschen der Schlüsselvereinbarung
Beschreibung	Bei der Ausserbetriebnahme eines Fahrzeugs muss der Fahrzeughalter sicherstellen, dass die Schlüsselvereinbarung auf dem Fahrzeug und bei allen durch den Fahrzeughalter in den gesamten Prozess der Schlüsselverwaltung, resp. -vereinbarung und -installation involvierten Stellen sicher gelöscht wird. Das KMC-CH kann Ausnahmen von dieser Regel zulassen.
Anmerkung	
Querverweis	Keiner
Prüfhinweis	Nachweis

Identifikation	Anf. CKM-17
Titel	Installation des Transportschlüssels (KTRANS)
Beschreibung	Gemäss Subset-114 [4] kann die Installation des Transportschlüssels (KTRANS) auf den Fahrzeugen nicht verschlüsselt erfolgen. Der Fahrzeughalter muss deshalb sicherstellen, dass die Schlüsselvereinbarung zur Installation von KTRANS zu jedem Zeitpunkt vor unbefugtem Zugriff geschützt ist. Die Schlüsselvereinbarung ist insbesondere sicher aufzubewahren oder nach erfolgter Installation sicher zu löschen. Bei Verwendung eines KDC muss der Fahrzeughalter sicherstellen, dass diese Anforderung auch durch sein(e) KDC eingehalten wird.
Anmerkung	Diese Anforderung gilt für ETCS-Fahrzeugausrüstungen gemäss Baseline 3, welche Subset-114 [4] verwenden.
Querverweis	Keiner
Prüfhinweis	Nachweis

4.2 Vorgaben an Fahrzeughalter mit KMC-CH als nicht Home-KMC

Identifikation	Anf. CKM-05
Titel	Security Policy
Beschreibung	Der Fahrzeughalter ist dafür verantwortlich, dass die KMC-CH Security Policy [1] von allen durch den Fahrzeughalter in den gesamten Prozess der Schlüsselverwaltung, resp. -vereinbarung und -installation involvierten Stellen eingehalten wird. Insbesondere muss der Fahrzeughalter sicherstellen, dass die KMC-CH Security Policy [1] auch durch sein(e) KDC eingehalten wird.
Anmerkung	Dies gilt nur für Schlüssel, welche das KMC-CH besitzt, d.h. generiert hat.
Querverweis	Keiner
Prüfhinweis	Nachweis

Identifikation	Anf. CKM-06
Titel	Übertragbarkeit Schlüsselvereinbarung
Beschreibung	Der Fahrzeughalter muss sicherstellen, dass eine Schlüsselvereinbarung für eine ETCS-Level-2-Strecke in der Schweiz nicht von einem Fahrzeug auf ein anderes Fahrzeug übertragen wird, auch wenn es sich um baugleiche Fahrzeuge handelt. Das KMC-CH kann Ausnahmen von dieser Regel zulassen.
Anmerkung	
Querverweis	Keiner
Prüfhinweis	Nachweis

Identifikation	Anf. CKM-07
Titel	Unveränderbarkeit der Schlüsselvereinbarung
Beschreibung	Der Fahrzeughalter darf ohne Einverständnis des KMC-CH Schlüsselvereinbarungen, welche für ETCS-Level-2-Strecken in der Schweiz gültig sind, nicht ändern.
Anmerkung	
Querverweis	Keiner
Prüfhinweis	Nachweis

Identifikation	Anf. CKM-08
Titel	Bestellung von Schlüsselvereinbarung
Beschreibung	Der Fahrzeughalter muss für jedes Fahrzeug, welches in der Schweiz unter ETCS Level 2 verkehren soll, sein Home-KMC beauftragen, eine Schlüsselvereinbarung für die ETCS-Level-2-Strecken in der Schweiz mit dem KMC-CH zu vereinbaren.
Anmerkung	
Querverweis	Keiner
Prüfhinweis	Nachweis

Identifikation	Anf. CKM-09
Titel	Subset-038 Schnittstelle
Beschreibung	Der Fahrzeughalter muss sicherstellen, dass sein Home-KMC über eine funktionierende, bidirektionale Schnittstelle gemäss Subset-038 v2.1.9 [2] mit dem KMC-CH verfügt.
Anmerkung	
Querverweis	Keiner
Prüfhinweis	Nachweis

Identifikation	Anf. CKM-14
Titel	Löschen der Schlüsselvereinbarung
Beschreibung	Bei der Ausserbetriebnahme eines Fahrzeugs muss der Fahrzeughalter sicherstellen, dass die Schlüsselvereinbarung für ETCS-Level-2-Strecken in der Schweiz auf dem Fahrzeug und bei allen durch den Fahrzeughalter in den gesamten Prozess der Schlüsselverwaltung, resp. -vereinbarung und -installation involvierten Stellen sicher gelöscht wird. Das KMC-CH kann Ausnahmen von dieser Regel zulassen.
Anmerkung	
Querverweis	Keiner
Prüfhinweis	Nachweis

5 Vorgaben an die Streckenbetreiber

Identifikation	Anf. CKM-10
Titel	Security Policy
Beschreibung	Der Streckenbetreiber ist dafür verantwortlich, dass die KMC-CH Security Policy [1] von allen durch den Streckenbetreiber in den gesamten Prozess der Schlüsselverwaltung, resp. -vereinbarung und -installation involvierten Stellen eingehalten wird. Insbesondere muss der Streckenbetreiber sicherstellen, dass die KMC-CH Security Policy [1] auch durch sein(e) KDC eingehalten wird.
Anmerkung	
Querverweis	Keiner
Prüfhinweis	Nachweis

Identifikation	Anf. CKM-11
Titel	Übertragbarkeit Schlüsselvereinbarung
Beschreibung	Der Streckenbetreiber muss sicherstellen, dass eine Schlüsselvereinbarung nicht von einem RBC auf ein anderes RBC übertragen wird. Das KMC-CH kann Ausnahmen von dieser Regel zulassen.
Anmerkung	
Querverweis	Keiner
Prüfhinweis	Nachweis

Identifikation	Anf. CKM-12
Titel	Unveränderbarkeit der Schlüsselvereinbarung
Beschreibung	Der Streckenbetreiber darf ohne Einverständnis des KMC-CH Schlüsselvereinbarungen nicht ändern.
Anmerkung	
Querverweis	Keiner
Prüfhinweis	Nachweis

Identifikation	Anf. CKM-15
Titel	Löschen der Schlüsselvereinbarung
Beschreibung	Bei der Ausserbetriebnahme eines RBC muss der Streckbetreiber sicherstellen, dass die Schlüsselvereinbarung auf dem RBC und bei allen durch den Streckenbetreiber in den gesamten Prozess der Schlüsselverwaltung, resp. -vereinbarung und -installation involvierten Stellen sicher gelöscht wird. Das KMC-CH kann Ausnahmen von dieser Regel zulassen.
Anmerkung	
Querverweis	Keiner
Prüfhinweis	Nachweis

6 Vorgaben im Zusammenhang mit Tests

Identifikation	Anf. CKM-16
Titel	Eindeutigkeit der Schlüsselvereinbarung
Beschreibung	Der Lieferant der ETCS Fahrzeugausrüstung muss sicherstellen, dass eine Schlüsselvereinbarung auch zu Testzwecken nicht auf mehreren ETCS Fahrzeugausrüstungen gleichzeitig installiert ist.
Anmerkung	
Querverweis	Keiner
Prüfhinweis	Nachweis

7 Kontakt

7.1.1.1 Das KMC-CH kann unter folgender E-Mail Adresse kontaktiert werden:

kmc-ch@sbb.ch