
SŽDC PPD-x/2018

Pokyn provozovatele dráhy k zajištění plynulé a bezpečné drážní dopravy – Vydávání šifrovacích klíčů pro komunikaci v systému ETCS

Účinnost od **x. xx. 2018**

Schváleno pod čj. /

dne

dne

Titul, jméno, příjmení, titul
funkce / pracovní zařazení

Titul, jméno, příjmení, titul
funkce / pracovní zařazení

SŽDC PPD-x/2018**Pokyn provozovatele dráhy k zajištění plynulé a bezpečné drážní dopravy – Vydávání šifrovacích klíčů pro komunikaci v systému ETCS**

Gestorský útvar: Správa železniční dopravní cesty, státní organizace
Technická ústředna dopravní cesty
Úsek automatizační a telekomunikační techniky
Malletova 10, Praha 9
www.szdc.cz

Rok vydání: 2018

Náklad: vydáno pouze v elektronické podobě

© Správa železniční dopravní cesty, státní organizace, rok 2018

Tento dokument je duševním vlastnictvím státní organizace Správa železniční dopravní cesty, na které se vztahuje zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů. Státní organizace Správa železniční dopravní cesty je v uvedené souvislosti rovněž vykonavatelem majetkových práv. Tento dokument smí fyzická osoba použít pouze pro svou osobní potřebu, právnická osoba pro svou vlastní vnitřní potřebu. Poskytování tohoto dokumentu nebo jeho části v jakékoliv formě nebo jakýmkoliv způsobem třetí osobě je bez svolení státní organizace Správa železniční dopravní cesty zakázáno.

ZÁZNAMY O OPRAVÁCH A ZMĚNÁCH

Držitel listinné podoby tohoto dokumentu je odpovědný za včasné a správné zapracování účinných oprav a změn a za provedení příslušného záznamu.

Oprava/změna a její pořadové číslo	Číslo jednací	Účinnost od	Opravu/změnu zapracoval

OBSAH

ZÁZNAMY O OPRAVÁCH A ZMĚNÁCH.....	3
OBSAH	4
ROZSAH ZNALOSTÍ.....	5
ZKRATKY A ZNAČKY.....	6
1 ÚVODNÍ USTANOVENÍ	7
2 ZÁKLADNÍ NÁZVY A POJMY PRO ÚČELY POKYNU	7
3 PROCES PŘIDĚLOVÁNÍ KLÍČŮ	7
4 PODMÍNKY AKTIVACE A INSTALACE KLÍČŮ NA DANÉ ETCS ENTITY	8
5 ZÁVĚREČNÁ USTANOVENÍ.....	9
SOUVISEJÍCÍ DOKUMENTY	9
PŘÍLOHY.....	9
Příloha A (normativní)	
Žádost pro vydání šifrovacích klíčů pro komunikaci v systému ETCS.....	10

ROZSAH ZNALOSTÍ

Níže uvedená tabulka stanovuje rozsah znalostí tohoto dokumentu pro pracovní zařazení (funkci) nebo činnost, přičemž:

- informativní znalostí se rozumí taková znalost, při které příslušný zaměstnanec má povědomí o tomto dokumentu, zná předmět jeho úpravy a při náhledu do příslušného ustanovení je schopen se podle takového ustanovení samostatně řídit nebo podle něj samostatně konat;
- úplnou znalostí se rozumí taková znalost, při které příslušný zaměstnanec má povědomí o tomto dokumentu, zná předmět jeho úpravy a bez náhledu do příslušného ustanovení je schopen se podle takového ustanovení samostatně řídit nebo podle něj samostatně konat;
- doslovnou znalostí se rozumí taková znalost, při které příslušný zaměstnanec zná text, který je v příslušném ustanovení napsán v uvozovkách kurzivou, přesně a je schopen jej bez náhledu do příslušného ustanovení samostatně reprodukovat.

Není-li rozsah znalostí pro pracovní zařazení (funkci) nebo činnost stanoven, stanoví rozsah znalostí, pokud je tak třeba učinit, příslušný vedoucí zaměstnanec.

Pracovní činnost nebo zařazení (funkce)	Znalost ustanovení
SŽDC – zaměstnanci, zabývající se činnostmi související s provozováním KMC SŽDC	úplná: celý Pokyn
SŽDC – zaměstnanci, podílející se na testování systému ETCS	informativní: celý Pokyn
Dopravci – odpovědný zástupce dopravce a jím určení zaměstnanci	úplná: celý Pokyn
Subjekt pro posuzování kompatibility – zaměstnanci podílející se na testování systému ETCS	informativní: celý Pokyn

ZKRATKY A ZNAČKY

Níže uvedený seznam obsahuje zkratky a značky použité v tomto dokumentu. V seznamu se neuvádějí legislativní zkratky, zkratky a značky obecně známé, zavedené právními předpisy, uvedené v obrázcích, příkladech nebo tabulkách.

CCS	Řízení a zabezpečení (Control Command and Signalling)
KMC	Centrum správy šifrovacích klíčů (Key Management Centre)
KMS	Management správy klíčů (Key Management System)
K-KMC	Transportní klíč KMC (Key-KMC)
KMAC	Autentifikační klíč (Key Message Authentication Code)
KTRANS	Transportní klíč (Key TRANSport)
ETCS	Evropský vlakový zabezpečovač (European Train Control System)
OBU	Mobilní (palubní) část systému ETCS (On-Board Unit), ETCS entita
RBC	Radiobloková centrála (Radio Block Centre), ETCS entita
SŽDC	Správa železniční dopravní cesty, státní organizace
TSI	Technické specifikace pro interoperabilitu
TÚDC	Technická ústředna dopravní cesty (organizační jednotka SŽDC)
VUZ	Výzkumný ústav železniční, a. s., Praha

1 ÚVODNÍ USTANOVENÍ

- 1.1 Správa železniční dopravní cesty, státní organizace (dále jen „SŽDC“), vydává tento Pokyn provozovatele dráhy k zajištění plynulé a bezpečné drážní dopravy (dále jen „Pokyn“) v souladu s ustanoveními § 22 odst. 3 písm. a) zákona č. 266/1994 Sb., o dráhách, ve znění pozdějších předpisů.
- 1.2 Pokyn stanovuje podmínky pro generování a přidělování šifrovacích klíčů potřebných pro provoz na tratích s evropským vlakovým zabezpečovačem ETCS úrovně 2. Pro tento účel provozuje SŽDC off-line centrum správy klíčů (dále jen KMC SŽDC), které odpovídá specifikacím TSI CCS (Subset-114 – KMC-ETCS Entity Off-line KM FIS a Subset-038 – Off-line Key Management FIS). Vzhledem k architektuře systému a očekávanému počtu radioblokových centrál (dále jen „RBC“) se předpokládá jedno KMC SŽDC pro všechny tratě provozované SŽDC.
- 1.3 Správu KMC SŽDC včetně generování a přidělování šifrovacích klíčů zajišťuje SŽDC, Technická ústředna dopravní cesty (dále jen TÚDC), Praha 9, Malletova 10, 190 00.

2 ZÁKLADNÍ NÁZVY A POJMY PRO ÚČELY POKYNU

- 2.1 **ETCS entita** – koncový uživatel šifrovacích klíčů (OBU, RBC);
- 2.2 **KMS** (Key Management System) – celoevropský management šifrovacích klíčů, který zahrnuje generování, ukládání a národní i mezinárodní přidělování klíčů ETCS entitám;
- 2.3 **KMC** (Key Management Centre) – centrum správy šifrovacích klíčů, které spravuje ETCS entity pomocí zpráv (požadavků a odpovědí);
- 2.4 **Domovské KMC** (Home KMC) – KMC, pod které patří daná ETCS entita;
- 2.5 **K-KMC** – transportní klíč pro zabezpečený přenos autentizačních klíčů mezi jednotlivými KMC;
- 2.6 **KMAC** – autentizační klíč pro komunikaci mezi jednotlivými RBC a OBU (ETCS entitami);
- 2.7 **KTRANS** – transportní klíč pro zabezpečený přenos (nahrání, smazání, aktualizace) autentizačních klíčů od KMC k jednotlivým ETCS entitám;
- 2.8 **Off-line KMS** – způsob aplikace KMS, který vyžaduje lidskou součinnost pro přenos zpráv mezi KMC a ETCS entitami;
- 2.9 **Typ OBU** je sestava konkrétních typů (konkrétního typu HW a verze SW) zařízení, které tvoří subsystém OBU na vozidle a podílí se na jeho funkci, včetně rádiových zařízení pro přenos dat (Data Only Radio) pro účely ETCS s konkrétním provedením rozhraní mezi OBU a ostatními systémy vozidla;
- 2.10 **Žadatel** – výrobce nebo dodavatel OBU, provozovatel drážní dopravy (dopravce) či jiný právní subjekt;

3 PROCES PŘIDĚLOVÁNÍ KLÍČŮ

- 3.1 Správce KMC SŽDC přiděluje žadateli na základě jeho žádosti šifrovací klíče pro zabezpečenou komunikaci mezi jednotlivými ETCS entitami, tedy mobilními částmi ETCS (dále jen „OBU“) a traťovou částí ETCS tvořenou souhrnem RBC. Formulář žádosti je ke stažení na portále provozování dráhy na adrese <http://provoz.szdc.cz> v záložce >Přístup na ŽDC>ETCS, případně na stránkách TÚDC na adrese <http://www.tudc.cz> v záložce >Dokumenty>ETCS.
- 3.2 Žadatel zašle žádost elektronickou poštou na emailovou adresu etcs@tudc.cz. Jednu žádost je možno předložit pro více OBU za předpokladu, že se jedná o stejnou typovou řadu vozidla se stejným typem OBU a pro daná OBU je požadováno vydání šifrovacích klíčů pro stejné traťové úseky (oblasti). Ve všech ostatních případech musí být žádost samostatná pro každou OBU.
- 3.3 Správce KMC SŽDC vydává šifrovací klíče v datové podobě ve formátu dle Subsetu-114, verze 1.1.0 (KMAC zašifrovaný pomocí KTRANS) nebo dle Subsetu-038, verze 3.1.0 (KMAC zašifrovaný pomocí K-KMC).
- 3.4 Proces přidělování šifrovacích klíčů je závislý na domovském centru správy klíčů pro OBU daného vozidla. Může jím být KMC SŽDC nebo jiné KMC (zpravidla KMC výrobce OBU). Je nepřijatelné, aby OBU daného vozidla mělo více než jedno domovské KMC.
 - 3.4.1 V případě, že je KMC SŽDC již domovským KMC pro OBU daného vozidla:
 - správce KMC SŽDC již negeneruje transportní klíč KTRANS (dále jen „KTRANS“);

- správce KMC SŽDC vygeneruje žadateli autentifikační klíč (dále jen KMAC), tento klíč zašifruje pomocí KTRANS a poté odešle elektronickou poštou na uvedenou kontaktní adresu spolu s informací o platnosti KMAC a seznamu ETCS entit, pro které platí;
 - žadatel je povinen informovat správce KMC SŽDC o provedené instalaci klíče KMAC do OBU daného vozidla a to buď datovou formou dle Subsetu-114, elektronickou poštou nebo písemně. Pokud žadatel nepotvrdí instalaci klíče KMAC na dané vozidlo, nebude klíč na straně traťové části aktivován. Pokud žadatel informuje správce KMC SŽDC elektronickou poštou nebo písemně, smí tak vždy učinit až po skutečném nahrání KMAC na vozidlo.
- 3.4.2 V případě, že OBU daného vozidla nepatří pod žádné domovské KMC a žadatel požaduje, aby se jím stalo KMC SŽDC:
- správce KMC SŽDC nejprve vygeneruje KTRANS a předá jej žadateli na vhodném přenosovém médiu (CD, flash disk apod.), z důvodu utajení nesmí být tento klíč odeslán elektronickou poštou. Žadatel tento klíč zároveň nesmí předávat třetím osobám;
 - následně správce KMC SŽDC vygeneruje žadateli KMAC, který je zašifrován pomocí KTRANS, a poté jej odešle elektronickou poštou na uvedenou kontaktní adresu spolu s informací o platnosti KMAC a seznamu ETCS entit, pro které platí;
 - žadatel je povinen informovat správce KMC SŽDC o provedené instalaci klíče KTRANS a KMAC do OBU daného vozidla a to buď datovou formou dle Subsetu-114, elektronickou poštou nebo písemně. Pokud žadatel nepotvrdí instalaci klíče KTRANS nebo KMAC na dané vozidlo, nebude klíč na straně traťové části aktivován. Pokud žadatel informuje správce KMC SŽDC elektronickou poštou nebo písemně, smí tak vždy učinit až po skutečném nahrání KTRANS a KMAC na vozidlo.
- 3.4.3 V případě, že domovským KMC pro OBU daného vozidla je jiné KMC:
- žadatel v žádosti musí uvést potřebné údaje o daném domovském KMC. V závislosti na tom, zda je se správcem daného KMC již navázán vztah nebo ne, musí žadatel poskytnout správci KMC SŽDC přiměřenou součinnost za účelem navázání spolupráce s jiným KMC, v opačném případě nemusí být klíče vydány;
 - správce KMC SŽDC nebo správce jiného domovského KMC vydá klíč KMAC. O tom, kdo generuje klíče, rozhoduje žadatel nebo ponechá rozhodnutí na dohodě správců KMC;
 - klíč KMAC je mezi správci KMC předáván zásadně datovou komunikací dle Subsetu-038;
 - domovské KMC musí správci KMC SŽDC potvrdit instalaci klíče do OBU daného vozidla, do té doby nebude klíč na straně traťové části aktivován.
- 3.5 Správce KMC SŽDC si vyhrazuje právo na vygenerování klíče KMAC pět pracovních dnů, jestliže je domovským KMC. Jestliže není, závisí doba rovněž na správci jiného KMC.

4 PODMÍNKY AKTIVACE A INSTALACE KLÍČŮ NA DANÉ ETCS ENTITY

- 4.1 Správce KMC SŽDC nikterak neodpovídá a nenese náklady za fyzickou instalaci klíčů do OBU daného vozidla. Způsob instalace klíčů do OBU daného vozidla si zajistí žadatel dle postupu stanoveného výrobcem nebo dodavatelem OBU.
- 4.2 Klíče KMAC se vydávají s platností na 10 let (dlouhodobá aktivace). Pokud se blíží vypršení časové platnosti klíče, musí žadatel včas požádat o vydání nového klíče.
- 4.3 Klíče KTRANS vydávané pro OBU jejichž domovským KMC je KMC SŽDC nemají časové omezení. Správce KMC SŽDC si však vyhrazuje právo je v případě nutnosti změnit.
- 4.4 Správce KMC SŽDC si vyhrazuje právo na možnost zneplatnění šifrovacích klíčů v RBC v případě, že by došlo k prolomení nebo byla známa akutní hrozba prolomení stávajících šifrovacích klíčů.
- 4.5 Podmínkou pro dlouhodobou aktivaci klíče KMAC na straně RBC je úspěšné provedení testů kompatibility dle vnitřního předpisu SŽDC PPD-2/2018 a Opatření k provádění posuzování shody mobilní a traťové části systému ETCS vydaného DÚ ČR. Úspěšné provedení testů kompatibility musí žadatel doložit. Neprovedení testů kompatibility sice nebrání vydání klíčů, ale brání jejich dlouhodobé aktivaci na straně traťové části ETCS.
- 4.6 Pokud chce žadatel dočasně aktivovat klíč na straně RBC i bez provedených testů kompatibility, musí o to požádat a specifikovat pro jaké časové období, pro jaké úseky (oblast RBC) a za jakým účelem chce klíče KMAC aktivovat. Správce KMC SŽDC oprávněnost posoudí, projedná s dotčenými útvary SŽDC a sdělí žadateli rozhodnutí.

- 4.7 Správce KMC SŽDC může omezit platnost klíčů na některé úseky vybavené traťovou částí systému ETCS, pokud na některých úsecích nebyla jednoznačně prokázána vzájemná kompatibilita mezi mobilní a traťovou částí systému ETCS.
- 4.8 Správce KMC SŽDC si vyhrazuje na aktivaci nebo nahrání klíčů do RBC pět pracovních dnů ode dne potvrzení instalace klíče KMAC do OBU daného vozidla. Tato lhůta neplatí pro případná RBC, která nejsou ve vlastnictví státu a SŽDC s nimi nemá právo hospodařit.
- 4.9 Pokud je proces přidělení šifrovacích klíčů úspěšný a klíče jsou nahrány do příslušných RBC, informuje správce KMC SŽDC žadatele podrobně o tom, pro jaká OBU daných vozidel (NID_ENGINE) a pro jaké traťové úseky (oblasti RBC) byly klíče vydány včetně jejich časové platnosti.
- 4.10 Žadatel je povinen informovat správce KMC SŽDC o každé změně OBU na daném vozidle, která by mohla mít souvislost s klíčovým managementem nebo může vyžadovat nové provedení testů kompatibility.
- 4.11 Na základě dohody s VUZ může KMC SŽDC vydat klíč KMAC i pro traťovou část ETCS úrovně 2 na zkušebním okruhu VUZ. Pokud má žadatel zájem o vydání klíče KMAC, musí doložit souhlas VUZ s udělením klíče pro konkrétní vozidlo.

5 ZÁVĚREČNÁ USTANOVENÍ

- 5.1 Se zněním tohoto Pokynu prokazatelně seznámte všechny zaměstnance uvedené v rozsahu znalostí.
- 5.2 Obsah tohoto Pokynu zařadte do náplně nejbližšího povinného školení zaměstnanců uvedených v rozsahu znalostí.
- 5.3 Pokyn je vydán pouze v elektronické podobě.
- 5.4 Pokyn nabývá platnosti dnem podpisu.
- 5.5 Pokyn nabývá účinnosti dne DD. MM. 2018.

SOUVISEJÍCÍ DOKUMENTY

SŽDC PPD-2/2018 Pokyn provozovatele dráhy pro zajištění plynulé a bezpečné drážní dopravy – Testy kompatibility palubních a traťových částí systému ERTMS/ETCS úrovně 2

PŘÍLOHY

Příloha A (normativní) Žádost o vydání šifrovacích klíčů pro komunikaci v systému ETCS

Příloha A (normativní)**Žádost o vydání šifrovacích klíčů pro komunikaci v systému ETCS****1. Identifikační údaje žadatele**

Obchodní firma (název)
 IČ / DIČ /
 Sídlo
 Ulice Č.p./Č. o. PSČ Město Země
 Kontaktní osoba e-mail..... tel./mob.

2. Identifikační údaje vozidel a zařízení

UIC číslo vozidla	Výrobní číslo OBU	Identifikační číslo OBU (NID_ENGINE)	Systémová verze ETCS OBU	Výrobce OBU

3. Stanovení domovského KMC

- ☐ domovským KMC daných OBU je KMC SŽDC
☐ uvedená OBU nemají přiděleno žádné domovské KMC, žádáme, aby se jím stalo KMC SŽDC
☐ domovským KMC je jiné KMC než KMC SŽDC: ID KMC
 Správce daného KMC Kontaktní osoba

4. Testy kompatibility daného typu OBU (systémová verze + výrobce)

- ☐ neprovedeny – žádáme o dočasné přidělení klíčů: od do
 za účelem:
☐ provedení jednorázových testovacích jízd s přijmutím zvláštních opatření,
☐ provedení testů kompatibility;
 Pozn. V případě, že žadatel následně doloží protokol (doklad) o úspěšném absolvování testů kompatibility, tak budou šifrovací klíče pro dané OBU automaticky aktivovány na deset let a není potřeba znovu žádost o vydání šifrovacích klíčů.
☐ provedeny pro celou síť SŽDC (nutno doložit k žádosti);
☐ provedeny pro určité traťové úseky (nutno doložit k žádosti).

5. Žádáme o přidělení šifrovacích klíčů pro:

- ☐ všechny tratě vybavené traťovou částí ETCS úrovně 2 a provozované SŽDC,
☐ zkušební okruh VUZ,
☐ pro určité traťové úseky (oblasti), specifikujte jaké:

.....

