Załącznik do uchwały Nr 83/2021
Zarządu PKP Polskie Linie Kolejowe S.A.
z dnia 23 lutego 2021 r.

PKP POLSKIE LINIE KOLEJOWE S.A.

Zarządca narodowej sieci linii kolejowych

Regulamin wydawania kluczy kryptograficznych do urządzeń ERTMS/ETCS poziomu 2

Ie-125

Warszawa, 2021

Właściciel: PKP Polskie Linie Kolejowe S.A.

Wydawca: PKP Polskie Linie Kolejowe S.A. Centrala
Biuro Rozwoju i Standaryzacji Technicznej
Materiał opracowany przez: Biuro Automatyki i Telekomunikacji
ul. Targowa 74, 03 – 734 Warszawa
tel. (22) 473-26-14
www.plk-sa.pl, e-mail: ist@plk-sa.pl

Spis treści

§ 1.

Cel i zakres dokumentu

1. Dokument opisuje proces wydawania kluczy kryptograficznych do urządzeń pokładowych systemu ERTMS/ETCS poziomu 2.
2. Dokument stanowi dopełnienie warstwy technicznej procesu zarządzania kluczami, która jest opisana w specyfikacji systemu ERTMS/ETCS, o aspekty proceduralne i organizacyjne obowiązujące w PKP Polskich Liniach Kolejowych S.A. takie jak:
   1) sposób wnioskowania o wydanie kluczy kryptograficznych;
   2) terminy realizacji poszczególnych czynności w procesie zarządzania kluczami;
   3) politykę w zakresie zarządzania terminami ważności kluczy;
   4) sposoby postępowania w przypadku zagrożenia bezpieczeństwa.

§ 2.

Podstawowe pojęcia i skróty

1. Określenia i skróty użyte w niniejszym dokumencie oznaczają:
   1) **Bezpieczeństwo** – stan, w którym zagwarantowane są poufność, autentyczność, dostępność i integralność kluczy kryptograficznych;
   2) **Biuro Automatyki i Telekomunikacji** – komórka organizacyjna Centrali PKP Polskich Linii Kolejowych S.A. merytorycznie odpowiedzialna za zarządzanie kluczami dla systemu ERTMS/ETCS. Dane kontaktowe:

      PKP Polskie Linie Kolejowe S.A.
      Biuro Automatyki i Telekomunikacji
      ul. Targowa 74
      03-734 Warszawa
      e-mail: iat@plk-sa.pl
   3) **Centrum Zarządzania Kluczami, CZK** – KMC PKP Polskich Linii Kolejowych S.A. wraz z personelem je obsługującym;
   4) **Dni robocze** – dni tygodnia od poniedziałku do piątku, z wyłączeniem dni ustawowo wolnych od pracy oraz dni wolnych od pracy obowiązujących w Centrali Spółki PKP Polskie Linie Kolejowe S.A.;
   5) **ERTMS** – Europejski System Zarządzania Ruchem Kolejowym (ang. *European Rail Traffic Management System*), obejmujący Europejski System Sterowania Pociągiem (ERTMS/ETCS) i Globalny System Kolejowej Radiokomunikacji Ruchomej (ERTMS/GSM-R);
   6) **ETCS (ERTMS/ETCS)** (ang. *European Train Control System*) – Europejski System Sterowania Pociągiem – system umożliwiający kontrolę prowadzenia pociągu przez

maszynistę, stanowiący część składową Europejskiego Systemu Zarządzania Ruchem Kolejowym (ERTMS);

7) **Interfejs wymiany kluczy** – standard techniczny, według którego odbywa się wymiana kluczy kryptograficznych, opisujący w szczególności struktury wiadomości zawierających polecenia operacji na kluczach, wiadomości zwrotnych, jak również formaty plików, do których wiadomości te są zapisywane; interfejs uważa się za interoperacyjny, jeżeli jego specyfikacja zawarta jest w którymkolwiek z obowiązujących wykazów specyfikacji obowiązkowych uwzględnionych w Załączniku A do TSI „Sterowanie" zgodnie z Rozporządzeniem Komisji (UE) 2016/919 z dnia 27 maja 2016 r. w sprawie technicznej specyfikacji interoperacyjności w zakresie podsystemów „Sterowanie" systemu kolei w Unii Europejskiej (Dz.U.UE.L.2016.158.1) [2];
8) **K-KMC –** klucz transportowy używany w celu ochrony kluczy uwierzytelniających KMAC w procesie wymiany informacji pomiędzy różnymi centrami zarządzania kluczami;
9) **Klucz kryptograficzny** – ciąg danych umożliwiający wykonanie określonych czynności kryptograficznych, m.in. takich jak: szyfrowanie, deszyfrowanie, obliczanie sum kontrolnych; w odniesieniu do niniejszego dokumentu kluczami kryptograficznymi są: klucze uwierzytelniające i klucze transportowe;
10) **Klucz transportowy** – KTRANS lub K-KMC;
11) **Klucz uwierzytelniający, KMAC** – klucz używany w procesie zestawiania połączeń między dwoma Urządzeniami ETCS z wykorzystaniem protokołu Euroradio;
12) **KMC** (ang. *Key Management Centre*) – interoperacyjny podmiot realizujący funkcje zarządzania kluczami w rozumieniu specyfikacji systemu ERTMS/ETCS;
13) **KMC PLK** – KMC PKP Polskich Linii Kolejowych S.A.
14) **KTRANS** – klucz transportowy używany w celu ochrony kluczy uwierzytelniających KMAC w procesie wymiany informacji pomiędzy KMC a Urządzeniami ETCS;
15) **Koordynator Wnioskodawcy, Koordynator** – osoba wskazana przez Wnioskodawcę jako kontakt w procesie wydawania kluczy kryptograficznych;
16) **Macierzyste KMC** – KMC, z którym dana jednostka ETCS komunikuje się w procesie zarządzania kluczami, tj. od którego otrzymuje polecenia operacji na kluczach i do którego wysyła meldunki o statusie wykonania tych operacji;
17) **OBU** – jednostka pokładowa (ang. *On-Board Unit*), urządzenia pokładowe systemu ERTMS/ETCS;
18) **Operacje na kluczach** – w szczególności: dodawanie, usuwanie bądź aktualizowanie kluczy kryptograficznych;

19) **Podmiot współpracujący** – niebędący Wnioskodawcą podmiot zaangażowany w proces zarządzania kluczami kryptograficznymi po stronie Wnioskodawcy, np. podmiot realizujący na zlecenie Użytkownika kluczy fizyczną instalację kluczy w urządzeniach pokładowych ETCS;
20) **RBC** – Centrum Sterowania Radiowego (ang. *Radio Block Centre*) – scentralizowana jednostka bezpieczna, sterująca następstwem pociągów w systemie ERTMS/ETCS poziom 2; jednostka przytorowa ETCS;
21) **Urządzenia ETCS** – OBU lub RBC;
22) **Użytkownik kluczy** – przewoźnik kolejowy / dysponent (w rozumieniu Ustawy z dnia 28 marca 2003 r. o transporcie kolejowym (Dz.U. z 2020 r. poz. 1043 z późn. zm.) [1]), eksploatujący bądź dysponujący pojazdami kolejowymi wyposażonymi w urządzenia pokładowe ETCS, dla których przeznaczone są klucze kryptograficzne wydawane przez CZK;
23) **Wnioskodawca** – podmiot uprawniony do występowania do CZK z wnioskami o wydanie kluczy kryptograficznych do urządzeń ERTMS/ETCS poziom 2;
24) **Zaufany adres e-mail** – adres e-mail wskazany przez Wnioskodawcę, przy użyciu którego, z jego strony, odbywać się będzie komunikacja z CZK, w szczególności składanie wniosków o wydanie kluczy.
25) **Zewnętrzne centrum zarządzania kluczami** – podmiot zarządzający kluczami, nieznajdujący się w strukturach PKP Polskich Linii Kolejowych S.A.

§ 3.
Komunikacja z CZK i wyznaczanie Koordynatorów

1. Użytkownik kluczy może wyznaczyć w swojej organizacji maksymalnie dwie osoby pełniące funkcję Koordynatorów, podając ich zaufane adresy e-mail oraz numery telefonów. Wyznaczenie odbywa się poprzez przesłanie podpisanego przez odpowiednio umocowaną osobę w organizacji Użytkownika kluczy formularza stanowiącego **Załącznik nr 1**:
   1) pocztą tradycyjną, na adres wskazany w § 2 ust. 1 pkt 2),
      lub
   2) pocztą elektroniczną, na adres e-mail wskazany § 2 ust. 1 pkt 2) – jeżeli dokument podpisano przy użyciu kwalifikowanego podpisu elektronicznego.
2. W przypadku, gdy Użytkownik kluczy, dla całości lub części swojej floty korzysta z usług podmiotu trzeciego w zakresie zarządzania kluczami kryptograficznymi ETCS, dopuszcza się, aby w jego imieniu z wnioskiem o wydanie kluczy występowała organizacja macierzystego KMC właściwego dla danej jednostki OBU. W takim przypadku Użytkownik kluczy powinien wydać administratorowi tego KMC imienne upoważnienie do

komunikowania się z CZK w swoim imieniu wraz ze wskazaniem identyfikatorów ETCS ID (NID_ENGINE) jednostek OBU, dla których jest on uprawniony do występowania do PKP Polskich Linii Kolejowych S.A. o wydanie kluczy. Wydanie upoważnienia odbywa się poprzez przesłanie podpisanego przez odpowiednio umocowaną osobę w organizacji Użytkownika kluczy formularza stanowiącego **Załącznik nr 1a**:

1) pocztą tradycyjną, na adres wskazany w § 2 ust. 1 pkt 2),
   lub
2) pocztą elektroniczną, na adres e-mail wskazany § 2 ust. 1 pkt 2) – jeżeli dokument podpisano przy użyciu kwalifikowanego podpisu elektronicznego.

Wskazany administrator macierzystego KMC pełni wówczas rolę Koordynatora Wnioskodawcy.

3. Przed przesłaniem formularza Użytkownik kluczy zobowiązany jest zapoznać wszystkie osoby wskazane w formularzu z treścią klauzuli informacyjnej administratora danych stanowiącą **Załącznik nr 2** do niniejszej instrukcji.
4. Każda zmiana Koordynatora lub jego danych kontaktowych powinna być niezwłocznie zgłoszona pisemnie do Biura Automatyki i Telekomunikacji, przy zachowaniu formy i trybu zgłoszenia zgodnych z ust. 1.
5. Komunikacja e-mail ze strony CZK odbywać się będzie za pomocą adresu e-mail: kmc.etcs@plk-sa.pl.

§ 4.
Role w procesie

1. CZK odpowiada za:
   1) przyjmowanie i weryfikowanie wniosków o wydanie kluczy kryptograficznych;
   2) przygotowywanie plików kluczy kryptograficznych i przekazywanie ich do Koordynatora;
   3) nadzór nad instalacją kluczy w RBC.
2. Koordynator Wnioskodawcy odpowiada za:
   1) przygotowywanie i składanie wniosków o wydanie kluczy kryptograficznych;
   2) odebranie kluczy przekazanych przez CZK;
   3) nadzór nad bezpieczeństwem otrzymanych plików z kluczami.

§ 5.

Wnioskowanie o wydanie kluczy

1. Wnioskodawcą w procesie wydawania kluczy może być Użytkownik kluczy.
2. Wnioskodawcą może być również zewnętrzne centrum zarządzania kluczami, z zastrzeżeniem § 3 ust. 2.
3. Wnioskodawca występuje do CZK o wydanie kluczy kryptograficznych dla OBU, zgodnie z wzorem wniosku, który stanowi **Załącznik nr 3** do niniejszego dokumentu. Wniosek należy przesłać na adres wskazany w § 3 ust. 5 (do wiadomości: iat@plk-sa.pl) w wersji edytowalnej (plik *.xlsx), oraz w postaci podpisanego skanu bądź pliku opatrzonego kwalifikowanym podpisem elektronicznym (*.pdf).
4. Wniosek, oprócz danych Wnioskodawcy, powinien zawierać:
   1) dane identyfikujące pojazd:
      a) nazwa producenta,
      b) serię i nr fabryczny,
      c) europejski numer pojazdu (EVN);
   2) dane charakteryzujące urządzenia pokładowe ETCS:
      a) nazwę producenta,
      b) identyfikator NID_ENGINE;
   3) informację o przeznaczeniu kluczy (na potrzeby testów czy na potrzeby prowadzenia komercyjnych przejazdów pociągów po liniach kolejowych zarządzanych przez PKP Polskie Linie Kolejowe S.A.);
   4) oczekiwany okres ważności kluczy (w przypadku wydania kluczy na potrzeby testów – maksymalnie 6 miesięcy);
   5) listę RBC, dla których mają być ważne klucze*;
   6) dane macierzystego KMC jednostek ETCS, których dotyczy wniosek, w szczególności jego identyfikator ETCS ID, jeżeli nie jest to KMC PLK;
   7) informację, jaki interfejs wymiany kluczy ma być zastosowany.

   Wszelkie inne informacje istotne z punktu widzenia zarządzania kluczami, należy podać w polu „Informacje dodatkowe”.
5. CZK w terminie 3 dni roboczych od otrzymania wniosku dokona weryfikacji jego poprawności i przekaże do Koordynatora informację o akceptacji lub konieczności jego uzupełnienia.
6. Zestawy kluczy w RBC aktualizowane są w cyklu miesięcznym, tj. aktywacja nowych kluczy będzie następować od pierwszego dnia miesiąca kalendarzowego.

* Wykaz RBC, dla których aktualnie możliwe jest uzyskanie kluczy kryptograficznych, dostępny jest w Biurze Automatyki i Telekomunikacji Centrali PKP Polskich Linii Kolejowych S.A.

7. Aby klucze, których dotyczy wniosek, zostały ujęte w danej aktualizacji, kompletny wniosek o wydanie kluczy powinien zostać złożony najpóźniej 15 dnia miesiąca poprzedzającego aktualizację. W innym przypadku klucze zostaną ujęte w kolejnej aktualizacji.
8. Przekazanie kluczy do Koordynatora odbywać się będzie nie później niż na 1 tydzień przed przewidywaną datą aktualizacji kluczy w RBC, o której mowa w ust. 6.

§ 6.
Interfejsy wymiany kluczy

1. CZK obecnie wykorzystuje wyłącznie zarządzanie kluczami kryptograficznymi „off-line". Polecenia operacji na kluczach zapisywane są do plików w sposób zgodny z jednym z poniższych interoperacyjnych interfejsów wymiany kluczy:
   1) UNISIG Subset-038 issue 2.3.0 / 3.0.0 / 3.1.0;
   2) UNISIG Subset-114 issue 1.0.0 / 1.1.0, metoda obsługi kluczy „Single";
   3) UNISIG Subset-114 issue 1.0.0 / 1.1.0, metoda obsługi kluczy „All".

   Wsparcie dla innych interfejsów wymiany kluczy (w tym interfejsów nieinteroperacyjnych) nie jest gwarantowane.
2. Jeżeli dany interfejs wymiany kluczy zakłada wykorzystanie wiadomości zwrotnych zawierających meldunki o statusie przetwarzania poleceń wykonania operacji na kluczach, Koordynator zobowiązany jest bez zbędnej zwłoki przekazywać takie wiadomości do CZK. Nieprzekazanie wiadomości zwrotnych może stanowić podstawę do nieaktywowania klucza w RBC.

§ 7.
Przekazywanie kluczy

1. Pliki kluczy kryptograficznych mogą być przekazane Koordynatorowi przy użyciu:
   1) nośników fizycznych,
   2) poczty elektronicznej,
   3) stosowanych w PKP Polskich Liniach Kolejowych S.A. narzędzi do bezpiecznej wymiany plików.
2. CZK, biorąc pod uwagę specyfikę zastosowanego interfejsu wymiany kluczy, dobiera sposób przekazania plików kluczy oraz ich zabezpieczenia. Pliki zawierające klucze transportowe są przekazywane odrębną drogą niż pozostałe pliki.
3. Jeżeli w procesie przekazywania plików kluczy zostały wykorzystane hasła szyfrowania, Koordynator po otrzymaniu wiadomości kontaktuje się telefonicznie z CZK w celu uzyskania hasła.

4. Klucze wydawane są z nieograniczonym terminem ważności (z zastrzeżeniem ust. 5 oraz z wyłączeniem kluczy testowych, o których mowa w § 5 ust. 4 pkt 4).
5. Jeżeli polityka zarządzania kluczami w organizacji Użytkownika kluczy uwzględnia wykorzystanie kluczy o ograniczonym terminie ważności, informację o tym fakcie należy zawrzeć we wniosku. W takim przypadku Wnioskodawca jest odpowiedzialny za nadzór nad okresami ważności kluczy oraz terminowe wnioskowanie o wymianę kluczy bądź o przedłużenie ich ważności.

§ 8.
Modyfikacje i usuwanie kluczy

1. Klucze można modyfikować poprzez:
   1) zmianę zakresu powiązań OBU-RBC;
   2) przedłużenie terminu ważności;
   3) zmianę z terminowych na bezterminowe;
   4) zmianę z bezterminowych na terminowe.
2. W przypadku konieczności modyfikacji kluczy, Wnioskodawca składa wniosek zgodnie z formularzem stanowiącym Załącznik nr 3, podając wszelkie dane umożliwiające CZK przygotowanie zmodyfikowanych plików kluczy.
3. Usunięcie kluczy może być inicjowane przez:
   1) Użytkownika kluczy;
   2) macierzyste KMC jednostki, dla której mają być usunięte klucze (jeżeli jest inne niż KMC PLK);
   3) w uzasadnionych przypadkach – CZK.
4. W przypadkach, o których mowa w ust. 3 pkt 1) i 2), Wnioskodawca składa wniosek zgodnie z formularzem stanowiącym Załącznik nr 3, w polu „Informacje dodatkowe” wpisując „Usunięcie kluczy”. Jeżeli zastosowany interfejs wymiany kluczy wymaga wykorzystania meldunków bądź poleceń usunięcia kluczy, odpowiednie pliki są przesyłane pomiędzy CZK, a Koordynatorem.
5. O potrzebie usunięcia kluczy w związku z okolicznościami, o których mowa w ust. 3 pkt 3), CZK informuje Wnioskodawcę z co najmniej 1-miesięcznym wyprzedzeniem. Wyjątkiem są sytuacje ujawnienia klucza bądź inne sytuacje zidentyfikowane jako mające bezpośredni wpływ na bezpieczeństwo ruchu kolejowego – w takim przypadku klucze powinny zostać usunięte natychmiast.
6. Jeżeli zastosowany interfejs wymiany kluczy wymaga wykorzystania meldunków bądź poleceń usunięcia kluczy, odpowiednie pliki są przesyłane pomiędzy CZK a Koordynatorem. Koordynator zobowiązany jest do nadzoru nad niezwłocznym usunięciem

kluczy we wskazanych urządzeniach ETCS. Jeżeli zachodzi potrzeba dalszej eksploatacji urządzeń, dla których klucze zostały usunięte, CZK prześle nowy zestaw kluczy.

§ 9.
Bezpieczeństwo kluczy

1. Od momentu otrzymania kluczy od CZK, Koordynator odpowiedzialny jest za ich bezpieczne przetwarzanie po stronie Wnioskodawcy oraz Podmiotów współpracujących. Wnioskodawca powinien wdrożyć wszelkie możliwe środki (techniczne, proceduralne, organizacyjne) zmierzające do zapewnienia bezpieczeństwa danych związanych z zarządzaniem kluczami.
2. Wewnątrz organizacji Wnioskodawcy i Podmiotów współpracujących niedopuszczalne jest:
   1) przesyłanie plików kluczy transportowych pocztą elektroniczną w postaci niezaszyfrowanej bądź w postaci umożliwiającej łatwe odszyfrowanie (np. wpisując hasło szyfrowania w treść wiadomości bądź z zastosowaniem krótkich, nieskomplikowanych haseł);
   2) przesyłanie pocztą elektroniczną jednocześnie plików zawierających klucze uwierzytelniające i klucze transportowe;
   3) udostępnianie plików kluczy nadmiernej liczbie osób bądź osobom niebiorącym udziału w procesie przetwarzania informacji związanych z kluczami;
   4) instalowanie kluczy w jednostkach ETCS, dla których dany klucz nie jest przeznaczony;
   5) ingerowanie w zawartość plików kluczy.
3. Pliki kluczy, po ich wyegzekwowaniu powinny zostać trwale usunięte z systemu informatycznego Wnioskodawcy i Podmiotów współpracujących.
4. W przypadku zaistnienia podejrzenia, że którykolwiek klucz został ujawniony, należy niezwłocznie zgłosić ten fakt do CZK. CZK w zależności od oceny sytuacji podejmuje stosowne środki zmierzające do wyeliminowania zagrożenia związanego z ujawnieniem klucza. Koordynator zobowiązany jest do ścisłej współpracy z CZK, w szczególności do nadzoru nad niezwłocznym wycofaniem z użytkowania wskazanych przez CZK kluczy.
5. Wydanie klucza nie stanowi potwierdzenia, że konkretny pojazd wraz z pokładowym systemem ERTMS/ETCS posiada niezbędne zezwolenia umożliwiające prowadzenie pojazdu z wykorzystaniem systemu ERTMS/ETCS na danej linii. Ocena możliwości bezpiecznej i zgodnej z przepisami krajowymi eksploatacji pojazdu wraz z zainstalowanym na nim systemem pokładowym ERTMS/ETCS, należy do przewoźnika kolejowego.

§ 10.

Dokumenty związane

[1] Ustawa z dnia 28 marca 2003 r. o transporcie kolejowym (Dz.U. z 2020 r. poz. 1043 z późn. zm.)

[2] Rozporządzenie Komisji (UE) 2016/919 z dnia 27 maja 2016 r. w sprawie technicznej specyfikacji interoperacyjności w zakresie podsystemów Sterowanie systemu kolei w Unii Europejskiej (Dz.U.UE.L.2016.158.1)

[3] UNISIG Subset-038 Off-line Key Management FIS issue 2.3.0

[4] UNISIG Subset-038 Off-line Key Management FIS issue 3.0.0

[5] UNISIG Subset-038 Off-line Key Management FIS issue 3.1.0

[6] UNISIG Subset-114 KMC-ETCS Entity Off-line KM FIS issue 1.0.0

[7] UNISIG Subset-114 KMC-ETCS Entity Off-line KM FIS issue 1.1.0

Tabela zmian

Lp. zmiany	Przepis wewnętrzny, którym zmiana została wprowadzona (rodzaj, nazwa i tytuł)	Jednostki redakcyjne w obrębie których wprowadzono zmiany	Data wejścia zmiany w życie	Biuletyn PKP Polskie Linie Kolejowe S.A., w którym zmiana została opublikowana (Nr/poz./rok)

Załącznik nr 1 - wzór formularza dot. wyznaczenia Koordynatorów

....
Miejscowość, data

.....

.....

.....
Dane Wnioskodawcy

PKP Polskie Linie Kolejowe S.A.
Biuro Automatyki i Telekomunikacji
ul. Targowa 74
03-734 Warszawa

Działając w trybie § 3 ust. 1 *Regulaminu wydawania kluczy kryptograficznych do urządzeń ERTMS/ETCS poziomu 2 Ie-125*, wyznaczam na Koordynatora/Koordynatorów* następującą osobę / następujące osoby*:

Lp.	Imię i nazwisko	adres e-mail	nr telefonu

.....
Podpis osoby reprezentującej Wnioskodawcę

* Niepotrzebne skreślić

Załącznik nr 1a – wzór upoważnienia dla podmiotu trzeciego do występowania o wydanie kluczy kryptograficznych

....
Miejscowość, data

.....

.....

.....
Dane Wnioskodawcy

PKP Polskie Linie Kolejowe S.A.
Biuro Automatyki i Telekomunikacji
ul. Targowa 74
03-734 Warszawa

Działając w trybie § 3 ust. 2 *Regulaminu wydawania kluczy kryptograficznych do urządzeń ERTMS/ETCS poziomu 2 Ie-125*, do występowania o wydanie kluczy kryptograficznych ETCS dla poniższych jednostek:

Lp.	Typ i nr pojazdu	EVN	NID_ENGINE

W razie potrzeby dodać kolejne wiersze do tabeli

upoważniam ich macierzyste KMC o identyfikatorze *ETCS ID w postaci szesnastkowej*, którego administratorem jest *imię, nazwisko, adres e-mail i nr telefonu administratora KMC*.

.....
Podpis osoby reprezentującej Użytkownika kluczy

Załącznik nr 2 – obowiązek informacyjny realizowany przez PKP Polskie Linie Kolejowe S.A. wobec osób zgłaszanych jako Koordynatorzy oraz osób reprezentujących we wniosku Wnioskodawcę

Zgodnie art. 13 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 2016 r., str. 1-88), zwanego dalej RODO, informuje się wymienione w tytule osoby, że:

1) Administratorem danych jest PKP Polskie Linie Kolejowe Spółka Akcyjna (dalej „Spółka"), z siedzibą pod adresem: 03-734, Warszawa, ul. Targowa 74;
2) w Spółce, funkcjonuje adres e-mail: iod.plk@plk-sa.pl Inspektora Ochrony Danych w PKP Polskie Linie Kolejowe S.A., udostępniony osobom, których dane osobowe są przetwarzane przez Spółkę;
3) dane osobowe przetwarzane będą w celu realizacji procesu zarządzania kluczami kryptograficznymi na potrzeby systemu ERTMS/ETCS poziomu 2
4) podstawą prawną przetwarzania danych osobowych przez Spółkę jest prawny interes Spółki mający na celu zapewnienie bezpieczeństwa procesu zarządzania kluczami kryptograficznymi, zgodnie z Regulaminem wydawania kluczy kryptograficznych do urządzeń ERTMS/ETCS poziomu 2 Ie-125 tj. art. 6 ust. 1 lit. f RODO;
5) dane osobowe nie będą udostępniane innym odbiorcom, chyba że przepisy szczególne stanowią inaczej;
6) dane osobowe nie będą przekazane do państwa nienależącego do Europejskiego Obszaru Gospodarczego (państwa trzeciego) lub organizacji międzynarodowej w rozumieniu RODO
7) dane osobowe będą przetwarzane we wskazanym celu **przez okres istnienia relacji umownych z Wnioskodawcą, który składa wniosek, a po tym okresie dla celów i przez czas oraz w zakresie wymaganym przez szczególne przepisy prawa**;
8) osoba, której dane dotyczą ma prawo do żądania dostępu do dotyczących jej danych osobowych oraz ich sprostowania, usunięcia lub ograniczenia przetwarzania, prawo do wniesienia sprzeciwu wobec przetwarzania, a także prawo do przenoszenia danych;
9) osoba, której dane dotyczą ma prawo do wniesienia skargi do organu nadzorczego, tzn. Prezesa Urzędu Ochrony Danych Osobowych;
10) Spółka nie będzie przeprowadzać zautomatyzowanego podejmowania decyzji, w tym profilowania na podstawie podanych we wniosku danych osobowych.

Załącznik nr 3 – wzór wniosku o wydanie kluczy

PKP POLSKIE LINIE KOLEJOWE S.A.

Załącznik nr 3
do Regulaminu wydawania kluczy kryptograficznych
do urządzeń ERTMS/ETCS poziom 2 Ie-125

Nr wniosku:
(wypełnia Operator CZK)

Wypełnia Wnioskodawca:

Data wypełnienia formularza:
Przewidywana data aktywacji kluczy:

Dane Wnioskodawcy:

Nazwa spółki:
Adres:

Dane Koordynatora:

Imię i nazwisko:
Stanowisko służbowe:
Adres e-mail:
Numer telefonu:

Dane do wygenerowania kluczy:

Lp.	Typ i numer pojazdu	EVN	Identyfikator ETCS OBU	Instalacja testowa?	Okres ważności kluczy	RBC
	np. EP09-001		*NID_ENGINE (dziesiętny)*		*w przypadku instalacji testowych*	*dla jakich RBC mają być ważne klucze*
1						

Macierzyste KMC:
Interfejs zarządzania kluczami:
ETCS ID macierzystego KMC (format szesnastkowy):

Informacje dodatkowe:

.....
podpis

Edytowalną oraz podpisaną (skan bądź kwalifikowany podpis elektroniczny) wersję wniosku należy przesłać na adres kmc.etcs@plk-sa.pl (DW: iat@plk-sa.pl)

(wypełnia Operator CZK)

Formularz wpłynął dnia:	Uwagi:
Klucze wygenerowano dnia:	
Klucze przesłano dnia:	
Klucze przekazano do (e-mail:)	Zgłoszenie obsługiwał (imię i nazwisko Operatora CZK):

.....
pieczęć i podpis Operatora CZK