Załącznik do uchwały Nr 1089/2018 Zarządu PKP Polskie Linie Kolejowe S.A. z dnia 27 grudnia 2018 r.

Regulamin wydawania kluczy kryptograficznych do urządzeń ERTMS/ETCS poziomu 2 le-125

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

Rozdział 1 Postanowienia ogólne

§ 1. Cel i zakres dokumentu

1. Dokument opisuje proces wydawania kluczy kryptograficznych do urządzeń pokładowych systemu ERTMS/ETCS poziomu 2.
2. W dokumencie opisano elementy procesu, na który składają się: złożenie wniosku o wydanie kluczy, weryfikacja wniosku, przygotowanie kluczy przez Operatora CZK i ich przekazanie do Wnioskodawcy.
3. Dodatkowo w dokumencie wskazano sposób postępowania w przypadku wycofania kluczy z użytkowania przez Wnioskodawcę oraz unieważnienia kluczy.

§ 2. Podstawowe pojęcia i skróty

Określenia i skróty użyte w niniejszym dokumencie oznaczają:

1) **Biuro Automatyki i Telekomunikacji** – komórka organizacyjna Centrali PKP Polskich Linii Kolejowych S.A., merytorycznie odpowiedzialna za zarządzanie kluczami dla systemu ERTMS/ETCS oraz systemem radiołączności GSM-R.
   Adres:
   PKP Polskie Linie Kolejowe S.A.
   Biuro Automatyki i Telekomunikacji
   ul. Targowa 74
   03-734 Warszawa
   e-mail: iat@plk-sa.pl
2) **CZK** – Centrum Zarządzania Kluczami – zespół w Biurze Automatyki i Telekomunikacji zajmujący się zarządzaniem kluczami w systemie ETCS;
3) **Dni robocze** - dni tygodnia od poniedziałku do piątku, z wyłączeniem dni ustawowo wolnych od pracy, obowiązujących w Rzeczypospolitej Polskiej;
4) **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);
5) **ETCS** (ang. European Train Control System) - Europejski System Sterowania Pociągiem;
6) **EVN** (ang. European Vehicle Number) – Europejski numer pojazdu;
7) **GSM-R** (ang. Global System for Mobile Communications for Railways) – Globalny System Kolejowej Radiokomunikacji Ruchomej;

8) **Klucz kryptograficzny** – blok danych służący do szyfrowania przesyłanych informacji, w szczególności jest to klucz uwierzytelniający (KMAC) i klucz transportowy (KTRANS);
9) **KMAC** – klucz uwierzytelniający połączenie między dwoma Urządzeniami ETCS;
10) **KTRANS** – klucz transportowy używany w celu ochrony kluczy uwierzytelniających KMAC w procesie przekazywania z CZK do Urządzenia ETCS;
11) **Koordynator** – osoba wskazana przez Wnioskodawcę jako kontakt w procesie wydawania kluczy kryptograficznych;
12) **OBU** – jednostka pokładowa (ang. On-Board Unit), urządzenia pokładowe systemu ERTMS/ETCS;
13) **Operator CZK** – osoba prowadząca w imieniu PLK proces wydawania kluczy kryptograficznych;
14) **PLK** – PKP Polskie Linie Kolejowe Spółka Akcyjna z siedzibą w Warszawie;
15) **RBC** – Centrum Sterowania Radiowego (ang. Radio Block Centre) – scentralizowana jednostka bezpieczna, sterująca następstwem pociągów w systemie ERTMS/ETCS poziom 2;
16) **Urządzenia ETCS** – OBU lub RBC;
17) **Wnioskodawca** – podmiot zainteresowany pozyskaniem kluczy kryptograficznych w celu użytkowania systemu ERTMS/ETCS poziom 2, będący właścicielem lub użytkownikiem trakcyjnego pojazdu kolejowego, w szczególności aplikant, z którym zawarto umowę o przydzielenie zdolności przepustowej lub przewoźnik kolejowy, z którym zawarto umowę o wykorzystanie zdolności przepustowej;
18) **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.

§ 3. Komunikacja

1. Wnioskodawca wyznacza imiennie maksymalnie dwie osoby pełniące funkcję Koordynatorów, podając ich zaufane adresy e-mail oraz numery telefonów. Wyznaczenie odbywa się poprzez przesłanie formularza stanowiącego **Załącznik nr 1**, pocztą tradycyjną oraz dodatkowo pocztą elektroniczną, na adresy wskazane w § 2 pkt 1. Przed przesłaniem formularza Wnioskodawca zobowiązany jest zapoznać wszystkie osoby wskazane w formularzu z treścią klauzuli informacyjnej administratora danych stanowiącą Załącznik nr 2 do niniejszej instrukcji.

2. Każda zmiana na stanowisku Koordynatora lub jego danych kontaktowych musi być niezwłocznie zgłoszona pisemnie do Biura Automatyki i Telekomunikacji, przy zachowaniu formy i trybu zgłoszenia zgodnych z ust. 1.
3. Komunikacja e-mail ze strony Operatora CZK będzie się odbywać za pomocą adresu e-mail: bok.ertms@plk-sa.pl.

Rozdział 2 Zarządzanie kluczami kryptograficznymi systemu ERTMS/ETCS poziomu 2

§ 4. Role w procesie

1. Operator CZK odpowiada za:
   1) generowanie kluczy KMAC dla RBC i OBU;
   2) przekazywanie kluczy KMAC oraz KTRANS dla urządzeń OBU do Koordynatora;
   3) przekazywanie kluczy KMAC dla RBC do odpowiednich służb PLK, odpowiedzialnych za instalację kluczy w urządzeniach przytorowych.
2. Koordynator odpowiada za:
   1) odebranie kluczy przekazanych przez Operatora CZK;
   2) nadzór nad instalacją kluczy w OBU;
   3) nadzór nad usunięciem plików z kluczami.

§ 5. Wnioskowanie o wydanie lub wycofanie kluczy

1. Wnioskodawca przez złożenie wniosku oświadcza, że jest/będzie właścicielem trakcyjnych pojazdów kolejowych wyposażonych w urządzenia pokładowe systemu ETCS poziom 2 (OBU) przewidzianych do współpracy z urządzeniami przytorowymi ETCS (RBC) z wykorzystaniem kluczy kryptograficznych używanych do uwierzytelniania sesji transmisyjnej.
2. Klucze kryptograficzne wydawane Wnioskodawcy umożliwią współpracę ze wskazanymi we wniosku RBC występującymi w sieci PLK.
3. Wnioskodawca występuje do Biura Automatyki i Telekomunikacji z wnioskiem o wydanie kluczy kryptograficznych dla OBU, zgodnie ze wzorem wniosku, który stanowi **Załącznik nr 3** do niniejszego dokumentu. Wniosek należy przesłać na adres wskazany w § 3 ust. 3 (do wiadomości: iat@plk-sa.pl) w wersji edytowalnej (plik *.xls/*.xlsx), oraz w postaci podpisanego skanu (*.pdf).
4. Wniosek musi zawierać dane Wnioskodawcy oraz:
   1) listę pojazdów wyposażonych w OBU, dla których wnioskuje się o wydanie kluczy, zawierającą:
      a) typ i numer pojazdu, numer EVN pojazdu, na którym OBU jest zainstalowane,
      b) identyfikator ETCS ID (NID_ENGINE) w postaci dziesiętnej,
      c) typ (producenta) OBU,
      d) listę RBC, dla których mają być ważne klucze;

2) przeznaczenie kluczy (na potrzeby testów czy na potrzeby prowadzenia przejazdów pociągów po liniach kolejowych zarządzanych przez PLK);
3) okres ważności kluczy (w przypadku wydania kluczy na potrzeby testów – maksymalnie 6 miesięcy).

Niektóre pola zawierają listę dostępnych wartości.

5. W przypadku konieczności usunięcia kluczy (np. na skutek zmiany właściciela pojazdu, złomowania pojazdu, deinstalacji OBU itp.), Wnioskodawca będzie przekazywał do Biura Automatyki i Telekomunikacji zestawienie OBU, dla których klucze powinny być wycofane. Należy podać dane wskazane w ust. 4 pkt 1.
6. Zestawienie, o którym mowa w ust. 5, powinno zostać przekazane do Biura Automatyki i Telekomunikacji nie później niż 1 miesiąc od zaistnienia okoliczności skutkującej koniecznością wycofania kluczy.
7. W przypadku, gdy niezbędna jest modyfikacja zestawu kluczy dla danego OBU (np. spowodowana zmianą listy RBC, zmianą typu eksploatacji lub upływem okresu ważności) – Wnioskodawca składa nowy wniosek z zakresem danych, o których mowa w ust. 4.
8. PLK będzie aktualizować zestawy kluczy w RBC w cyklu miesięcznym, tj. aktywacja nowych kluczy będzie następować od pierwszego dnia miesiąca kalendarzowego.
9. Aby wnioskowane klucze 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.
10. Operator CZK w terminie 3 dni roboczych od otrzymania wniosku dokona weryfikacji jego poprawności i przekaże do Koordynatora informację o akceptacji lub konieczności jego uzupełnienia.
11. Przekazanie kluczy do Koordynatora odbywać się będzie nie później niż na 1 tydzień przed przewidywaną datą aktualizacji kluczy w RBC.
12. Niedopuszczalne jest stosowanie kluczy na innym pojeździe niż ten, dla którego klucze zostały wydane.
13. PLK może w uzasadnionych przypadkach zarządzić wymianę kluczy KMAC i/lub KTRANS, informując o tym Wnioskodawców z co najmniej miesięcznym wyprzedzeniem.
14. Wnioskodawca może występować o wydanie kluczy dla pojazdów będących w fazie produkcji, wskazując podmiot produkujący pojazd. Wymiana kluczy dla pojazdów w tej fazie odbywa się również za pośrednictwem Koordynatora.

§ 6. Tworzenie/usuwanie kluczy

1. Operator CZK na podstawie otrzymanych wniosków generuje komplety kluczy KMAC dla kombinacji RBC-OBU wynikających z informacji zawartych we wniosku oraz wyposażenia linii.
2. W przypadku usuwania kluczy generowany jest nowy zestaw niezawierający kluczy usuwanych.
3. Należy posługiwać się nazwami pojazdów umożliwiającymi jednoznaczną identyfikację egzemplarza pojazdu, dla którego wydany jest klucz.
4. Nazwa pliku (lub katalogu plików) zawierającego klucze KMAC dla pojazdu powinna być tworzona wg wzorca:
   XXX_NNNNN-ZZZ_YYYYYYYY
   Gdzie:
   XXX – skrót nazwy Przewoźnika, do którego należy pojazd,
   NNNNNN-ZZZ – typ i numer pojazdu (możliwe dodanie litery a i b oznaczających kabinę),
   YYYYYYYY – 8 ostatnich cyfr numeru jednostki trakcyjnej (EVN).
   W szczególnych przypadkach, za obustronnym uzgodnieniem, format nazewnictwa plików/katalogów z kluczami może ulec zmianie.
5. Klucze KMAC przekazywane są w postaci zaszyfrowanej z użyciem klucza KTRANS.

§ 7. Przekazywanie i instalacja kluczy

1. Pliki z kluczami dla OBU (KMAC oraz KTRANS) przekazywane są przez Operatora CZK do Koordynatora.
2. Operator CZK dokonuje kompresji plików z kluczami do formatu pliku *.zip, z zastosowaniem hasła szyfrowania. Każde archiwum powinno być zabezpieczone innym hasłem.
3. Hasło szyfrowania dla pliku z kluczami powinno zawierać minimum 12 znaków (w tym duże i małe litery, cyfry oraz znaki specjalne).
4. Skompresowane i zaszyfrowane pliki z kluczami KMAC są wysyłane na zaufany adres e-mail Koordynatora.
5. Klucz KTRANS powinien być przekazywany odrębnymi środkami komunikacji – w tym celu zaleca się użycie nośników fizycznych (np. płyta CD, pamięć USB). Sposób dostarczenia klucza KTRANS będzie uzgodniony między Operatorem CZK a Koordynatorem.
6. Koordynator po otrzymaniu wiadomości kontaktuje się telefonicznie z Operatorem CZK i uzyskuje hasło szyfrowania pliku.

7. Po otwarciu archiwum Koordynator potwierdza Operatorowi CZK otrzymanie poprawnych plików.
8. Po przeprowadzeniu instalacji kluczy w OBU Koordynator dokonuje trwałego usunięcia z nośnika plików z kluczami KMAC, skasowania e-maili oraz wszystkich pośrednich plików, które powstały w trakcie procesu przekazywania i instalacji kluczy.
9. Zakończeniem procesu jest przekazanie przez Koordynatora do Operatora CZK informacji, w formie wiadomości elektronicznej e-mail, o poprawnej instalacji kluczy, wraz ze wskazaniem daty instalacji.
10. W przypadku nieprzewidzianych zdarzeń związanych z instalacją kluczy, należy tę informację przekazać do Operatora CZK.
11. Operator CZK usuwa pośrednie pliki oraz e-maile, które służyły do przekazania kluczy, zachowując wyłącznie pliki z kluczami w narzędziu dedykowanym do zarządzania kluczami.

§ 8. Bezpieczeństwo kluczy

1. Od momentu otrzymania kluczy od Operatora CZK, Koordynator odpowiedzialny jest za bezpieczne ich przetwarzanie po stronie Wnioskodawcy. W związku z tym, Wnioskodawca powinien wdrożyć wszelkie możliwe środki (techniczne, proceduralne, organizacyjne) zmierzające do zapewnienia bezpieczeństwa i integralności danych związanych z zarządzaniem kluczami.
2. Operator CZK, na każdym etapie procesu przekazywania kluczy, ma prawo do:
   1) dokonywania dodatkowej weryfikacji danych przekazywanych w ramach wymiany informacji między CZK a Wnioskodawcą;
   2) uzyskiwania informacji na temat przebiegu instalacji kluczy w urządzeniach pokładowych Wnioskodawcy.
3. W przypadku zaistnienia podejrzenia, że którykolwiek klucz został przejęty przez osobę niepowołaną i tym samym może zostać naruszona integralność systemu, należy dokonać usunięcia (wyłączenia z użycia) kluczy, które zostały ujawnione lub co do których istnieje podejrzenie, że mogły zostać ujawnione. Każdy taki przypadek powinien zostać niezwłocznie zgłoszony Operatorowi CZK.

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 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:
Oczekiwana data aktywacji kluczy:

Dane firmy:

Nazwa spółki:
Adres:

Dane koordynatora:

Imię i nazwisko:
Stanowisko służbowe:
Adres e-mail:
Numer telefonu: ◉ Komórkowy ○ Stacjonarny

Dane do wygenerowania kluczy:

Lp.	Typ i numer pojazdu	EVN	ETCS_ID	Typ OBU	Instalacja testowa?	Okres ważności kluczy	RBC
	np. EP09-001		NID_ENGINE		tak/nie	w przypadku instal. testowych	dla jakich RBC mają być ważne klucze
1							

Informacje dodatkowe:

podpis

Wypełniony wniosek należy wydrukować, podpisać, i przesłać skan oraz w wersji edytowalnej na adres bok.ertms@plk-sa.pl (do wiadomości: le@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