



<b>ZAMAWIAJĄCY:</b>  <b>Gmina Wrocław</b>	Rozbudowa narzędzi informatycznych umowa TXU/TXXI/256/224/2018 Dokumentacja powykonawcza	<b>Numer sygnatury</b> 5434/05/2022
---	--	--

## Dokumentacja powykonawcza

### Załącznik nr 10 Podłączenie sterowników sygnalizacji świetlnej

**Numer sygnatury**  
**5434/05/2022**

<b>Przygotowano dla:</b>	 <b>Gmina Wrocław</b> <b>50-141 Wrocław,</b> <b>pl. Nowy Targ 1/8</b> tel. (071) 777-70-00 <a href="http://www.wroclaw.pl">www.wroclaw.pl</a>
<b>Przedstawiciel Zamawiającego</b>	 Zarząd Dróg i Utrzymania Miasta <b>53-633 Wrocław, ul. Długa 49</b> <b>tel. 71/ 355 90 78</b>
<b>Nazwa Projektu:</b>	„Rozbudowa systemu zarządzania ruchem we Wrocławiu, w tym o nowe sygnalizacje świetlne, wyświetlacze pomocnicze ITS oraz aplikację mobilną” Część III: Rozbudowa narzędzi informatycznych Umowa: TXU/TXXI/256/224/2018
<b>Wersja:</b>	1.00
<b>Ostatnio zmodyfikowano:</b>	30-05-2022
<b>Autor:</b>	Mariusz Słonina, Kamil Bolek
<b>Wykonawca:</b>	<b>WASKO S.A.</b> ul. Berbeckiego 6, 44-100 Gliwice
<div>  <b>Fundusze Europejskie</b>  Program Regionalny </div> <div>  <b>Rzeczpospolita Polska</b> </div> <div>  <b>DOLNY ŚLĄSK</b> </div> <div> <b>Unia Europejska</b>  Europejski Fundusz Rozwoju Regionalnego  </div>	


<b>ZAMAWIAJĄCY:</b>  <b>Gmina Wrocław</b>	Rozbudowa narzędzi informatycznych umowa TXU/TXXI/256/224/2018 Dokumentacja powykonawcza	Numer sygnatury
		5434/05/2022

#### Metryka dokumentu

<b>Tytuł dokumentu:</b>	Dokumentacja powykonawcza Załącznik nr 10 Podłączenie sterowników sygnalizacji świetlnej		
<b>Nazwa Projektu:</b>	Rozbudowa systemu zarządzania ruchem we Wrocławiu, w tym o nowe sygnalizacje świetlne, wyświetlacze pomocnicze ITS oraz aplikację mobilną". Część III: Rozbudowa narzędzi informatycznych		
<b>Autor (rzy):</b>	Mariusz Słonina Kamil Bolek	<b>Numer wersji dokumentu:</b>	1.00
<b>Klauzula poufności:</b>	Nie	<b>Data utworzenia dokumentu:</b>	30.05.2022


#### Historia dokumentu

Nr wersji	Data wersji	Autor zmiany	Komentarz/Uwagi/Zakres zmian
1.00	30-05-2022	Mariusz Słonina Kamil Bolek	Utworzenie dokumentu

<p>ZAMAWIAJĄCY:</p>  <p><b>Gmina Wrocław</b></p>	<p>Rozbudowa narzędzi informatycznych umowa TXU/TXXI/256/224/2018 Dokumentacja powykonawcza</p>	<p>Numer sygnatury</p> <p>5434/05/2022</p>
---	---	--

## Spis treści

1	Zakres i cel dokumentacji .....	4
2	Zawartość dokumentu .....	4
3	Zasady ogólne podłączenia.....	4
4	Podłączenie do systemu ITS – zasady ogólne.....	6
4.1	Połączenie sieciowe .....	7
4.2	Opis pliku uwierzytelniającego .....	7
4.3	Hasła do plików uwierzytelniających .....	9
4.4	Operacje matematyczne i kryptograficzne .....	11
4.5	Pseudokod.....	15
5	Podłączenie do Modułu Nadawania Priorytetu – MNP.....	16
5.1	Autoryzacja MNP - opis wiadomości XYZ.....	16
5.2	Komunikacja i szyfrowanie MNP .....	18
5.3	Interfejs wymiany danych z pojazdów.....	19
5.4	Przesyłanie danych z pojazdu – zasady obsługi .....	23
6	Podłączenie do systemu sterowania ruchem Gertrude.....	30
6.1	Komunikacja GTR.....	30
6.2	Autoryzacja GTR - opis wiadomości XYZ .....	30
7	Dane konfiguracyjne .....	32
8	Terminy i wyrażenia użyte w dokumencie .....	32

<p>ZAMAWIAJĄCY:</p>  <p><b>Gmina Wrocław</b></p>	<p>Rozbudowa narzędzi informatycznych umowa TXU/TXXI/256/224/2018 Dokumentacja powykonawcza</p>	<p>Numer sygnatury</p> <p>5434/05/2022</p>
---	---	--

## 1 Zakres i cel dokumentacji

Niniejszy dokument stanowi Załącznik nr 10 do Dokumentacji powykonawczej zrealizowanej w ramach Projektu „Rozbudowa systemu zarządzania ruchem we Wrocławiu, w tym o nowe sygnalizacje świetlne, wyświetlacze pomocnicze ITS oraz aplikację mobilną” Część III: Rozbudowa narzędzi informatycznych (Umowa TXU/TXXI/256/224/2018).

W dokumencie przedstawiono proces podłączenia i potwierdzenia tożsamości sterowników sygnalizacji ulicznej do systemu ITS oraz innych zabezpieczeń mających na celu zapewnienie bezpieczeństwa komunikacji.

Opis dotyczy wyłącznie podłączenia sterownika sygnalizacji do systemu sterowania ruchem Gertrude (GTR) oraz modułu nadawania priorytetów (MNP).

Dodatkowo w dokumencie opisano interfejs komunikacyjny pomiędzy podsystemem Nadawania Priorytetów (MNP) / Tras Alternatywnych (MTA) a sterownikami sygnalizacji ulicznej.

## 2 Zawartość dokumentu

Niniejszy dokument opisuje:

- Ogólne zasady podłączenia sterownika do Systemu ITS
- Sposób pozyskania plików uwierzytelniających z danymi dla MNP oraz GTR
- Strukturę plików z danymi
- Uwierzytelnienie dla łączności z serwerem GTR <-> TLC oraz MNP <-> TLC
- Wymianę danych (warstwa transportowa i logiczna) dla „MNP”
- Nawiązywanie i utrzymanie sesji dla „MNP”
- Wymianę metryki urządzeń dla łączność „MNP” oraz „Gertrude”
- Szyfrowanie łączności dla „MNP”
- Algorytmy do uzyskania uwierzytelniania dla „Gertrude” oraz „MNP”
- Dane konfiguracyjne


## 3 Zasady ogólne podłączenia

W niniejszym rozdziale opisano ogólne zasady podłączenia sterownika sygnalizacji ulicznej do systemu ITS.

W celu podłączenia sterownika do systemu sterowania ruchem oraz modułu nadawania priorytetów / tras alternatywnych w systemie ITS zarejestrować certyfikat poświadczający zgodność urządzenia z systemem GTR lub dodatkowo do MNP.

Certyfikat jest wydawany w formie cyfrowej, jest to ciąg literowo-cyfrowy, który należy użyć przy uwierzytelnianiu się do systemów. Certyfikat jest w dokumencie opisany również jako metryka (zamiennie).


Certyfikat GTR, jest wydawany przez producenta systemu sterowania ruchem w celu potwierdzenia kompatybilności i poprawnej realizacji poleceń, algorytmów i mechanizmów kontroli oraz przekazywania wymaganych danych przez system sterowania ruchem.

ZAMAWIAJĄCY:  <b>Gmina Wrocław</b>	Rozbudowa narzędzi informatycznych umowa TXU/TXXI/256/224/2018 Dokumentacja powykonawcza	Numer sygnatury
		5434/05/2022

Certyfikat MNP jest wydawany przez administratora systemu.

Producent sterownika zobowiązany jest do prawidłowego użycia wydanego certyfikatu we własnym oprogramowaniu wg własnej implementacji zasad opisanych w niniejszym dokumencie.

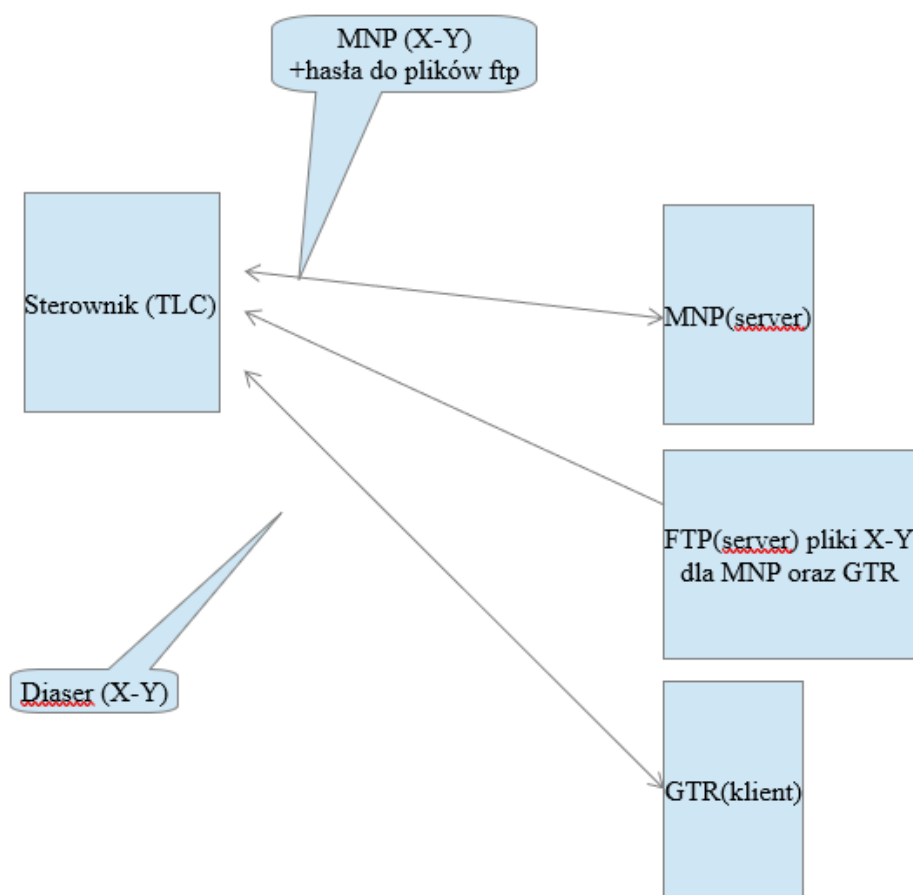
Certyfikat wydawany jest dla danego sterownika wg kategorii producent (typ sterownika) zawiera uprawnienia do wybranych serwisów. Tego samego certyfikatu można używać w wielu urządzeniach tej samej serii.

ZAMAWIAJĄCY:  <b>Gmina Wrocław</b>	Rozbudowa narzędzi informatycznych umowa TXU/TXXI/256/224/2018 Dokumentacja powykonawcza	Numer sygnatury
		5434/05/2022


## 4 Podłączenie do systemu ITS – zasady ogólne

W celu podłączenia sterownika wykonaj następujące kroki w poniższej kolejności:

1. Uzyskaj certyfikat
2. Zarejestruj certyfikat w serwisie uwierzytelniającym (czynność administracyjna).
3. Użyj certyfikatu w swoim systemie w sterowniku.
4. Skonfiguruj sterownik dla GTR jako klient UDP port 30000,
5. Skonfiguruj sterownik dla MNP jako serwer TCP .
6. Skonfiguruj sterownik jako klient FTP w celu pobierania plików uwierzytelniających
7. Podłącz się do serwisu MNP ze swoją metryką (certyfikatem)
8. Otrzymaj hasła do plików uwierzytelniających dla GTR oraz MNP
9. Pobierz pliki z serwisu FTP i rozpakuj je z użyciem otrzymanych haseł
10. Prowadź sesję komunikacji i wymieniaj dane uwierzytelniające (wiadomość X Y) zgodnie z zasadami komunikacji z systemami MNP i GTR.



Rysunek 1 Schemat blokowy połączeń sieciowych

ZAMAWIAJĄCY:  <b>Gmina Wrocław</b>	Rozbudowa narzędzi informatycznych umowa TXU/TXXI/256/224/2018 Dokumentacja powykonawcza	Numer sygnatury
		5434/05/2022

## 4.1 Połączenie sieciowe

Nawiązanie łączności odbywa się w sposób wieloetapowy.

1. nawiąż połączenie z serwisem MNP „przedstaw się i podaj metrykę”
2. uzyskaj hasła do plików uwierzytelniających dla GTR oraz MNP oraz klucz do komunikacji szyfrowanej z MNP
3. Pobierz pliki z serwisu FTP i rozpakuj je z użyciem otrzymanych haseł
4. uwierzytelnij się w serwisach MNP i GTR - na podstawie plików uwierzytelniających podaj właściwą odpowiedź na zapytanie autoryzacyjne
5. nawiąż sesję z MNP i/lub Gertrude
6. rozpocznij wymianę danych z serwisem MNP i GTR

Warstwa (sposób) komunikacji z systemem GTR oraz systemu MNP są różne i zostały przedstawione w innych opracowaniach, natomiast sposób (metody) uzyskania danych do uwierzytelnienia w systemach GTR i MNP jest identyczny dla obydwóch systemów.

Poniżej opisana metoda umożliwia bezpieczne uwierzytelnianie klient->serwer na podstawie unikalnych kodów wyliczanych metodami kryptograficznymi.

Metoda bazuje na kluczu 8 bajtowym pytania, oraz 8 bajtowym odpowiedzi. Pytania i odpowiedzi znajdują się w udostępnionych plikach uwierzytelniających na serwerze ftp. Pliki są skompresowane i zaszyfrowane, hasła do plików pozyskuje się poprzez odpowiedź od serwisu MNP. Zapytanie o hasło uwzględnia metrykę pozyskaną od producenta systemu sterowania ruchem lub nadaną przez administratora MNP.

Metryka rejestrowana jest w serwisie (poprzez Administratora) udzielającym odpowiedzi oraz w sterownikach (do implementacji po stronie dostawcy urządzeń).

## 4.2 Opis pliku uwierzytelniającego

Cały zapis zrealizowany jest w formacie tekstowym rozdzielonym przecinkami. Wszystkie wartości w pliku zapisane są w formie cyfr z dziedziny od 0 do 255 (zmienna długość 1-3 cyfr) . Prawidłowe wartości zawierają się od 0 do 255. W przypadku innych wartości należy je pominąć, offsetu nie należy zwiększać. Pojęcia offset/len odnoszą się do nr wartości uzyskanej po przecinku !!!!! nie jest to absolutny adres w pliku.

Schemat kodowania pliku Pliku (nagłówek pliku)


	Offset	len	opis
version	0	32	Wersja kodowania pliku (określa sposób kodowania pliku)
CRC file		4	Adres pola CRC 4 elementy (długość CRC to 4) nie używane
ENC method address		4	Adres do opisu metody szyfrowania (typ szyfrowania) długość to 1
AES key address		4	Adres do klucza 32 AES (długość to 32 elementy)
Not implemented		4	Bez znaczenia
start XY msg address start		4	Adres początku obszaru występowania kluczy X-Y długość to 4
len XY msg address len		4	Adres gdzie zapisana jest długość obszaru kluczy X-Y długość to 4

typ szyfrowania:

- 65 Szyfrowanie AES (należy pobrać klucz do szyfrowania)
- 66 Brak szyfrowania (klucz nie ma znaczenia)
- 69 Szyfrowanie ECC (nie używane)
- 84 Szyfrowanie Trivium (nie używane)





<b>ZAMAWIAJĄCY:</b>  <b>Gmina Wrocław</b>	Rozbudowa narzędzi informatycznych umowa TXU/TXXI/256/224/2018 Dokumentacja powykonawcza	<b>Numer sygnatury</b> 5434/05/2022
---	--	--

## 4.3 Hasła do plików uwierzytelniających

W celu uzyskania haseł do plików uwierzytelniających należy nawiązać połączeniem TCP z serwisem uwierzytelniającym MNP wysyłając zapytanie (ramkę) opisaną poniżej. Pola wyróżnione kolorem należy uzupełnić po stronie nawiązującego urządzenia

Na poniższym przykładzie przedstawiono kompletne zapytanie dla urządzenia o id=111. Pola wyróżnione kolorem oznaczają metrykę nadaną GTR i MNP.

	ASCII					bin				hex		Bin					ASCII		bin		bin	bin	ASCII												
																			Controller ID																
nr bajtu	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29					
treść:	W	R	D	v	1	74	0	46	0	AA	AA	n	n	n	N	78	L	W	111	0	n	n	n	W	<	c	e	r	t	>					

Cd:

hex																													
metryka																													
30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59
FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF

cd:

ASCII											
63	64	65	66	67	68	69	70	71	72	73	
<	/	c	e	r	t	>	E	N	D	p	

Jeżeli metryka jest poprawna (zarejestrowana w serwisie) wówczas zostanie udzielona odpowiedź zawierająca hasła do plików które należy pobrać z zasobu ftp:

	ASCII					bin				hex		bin					ASCII		bin	AS CII	bin	bin	bin			ASCII																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																									

Gdzie: 1,2 port przydzielany przez serwer, 3, timeout serwera na przydzielonym porcie.


Hasła do plików jest zapisane w formie hex w następujący sposób:

cd: ramki

hex																													
hasło																													
33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62
FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF

koniec ramki to:


ASCII											
66	67	68	69	70	71	72	73	74	75	76	
<	/	c	e	r	t	>	E	N	D	p	

ZAMAWIAJĄCY:  <b>Gmina Wrocław</b>	Rozbudowa narzędzi informatycznych umowa TXU/TXXI/256/224/2018 Dokumentacja powykonawcza	Numer sygnatury
		5434/05/2022

Plik z danymi do uwierzytelnienia jest skompresowany przy użyciu metody .zip. i zabezpieczony hasłem pozyskanym z usługi jak opisano powyżej. Pozyskany plik należy rozpakować z użyciem haseł stanowiących odpowiedź na metrykę.

Odpowiedź na metrykę zawiera dwa hasła o długości 16 znaków. Pierwsze 16 dotyczy GTR kolejne MNP.

Aby odczytać poprawnie hasło do GTR należy użyć metody AES256 EBC. Hasło AES jest nadawane do metryki przez producenta sterowania ruchem. Hasło należy chronić przed nieuprawnionym dostępem.

ZAMAWIAJĄCY:  <b>Gmina Wrocław</b>	Rozbudowa narzędzi informatycznych umowa TXU/TXXI/256/224/2018 Dokumentacja powykonawcza	Numer sygnatury 5434/05/2022
--	--	---------------------------------

## 4.4 Operacje matematyczne i kryptograficzne

Dla zapytania uwierzytelniającego z serwisu MNP oraz serwisu GTR (msg X) należy odszukać w plikach uwierzytelniających klucze i następnie zbudować wiadomość MSG-Y i odpowiedzieć odpowiedniemu serwisowi.

Format wiadomości msg X-Y jest różny dla serwisu MNP i serwisu GTR, natomiast metody ją opisujące są identyczne niezależnie od formy transportowej.

**Uwaga.** Poniższe przykłady matematyczne i kryptograficzne nie odzwierciedlają faktycznych wyników mają jedynie charakter poglądowy, opisujący metody, nie wyniki.

Przykład:

zawartość pliku:

.....1,2,245,8,9,10,1,5,7,8,9,23,225,234,0,9,16,134,67,54,23,56,100,44,48,.....

pytanie uwierzytelniając msg X: pobierz pierwsze 8 liczb z wiadomości MSG-X

8,9,23,225,234,0,9,16.....

znajdź wskazany ciąg w pliku.

Pobierz kolejne 8 liczb znajdujące się za wyszukiwanym ciągiem

134,67,54,23,56,100,44,48

zbuduj macierz liczb w następujący sposób:

8,9,23,225,234,0,9,16,134,67,54,23,56,100,44,48

następnie zmieniając kolejność liczb w następujący sposób: weź pierwszą liczbę z klucza i umieść ją na ostatniej pozycji tworząc nowy 16- elementowy klucz co pokazano na poniższym przykładzie




9,23,225,234,0,9,16,134,67,54,23,56,100,44,48,8



23,225,234,0,9,16,134,67,54,23,56,100,44,48,8,9,



W opisie algorytmu użyto parametrów **n** i **k** są to wartości stałe i wynoszą one odpowiednio **n=7** **k=7**

ZAMAWIAJĄCY:  <b>Gmina Wrocław</b>	Rozbudowa narzędzi informatycznych umowa TXU/TXXI/256/224/2018 Dokumentacja powykonawcza	Numer sygnatury 5434/05/2022
--	--	---------------------------------

Operację powtórz 16 razy aż do uzyskania tabeli dwuwymiarowej 16X16 liczb jak opisano w tabeli poniżej. Tablicę należy traktować jako macierz kwadratową 2X2 liczb `double[2][2]`, oraz 16X16 dla liczb typu `char[16][16]` (ze znakiem):

Przykładowa tabela (macierz) liczb ułożona w formie tablicy[][] przedstawiona poniżej dla  $k=0$

	Double a(x)								double b(x)								
Oś y	8	9	23	255	234	0	9	16	134	67	54	23	56	100	44	48	double a(y)
	9	23	255	234	0	9	16	134	67	54	23	56	100	44	48	8	
	23	255	234	0	9	16	134	67	54	23	56	100	44	48	8	9	
	255	234	0	9	16	134	67	54	23	56	100	44	48	8	9	23	
	234	0	9	16	134	67	54	23	56	100	44	48	8	9	23	255	
	0	9	16	134	67	54	23	56	100	44	48	8	9	23	255	234	
	9	16	134	67	54	23	56	100	44	48	8	9	23	255	234	0	
	16	134	67	54	23	56	100	44	48	8	9	23	255	234	0	9	
	134	67	54	23	56	100	44	48	8	9	23	255	234	0	9	16	double b(y)
	67	54	23	56	100	44	48	8	9	23	255	234	0	9	16	134	
	54	23	56	100	44	48	8	9	23	255	234	0	9	16	134	67	
	23	56	100	44	48	8	9	23	255	234	0	9	16	134	67	54	
	56	100	44	48	8	9	23	255	234	0	9	16	134	67	54	23	
	100	44	48	8	9	23	255	234	0	9	16	134	67	54	23	56	
	44	48	8	9	23	255	234	0	9	16	134	67	54	23	56	100	
	48	8	9	23	255	234	0	9	16	134	67	54	23	56	100	44	
(0,0)	Oś x																

1,2,3,4,5,6,7,8, 134,67,54,23,56,100,44,48,


weź ostatnie **k** liczb z ciągu (pierwszych 8 liczb) i ułóż je wg poniższego wzorca (przykład dla  $k=7$ )

8,9,23,225,234,0,9,16

							<b>k</b>										
8	9	23	225	234	0	9	16	134	67	54	23	56	100	44	48		
8	9	23	225	234	0	16	9	134	67	54	23	56	100	44	48		
8	9	23	225	234	9	0	16	134	67	54	23	56	100	44	48		
8	9	23	225	234	9	16	0	134	67	54	23	56	100	44	48		
8	9	23	225	234	16	0	9	134	67	54	23	56	100	44	48		
8	9	23	225	234	16	9	0	134	67	54	23	56	100	44	48		
...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...		
8	16	9	0	234	225	23	9	134	67	54	23	56	100	44	48		

(permutacja- wariacja bez powtórzeń):

dla **k**=7 należy wykonać ( $k!$ ) macierzy kwadratowych wg opisu powyżej (Przykładowa tabela dla  $k=7$ ).

ZAMAWIAJĄCY:  <b>Gmina Wrocław</b>	Rozbudowa narzędzi informatycznych umowa TXU/TXXI/256/224/2018 Dokumentacja powykonawcza	Numer sygnatury
		5434/05/2022

Na wytworzonych macierzach wykonaj funkcję AES\_ecb\_encrypt (x,y,128), operację należy wykonać wg parametru **n**.

Wykonaj w osi x operację AES128, jako klucza użyj liczby 16 bajtowej z osi y, przykład dla **n = 2**:


**n=0** AES\_ecb\_encrypt(

in=

48	8	9	23	255	23	0	9	16	134	67	54	23	56	100	44
					4										

key

48	44	100	56	23	54	67	134	16	9	0	234	25	23	9	8
												5			

ZAMAWIAJĄCY:  <b>Gmina Wrocław</b>	Rozbudowa narzędzi informatycznych umowa TXU/TXXI/256/224/2018 Dokumentacja powykonawcza	Numer sygnatury 5434/05/2022
--	--	---------------------------------

$n = 1$  AES\_ecb\_encrypt(

in=

44	48	8	9	23	25	234	0	9	16	134	67	54	23	56	100
----	----	---	---	----	----	-----	---	---	----	-----	----	----	----	----	-----

key=

8	48	44	100	56	23	54	67	13	16	9	0	23	255	23	9
---	----	----	-----	----	----	----	----	----	----	---	---	----	-----	----	---

N=..... powtórzyć opercję zgodnie ze schematem jw.

uzyskasz łącznie  $n = 2$  operacji wyników operacji AES128 (tablica  $[n][16]$ ), wyniki rzutuj na zmienne typu double .

double  $\Sigma a(x) = 5,9,80,34,57,12,24,0$

+

double  $\Sigma b(x) = 12,45,23,56,78,34,25,100$

=

double  $C(x) = C = 15,16,125,134,157,102,204,5$

Zsumuj wyniki  $\Sigma a(x)$  i  $\Sigma b(x)$  dla wszystkich macierzy dla parametrów wg  $k$ , rezultat stanowi 8 liczb ułożonych, kolejno po sobie, co daje klucz do wyszukania w całym pliku dla następnego ciągu.

$C = 15,16,125,134,157,102,204,5$  C=takiego wyrażenia szukaj w pliku

Znajdź w całym pliku ciąg odpowiadający wynikowi dla pierwszych 8 liczb, powyższej sumy operacji kryptograficznej. Następnie oblicz sumę wyznaczników wszystkich utworzonych macierzy (char)([16][16]) wg parametru  $k$  co da wartość  $X$ , rzutuj na unsigned char, ((modulo 7)+1). Wynik operacji jest w zakresie 1-7. Uzyskana wartość jest przesunięciem w pliku do wartości odpowiedzi na dany klucz (8 kolejnych liczb po przecinku).

Przykład:


unsigned char  $X = 15,16,125,134,157,102,204,5,12,45,23,56,78,34,25,100$

Dla  $X$  równego 3 odpowiedź znajduje się jak poniżej:

1,2,245,8,9,10,1,5,7,8,9,23,225,234,0,9,16,134,67,54,23,56,100,44,48,236(...),  
15,16,125,134,157,102,204,5,1,8,33,74,73,68,11,4,70,98,244

pytanie = odpowiedz:

8,9,23,225,234,0,9,16=74,73,68,11,4,70,98,244

ZAMAWIAJĄCY:  <b>Gmina Wrocław</b>	Rozbudowa narzędzi informatycznych umowa TXU/TXXI/256/224/2018 Dokumentacja powykonawcza	Numer sygnatury 5434/05/2022
--	--	---------------------------------

W wyniku otrzymujemy zawartość MSG-X 8 bajtów + 8 bajtów, oraz gotową zawartość: MSG-Y 8 bajtów + 8 bajtów (znaków/liczb – zależy od protokołu warstwy komunikacyjnej!)

gdzie :

wiadomość MSG-X to ciąg:

8,9,23,225,234,0,9,16,134,67,54,23,56,100,44,48

wiadomość MSG-Y to ciąg

74,73,68,11,4,70,98,244,?,?,?,?,?,?,?,


Liczby określone w MSG-Y jako „?” (zakres 0-255) nie mają znaczenia w procesie uwierzytelniania.

## 4.5 Pseudokod

### Pseudokod (k=7 i n=7):

Pobierz plik z serwera zawierający liczby oddzielone przecinkami. Przetwórz plik zgodnie z opisem nagłówka.

1. Odbierz wiadomość od serwera podczas inicjalizacji połączenia (klucz – message X)
2. Wyszukaj wskazaną liczbę w pliku
3. Pobierz kolejne 8 liczb znajdujących się po wskazanym kluczu (będących wartością)
4. Wykonaj permutację 7 ostatnich elementów klucza
5. Dla każdej permutacji wykonaj następujące działania:
6. Scal 8 liczb klucza oraz 8 kolejnych liczb z pliku w jeden ciąg "S"
7. Zbuduj tablicę dwuwymiarową liczb całkowitych o wymiarach 16x16
8. Wypełnij tablicę wykonując poniższe operacje:
  - a) Dla każdego indeksu tablicy wpisz S
  - b) Zmodyfikuj S przesuując pierwszy element na ostatnią pozycję
  - c) Inkrementuj numer indeksu
9. Wykonaj AES128 dla n=7 wierszy wykorzystując n-ty wiersz jako klucz i n-tą kolumnę jako wartość
10. Zsumuj wyniki AES, a następnie uzyskany w ten sposób ciąg liczb wyszukaj w pobranym pliku
11. Oblicz wyznacznik wszystkich utworzonych macierzy i wykonaj na nich modulo 7, a następnie dodaj 1. Uzyskana liczba określa przesunięcie w pliku od końca znalezionego w pliku klucza
12. Zwróć do serwera nową wartość znajdującą się za nowym kluczem z wyliczonym przesunięciem (message Y)

ZAMAWIAJĄCY:  <b>Gmina Wrocław</b>	Rozbudowa narzędzi informatycznych umowa TXU/TXXI/256/224/2018 Dokumentacja powykonawcza	Numer sygnatury
		5434/05/2022

## 5 Podłączenie do Modułu Nadawania Priorytetu – MNP

### 5.1 Autoryzacja MNP - opis wiadomości XYZ

Komunikacja wiadomościami XYZ odbywa się na porcie docelowym otrzymanym od serwera.

Sterownik musi uwierzytelnić się z użyciem kluczy pozyskanych z plików uwierzytelniających

Format Wiadomości „X” , wysyła serwer do sterownika

	ASCII					bin				hex		bin					ASCII		bin		bin	bin	ASCII								
nr bajtu	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	
treść:	W	R	D	v	1	67	0	3 9	0	AA	AA	n	n	n	n	78	U	W	n	n	n	n	n	W	<	X	>	FF	FF	FF	

Cd:


Ca:

ASCII																																	
Message X																																	
30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	
FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	<	/	X	>

cd:

ASCII											
63	64	65	66	67	68	69	70	71	72	73	
E	N	D	p								



<b>ZAMAWIAJĄCY:</b>  <b>Gmina Wrocław</b>	Rozbudowa narzędzi informatycznych umowa TXU/TXXI/256/224/2018 Dokumentacja powykonawcza	Numer sygnatury
		5434/05/2022

Format wiadomości „Y” wysyła sterownik do serwera w odpowiedzi na wiadomość „X”

	ASCII					bin				hex		bin					ASCII		bin		bin		ASCII								
																		Controller ID													
nr bajtu	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	
treść:	W	R	D	v	1	67	0	39	0	AA	AA	n	n	n	n	78	U	W	111	0	n	n	n	W	<	Y	>	FF	FF	FF	

Cd:

ASCII																																
Message Y																																
30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62
FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	<	/	Y	>

cd:


ASCII										
63	64	65	66	67	68	69	70	71	72	73
E	N	D	p							

Format wiadomości „Z”, wysyła serwer do sterownika celu potwierdzenia zestawienia transmisji

	ASCII					bin				hex		bin					ASCII		bin		bin	bin	ASCII									
nr bajtu	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29		
treść:	W	R	D	v	1	51	0	24	0	AA	AA	n	n	n	n	78	U	W	n	n	n	n	n	W	<	Z	>	FF	FF	FF		

Cd:

ASCII																																
Message Z																																
30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62
FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	<	/	Z	>															

ZAMAWIAJĄCY:  <b>Gmina Wrocław</b>	Rozbudowa narzędzi informatycznych umowa TXU/TXXI/256/224/2018 Dokumentacja powykonawcza	Numer sygnatury 5434/05/2022
--	--	---------------------------------

## 5.2 Komunikacja i szyfrowanie MNP

Metoda szyfrowania jest opisana w nagłówku pliku uwierzytelniającego.  
Klucze szyfrowania zależą od metryki urządzenia i mogą być unikalne dla każdej z nich.

W przypadku zastosowania metody AES256 (określa to plik uwierzytelniający pobrany z serwera ftp) klucze umieszczone są w pliku i stanowią odrębną część patrz opis struktury pliku. Każda nowa sesja poprzedzona uwierzytelnieniem może być rozpoczęta innym kluczem (należy sprawdzić plik) .

Klucz pozostaje niezmienny podczas trwania sesji. Podczas trwania sesji może być wysłane żądanie uwierzytelnienia(wówczas postępuj jak dla nowej sesji).

Wiadomości serwisu MNP znajdują się w ramach o następującym formacie

Właściwości serwisu MINI znajdują się w ramkach o następujących formacie																								
	ASCII					bin				hex		bin				ASCII		bin		ASCII	bin		ASCII	
																		Controller ID						
nr bajtu	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
treść:	W	R	D	v	1	N	N	N	N	AA	AA	?	?	?	?	78	D	S	111	0	M	0	0	M

CD:

bin																														
Dane																														
24	25	26	27	28	29	30	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..
FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF

Dane posiadają zmienną długość, dane są wypełniane zgodnie z Interfejsem wymiany danych do zarządzania wsparciem przejazdów po trasach alternatywnych i rozkładowych opisanym w dalszej części dokumentu

CD:

ASCII			
N+1	N+2	N+3	N+4
E	N	D	p

Dane w ramce zaznaczone kolorem ..... są zakodowane w całości metodą szyfrowania  
W przypadku MNP konieczne jest również utrzymanie MNP sesji odrębną wiadomością o formacie:

serwer→ Klient


Server - Klient																								
	ASCII					bin				hex		bin				ASCII		bin		ASCII	bin	ASCII		
																		Controller ID						
nr bajtu	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
treść:	W	R	D	v	1	?	?	?	?	AA	AA	?	?	?	?	78	C	S	111	0	M	0	0	?

CD:

bin																ASCII			
24	25	26	27	28	29	30	31	..	..	..	..	..	..	..	..	N+1	N+2	N+3	N+4
1	2	3	4	5	6	7	8									E	N	D	p

gdzie 1234 oznacza czas trwania sesji w sekundach

gdzie 5678 oznacza czas co ile sekund klient ma wysyłać wiadomość utrzymania sesji określoną poniżej:

<b>ZAMAWIAJĄCY:</b>  <b>Gmina Wrocław</b>	Rozbudowa narzędzi informatycznych umowa TXU/TXXI/256/224/2018 Dokumentacja powykonawcza	Numer sygnatury 5434/05/2022
---	--	---------------------------------

Klient->Serwer

	ASCII				bin				hex		bin				ASCII		bin		ASCII		bin		ASCII	
																					Controller ID			
nr bajtu	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
treść:	W	R	D	v	1	?	?	?	?	AA	AA	?	?	?	?	78	C	S	0	0	M	111	0	?

Cd:

bin																ASCII			
24	25	26	27	28	29	30	31	..	..	..	..	..	..	..	..	N+1	N+2	N+3	N+4
1	2	3	4	5	6	7	8									E	N	D	p

Gdzie 1234 oznacza czas trwania sesji w sekundach

Gdzie 5678 oznacza czas życia modułu w sekundach

Gdzie Controller ID unikalny numer sterownika

Z uwagi na to iż dane są kodowane blokowo, długość danych jest uwarunkowana od sposobu szyfrowania wskazanej w pliku uwierzytelniającym. W bajtach dopełniających (nie stanowiących treści) mogą znajdować się wartości nieokreślone.

## 5.3 Interfejs wymiany danych z pojazdów


Poniżej przedstawiono ogólne założenia budowy ramki komunikatu przekazywanym w polu „Dane” wiadomości serwisu MNP.

Nazwa pola	Rozmiar [B]	Wartość / zakres	Opis
BOP/BOA	1	0x62 ('b')	Znaczniki początku ramki
ADDR	2	0x0 – 0xFFFF	Adres ramki
PGN	1	0x0 – 0xFF	Numer grupy parametrów
DSIZE	1	0x0 – 0xFF	Wielkość pola DATA w bajtach
DATA	zmienny w zakresie 0-255		Pole danych
CRC	1	0x0 – 0xFF	Suma kontrolna crc8
EOP	1	0x65 ('e')	Znacznik końca ramki

Wszystkie dane techniczne identyfikujące urządzenia komunikacji radiowej, takie jak identyfikatory pętli Capsys, będą tłumaczone na kody entry przez PLC. Każdy PLC posiada już zapisane w pamięci tablice konwersji kodów, które wykorzystywane są do konwersji na numery entry, dla potrzeb Systemu Sterowania Ruchem Gertrude.

Komunikaty zapowiedzi pojazdu oraz emulowane zgłoszenia pojazdów wysyłane przez MNP nie będą zawierały definicji mapowań entry zgłaszanych przez pojazdy. Tablice definicji kodów entry w PLC zostaną rozbudowane o dodatkowy atrybut rodzaju zgłoszenia powiązanego z danym entry (patrz opis pola NOTIF\_TYPE w definicji komunikatu zgłoszenia 'n').

Wsparcie przejazdów przez MNP jest realizowane w trybie ciągłym i odrębnie dla każdego kursu. Dla każdego odrębnego przejazdu tego samego pojazdu przez skrzyżowanieysterowanie będzie odrębne, dlatego po otrzymaniu zapowiedzi od MNP PLC może na

<b>ZAMAWIAJĄCY:</b>  <b>Gmina Wrocław</b>	Rozbudowa narzędzi informatycznych umowa TXU/TXXI/256/224/2018 Dokumentacja powykonawcza	Numer sygnatury 5434/05/2022
---	--	---------------------------------

podstawie numeru bocznego i atrybutu zgłoszenia przekazanego przez komputer pokładowy odnaleźć rodzaj zgłoszenia i pobrać z konfiguracji zapowiedzi wartość właściwą dla entry. Wprowadzona została też notacja umożliwiająca sterowanie sposobem interpretowania zgłoszeń (ignorowanie / tylko obsługa lokalna / obsługa ze zgłoszeniem do Systemu Sterowania Ruchem).

W przypadku komunikatów zgłoszeniowych przekazywanych z PLC do MNP (kopia komunikatu A – komunikat A1) będą one zgodne co do struktury ze specyfikacją protokołu SRRP, przy czym:

- pole wJunctionID identyfikator skrzyżowania zgodny z numeracją skrzyżowań w Systemie Sterowania Ruchem,
- pola wGPSLoopID oraz bLoopID+bInterfaceID będą zawierały identyfikatory entry (tłumaczone przez PLC z numerów detektorów),
- pole wVehicleID numer boczny pojazdu, który nie wymaga tłumaczenia (numer będzie zgodny z tym, który KPP przekazuje poprzez GPRS).

MNP nie przesyła zwrotnie ramki potwierdzenia (ramki BOA=0x61).

W przypadku wykonania restartu PLC przekazuje do MNP następujący komunikat (komunikat restart):

Nazwa pola	Rozmiar [B]	Wartość zakres	Opis
BOP/BOA	1	0x72 ('r')	Znaczniiki początku ramki
ADDR	2	0x0 0xFFFF	Numer sterownika PLC
PGN	1	0xFF	Wartość stała
DSIZE	1	0x02	Wartość stała
DATA	2	0x0 0xFFFF	Czas w [s] od momentu restartu
CRC	1	0x0 – 0xFF	Suma kontrolna crc8
EOP	1	0x65 ('e')	Znaczniik końca ramki


W odpowiedzi na taki komunikat MNP wyśle ponownie wszystkie aktywne zapowiedzi udzielenia wsparcia, które dany PLC powinien otrzymać, a następnie wszystkie zgłoszenia dalekiego i bliskiego zasięgu, które były przesłane w czasie DATA sekund od chwili bieżącej.

Do przekazania informacji o zapowiedzi (**d**claration) tramwaju wykorzystywana jest następująca ramka:

Nazwa pola	Rozmiar [B]	Wartość zakres	Opis
BOP/BOA	1	0x64 ('d')	Znaczniiki początku ramki
ADDR	2	0x0 – 0xFFFF	Numer sterownika PLC
DSIZE	1	0x7 – 0xFF	Wielkość pola DATA w bajtach
DATA	7+[n]*5		Patrz opis niżej
CRC	1	0x0 – 0xFF	Suma kontrolna crc8
EOP	1	0x65 ('e')	Znaczniik końca ramki

Przy czym pole DATA zawiera następujące pola:

Nazwa pola	Rozmiar	Wartość	Opis
------------	---------	---------	------

ZAMAWIAJĄCY:  <b>Gmina Wrocław</b>	Rozbudowa narzędzi informatycznych umowa TXU/TXXI/256/224/2018 Dokumentacja powykonawcza	Numer sygnatury 5434/05/2022
--	--	---------------------------------

	[B]	/ zakres	
MODE	1	0x01 0x02 0x03	Definicja zapowiedzi Zmiana zapowiedzi Anulowanie zapowiedzi (wtedy wszystkie inne pola poza VEHICLE nie są interpretowane).
VEHICLE	2	0x0 – 0xFFFF	Numer boczny pojazdu
VTYPE	1	0x01 0x02 – 0xFF	Tramwaj Inny pojazd (rezerwa)
JUNCTION	2	0x0 – 0xFFFF	Identyfikator skrzyżowania w Systemie Sterowania Ruchem
COUNT	1	0x0 – 0xFF	ilość definicji mapowań [n]
DETtype	1	0x0 – 0xFF	Typ detektora: 0-capsys, 1-radio
DETid	1	0x0 – 0xFF	Maskowane urządzenie/zgłoszenie Identyfikator entry dla DETtype=1; adres capsys dla DETtype=0
DETidnew	1	0x0 – 0xFF	Docelowe urządzenie/zgłoszenie Identyfikator entry dla DETtype=1; adres capsys dla DETtype=0
DETdirection	1	0x0 – 0xFF	Kierunek dla definicji mapowania
DETPriority	1	0x0 – 0xFF	Priorytet dla definicji mapowania

Pole JUNCTION przenosi informację o numerze sterownika obsługującym detektor. W przypadku, gdy detektory dla relacji obsługuje więcej niż jeden sterownik, MNP wysyła odrębne definicje dla detektorów obsługujących, w każdej podając definicje dotyczące detektorów obsługiwanych przez dany sterownik.


Jeśli DETtype == 0x00, to pola DETid i DETidnew zawierają numer (adres) detektora Capsys. Jeśli VTYPE == 0x01, to pola DETid i DETidnew zawierają numer entry.

Pole DETdirection jest polem określającym kierunek przejazdu (wg numeracji Systemu Sterowania Ruchem).

Przekazanie ramki (d) zawierającej MODE=3 oznacza anulowanie poprzedniego zgłoszenia tramwaju i powrót sterownika PLC do normalnego trybu obsługi dla danego numeru bocznego.

Do przekazywania zgłoszeń emulowanych przez MNP zastosowany zostanie następujący format komunikatu (notification):

Nazwa pola	Rozmiar [B]	Wartość / zakres	Opis
BOP/BOA	1	0x6E ('n')	Znaczniki początku ramki
ADDR	2	0x0 0xFFFF	Numer sterownika PLC
PGN	1	0x45 ('E')	Wartość stała
DSIZE	1	0x0E	Wartość stała
DATA	14		Pole danych – patrz opis
CRC	1	0x0 – 0xFF	Suma kontrolna crc8
EOP	1	0x65 ('e')	Znacznik końca ramki

<b>ZAMAWIAJĄCY:</b>  <b>Gmina Wrocław</b>	Rozbudowa narzędzi informatycznych umowa TXU/TXXI/256/224/2018 Dokumentacja powykonawcza	Numer sygnatury
		5434/05/2022

Pole danych DATA składa się z następujących pól:


Nazwa pola	Rozmiar [B]	Wartość / zakres	Opis
VEHICLE	2	0x0 – 0xFFFF	Numer boczny pojazdu
VTYPE	1	0x01 – 0xFF	Tramwaj Inny pojazd (rezerwa)
JUNCTION	2	0x0 – 0xFFFF	Identyfikator skrzyżowania w Systemie Sterowania Ruchem
DIRECTION	1	0x0 – 0xFF	Kierunek relacji
NOTIF_TYPE	1	0x0 – 0xFF	Rodzaj zgłoszenia: 0x00 – zgłoszenie dalekiego zasięgu 0x01 – zgłoszenie zatrzymania na przystanku 0x02 – zgłoszenie otwarcia drzwi 0x03 – zgłoszenie zamknięcia drzwi 0x04 – zgłoszenie odjazdu z przystanku 0x05 – zgłoszenie bliskiego zasięgu przed linią zatrzymania 0x06 – zgłoszenie na linii zatrzymania 0x07 – zgłoszenie opuszczenia skrzyżowania 0x08 – 0xFF – zarezerwowane, nieużywane
ENTRY	2	0x0 – 0xFFFF	Identyfikator entry
DISTANCE	2	0x0 – 0xFFFF	Odległość od linii zatrzymania [m]
SPEED	2	0x0 – 0xFFFF	Prędkość pojazdu [m/s]
PRIORITY	1	0x0 – 0xFF	Priorytet (aktualnie wartość stała = 0x0 – brak priorytetu)

Do przekazania przez sterownik PLC kopii informacji odbieranych z detektorów (copy) wykorzystywana jest następująca ramka:

Nazwa pola	Rozmiar [B]	Wartość / zakres	Opis
BOP/BOA	1	0x63 ('c')	Znaczniki początku ramki
ADDR	2	0x0 – 0xFFFF	Numer sterownika PLC
DSIZE	1	0x0a	Wielkość pola DATA w bajtach
DATA	10		Patrz opis niżej
CRC	1	0x0 – 0xFF	Suma kontrolna crc8
EOP	1	0x65 ('e')	Znacznik końca ramki

Przy czym pole DATA zawiera następujące pola:

Nazwa pola	Rozmiar [B]	Wartość / zakres	Opis
SOURCE	1	0x00 – 0x01	Rodzaj detekcji: GPS (przekazane przez RKZ) CAPSYS
JUNCTION	2	0x0 – 0xFFFE	Numer skrzyżowania / sterownika PLC
ENTRY	2	0x0 – 0xFFFE	Numer zgłaszanego entry

<b>ZAMAWIAJĄCY:</b>  <b>Gmina Wrocław</b>	Rozbudowa narzędzi informatycznych umowa TXU/TXXI/256/224/2018 Dokumentacja powykonawcza	Numer sygnatury
		5434/05/2022

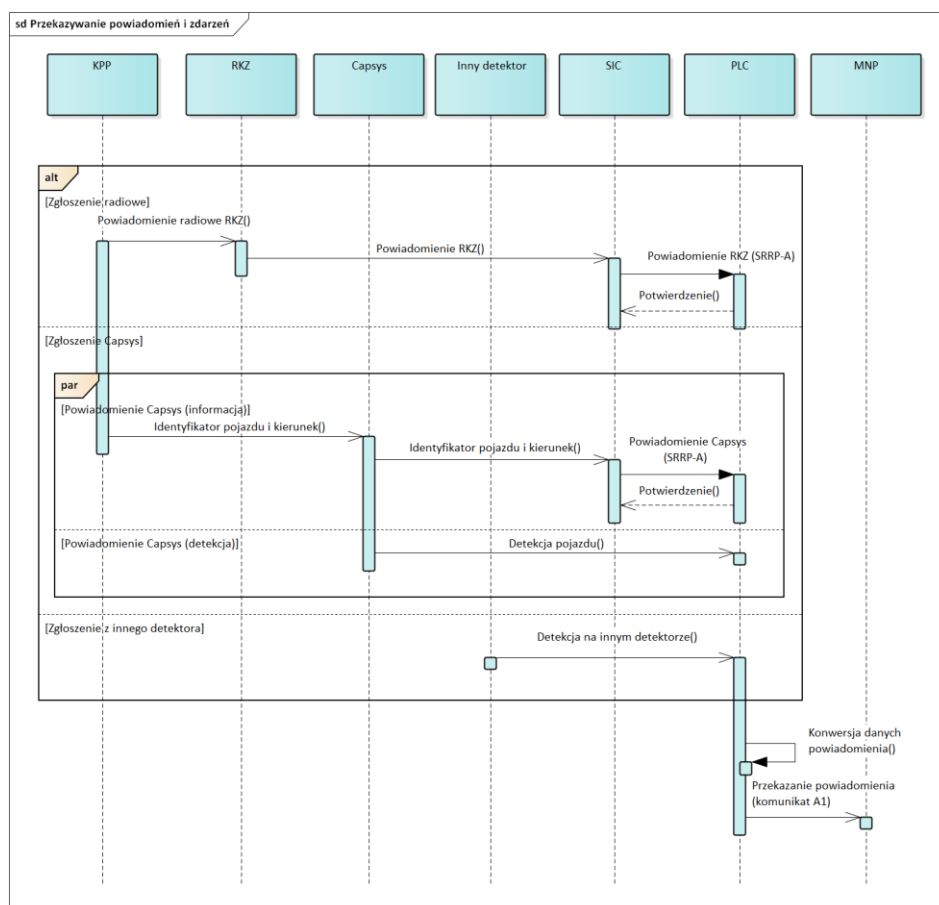
VEHICLE	2	0x0 – 0xFFFE	Numer boczny pojazdu
VTTYPE	1	0x01 0x02 – 0xFF	Tramwaj Inny pojazd (rezerwa)
PRIORITY	1	0x0 – 0xFF	Priorytet żądany
DIR_EVNT	1	0x0 – 0xFF	Kierunek żądany, informacja o zdarzeniu – patrz niżej

Zawartość pola DIR\_EVNT kodowana jest bitowo zgodnie z poniższą regułą:

Pole bitowe	Numer bitu	Liczba bitów	Wartość	Opis
LEFT	0 (LSB)	1	0 1	Żądanie jazdy w lewo: Nie Tak
STRAIGHT	1	1	0 1	Żądanie jazdy na wprost: Nie Tak
RIGHT	2	1	0 1	Żądanie jazdy w prawo: Nie Tak
RESVD	3..6	4	0000b	Stała wartość 0
DOORS	7 (MSB)	1	0 1	Stan otwarcia drzwi 0 – drzwi otwarte 1 – drzwi zamknięte

## 5.4 Przesyłanie danych z pojazdu – zasady obsługi

Poniżej przedstawiony został diagram czasowy komunikacji związany z przekazaniem przez sterownik PLC kopii informacji zgłoszeniowych otrzymywanych z komputera pokładowego tramwajów (komunikat A1).




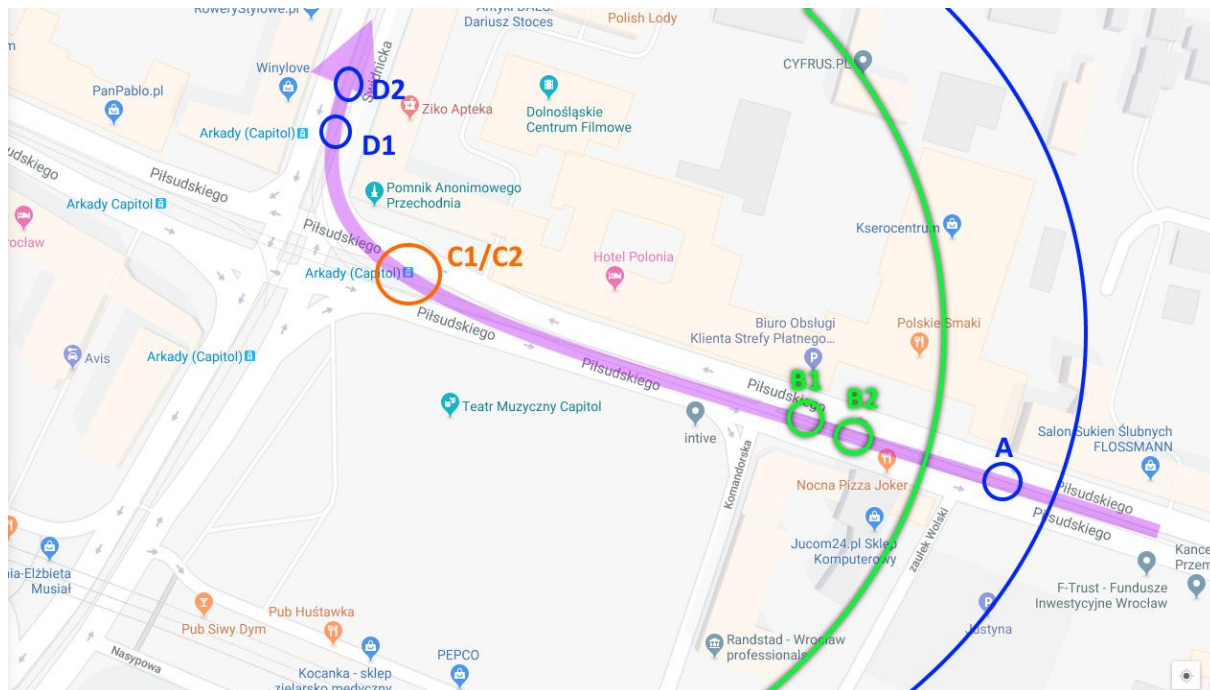
Rysunek 2 Diagram wymiany danych - przekazanie kopii zgłoszeń pojazdów ze sterownika PLC do modułu MNP

Każde otrzymane przez PLC zgłoszenie po konwersji danych jest przekazywane do MNP.

Poniższy obraz prezentuje szkic przykładowego dojazdu do skrzyżowania z zaznaczeniem charakterystycznych punktów czasowych obsługi dla przypadku, w którym tuż przed skrzyżowaniem znajduje się przystanek tramwajowy. Skala na obrazku nie jest zachowana.



<p>ZAMAWIAJĄCY:</p>  <p><b>Gmina Wrocław</b></p>	<p>Rozbudowa narzędzi informatycznych umowa TXU/TXXI/256/224/2018 Dokumentacja powykonawcza</p>	<p>Numer sygnatury 5434/05/2022</p>
---	---	---




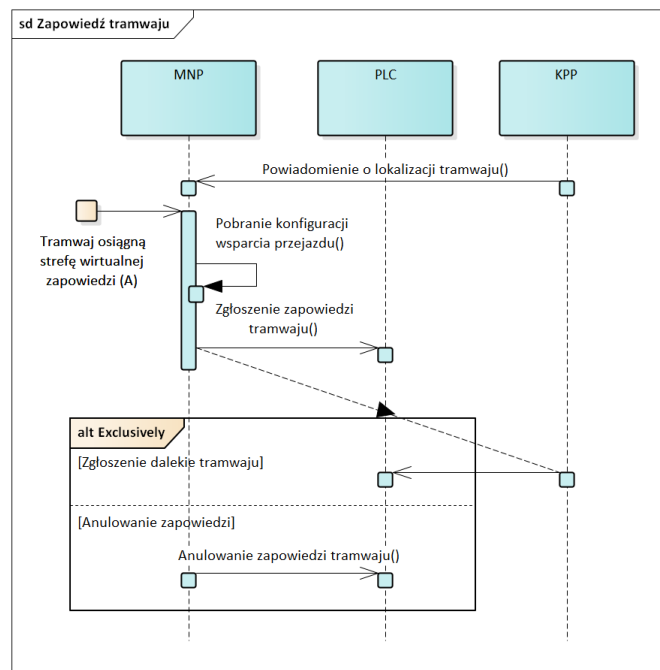
*Rysunek 3 Schemat realizacji przejazdu tramwaju z oznaczeniem lokalizacji stref detekcji*

Legenda do rysunku:

- A – punkt wysłania żądania maskowania,
- B2 – przekazanie zgłoszenia przystankowego z PLC do Systemu Sterowania Ruchem,
- B1 – przekazanie zgłoszenia przystankowego, emulowanego z MNP przez PLC do Systemu Sterowania Ruchem,
- C1 – przekazanie zgłoszenia bliskiego z PLC do Systemu Sterowania Ruchem,
- C2 – przekazanie zgłoszenia bliskiego, emulowanego z MNP przez PLC do Systemu Sterowania Ruchem,
- D1 – przekazanie zgłoszenia zjazdu z PLC do Systemu Sterowania Ruchem,
- D2 – przekazanie zgłoszenia zjazdu, emulowanego z MNP przez PLC do Systemu Sterowania Ruchem.

Poniższy diagram prezentuje scenariusz komunikacji związany z przekazaniem zapowiedzi tramwaju dla skrzyżowania ITS w punkcie A. Wejście tramwaju w strefę niebieską inicjuje proces wysłania zapowiedzi tramwaju.

<b>ZAMAWIAJĄCY:</b>  <b>Gmina Wrocław</b>	<b>Rozbudowa narzędzi informatycznych</b> <b>umowa TXU/TXXI/256/224/2018</b> <b>Dokumentacja powykonawcza</b>	<b>Numer sygnatury</b> <b>5434/05/2022</b>
---	---	---

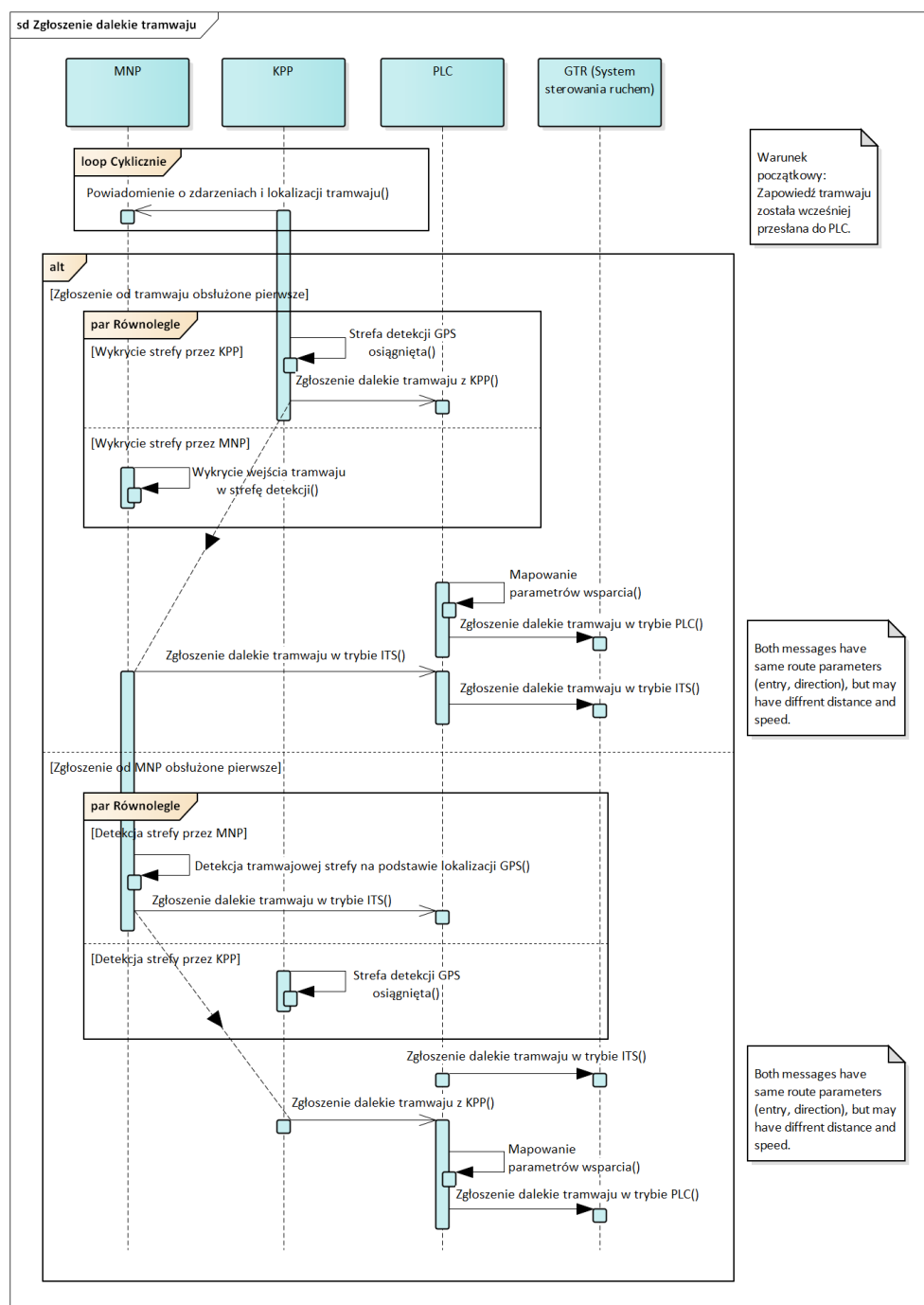


*Rysunek 4 Diagram wymiany danych - przekazanie zapowiedzi tramwaju*

Zaznaczony na diagramie przypadek odwołania zapowiedzi dotyczy sytuacji, w której tramwaj nie wykonał zapowiedzianego podejścia do skrzyżowania – np. tramwaj uległ awarii na odcinku lub zjechał z wytyczonej trasy w innym kierunku na wcześniejszym rozjeździe. Odwołanie zapowiedzi nie będzie dokonywane w sytuacji, w której tramwaj wykonuje dojazd do skrzyżowania.

Poniższy diagram prezentuje sekwencję czasową wymiany danych w ramach obsługi dalekiego zgłoszenia tramwaju.


Na diagramie uwidoczniono, że zależnie od tego, czy KPP na danym skrzyżowaniu będzie próbował wysyłać sygnały zapowiedzi, może dojść do sytuacji, że zarówno KPP, jak i MNP przekaże do PLC komunikat zgłoszenia dalekiego tramwaju (strefy B1 i B2). Sterownik PLC przyjmie oba zgłoszenia i prześle je do Systemu Sterowania Ruchem w kolejności, w jakiej je otrzymał, przy czym zgłoszenie KPP zawsze będzie zawierało skorygowane parametry kierowania (entry, direction) zgodnie z danymi przekazanymi z MNP do PLC w ramach zapowiedzi. Sytuacja przekazania komunikatu zgłoszenia przez MNP nie zostanie dokonana, o ile wcześniej PLC prześle do MNP informację o zgłoszeniu otrzymanym od KPP (komunikaty A1).

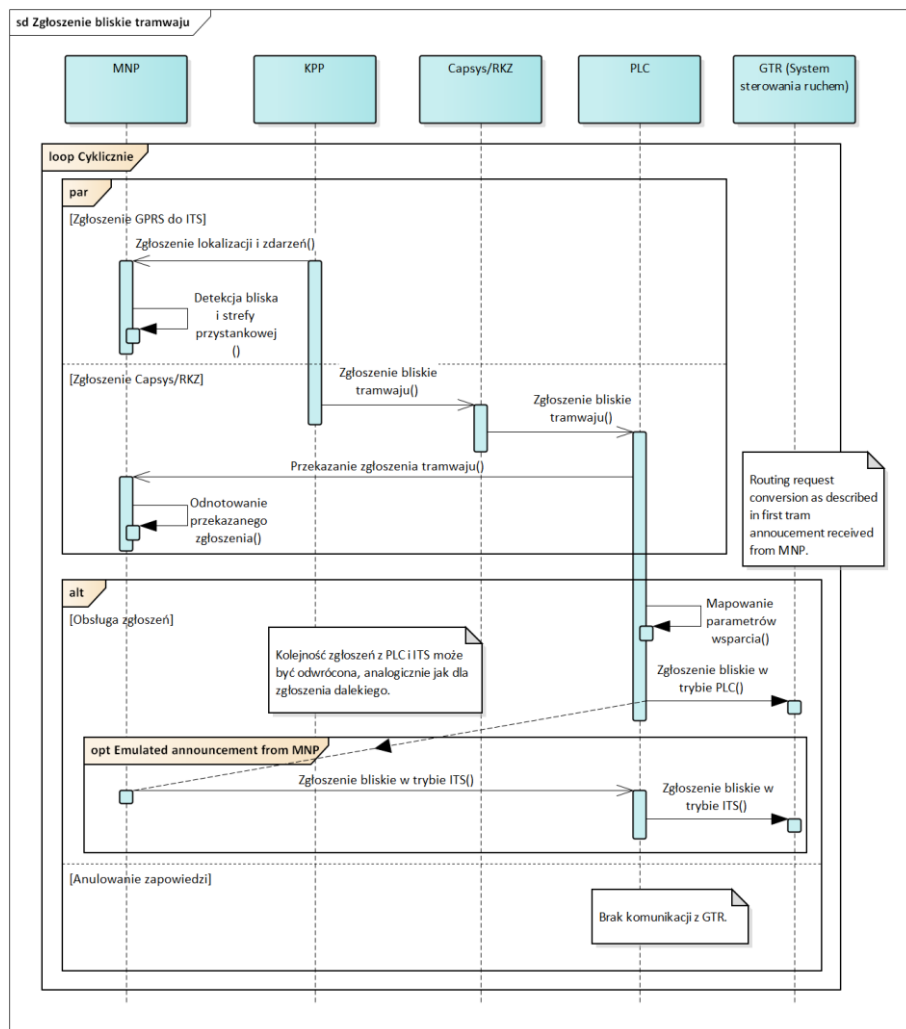


Rysunek 5 Diagram wymiany danych - obsługa zgłoszenia dalekiego tramwaju

Na diagramie pominięto szczegóły komunikacji pomiędzy komputerem pokładowym tramwaju a sterownikiem PLC za pośrednictwem urządzeń SIC oraz przypadek przekazania zgłoszeń od detektorów trakcyjnych i pętli indukcyjnych, które nie przekazują informacji o pojeździe i danych kierowania.

Na poniższym diagramie przedstawiono schemat przekazywania zgłoszeń bliskich od tramwajów.

ZAMAWIAJĄCY:  <b>Gmina Wrocław</b>	Rozbudowa narzędzi informatycznych umowa TXU/TXXI/256/224/2018 Dokumentacja powykonawcza	Numer sygnatury 5434/05/2022
--	--	---------------------------------




Rysunek 6 Diagram wymiany danych - obsługa zgłoszenia bliskiego tramwaju

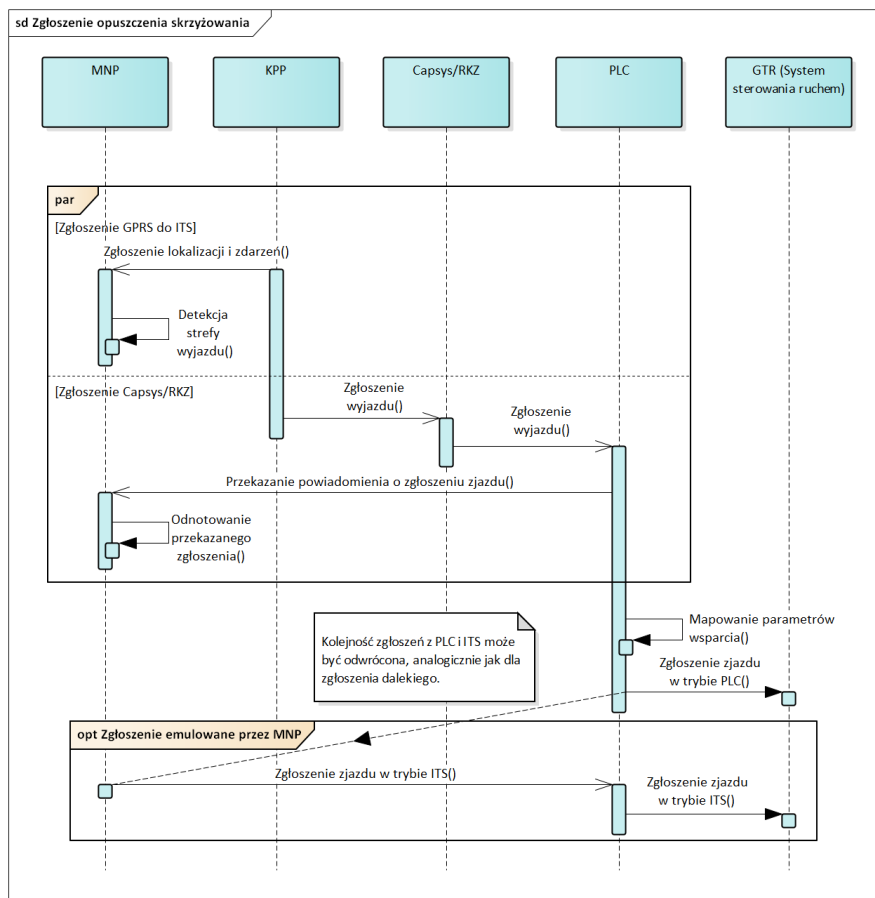
Na diagramie pokazano, że MNP przetwarza cyklicznie przekazywane z komputera pokładowego przez GPRS zgłoszenia lokalizacyjne oraz zgłoszenia przekazywane przez komputer pokładowy do sterownika PLC (kopiowanie zgłoszeń – komunikat A1).

Na diagramie pokazano, że PLC może całkowicie zamaskować wybrane zgłoszenia od tramwaju i nie przekazywać ich do Systemu Sterowania Ruchem. Będzie to miało miejsce w przypadku skrzyżowań na trasie alternatywnej, na których przystanek ma być pominięty z uwagi na błędne rozpoznanie przez KPP lokalizacji sąsiadujących przystanków przy skrzyżowaniach, przez które trasa rozkładowa przebiega w innym kierunku, niż trasa alternatywna. Z uwagi na zależności czasowe może występować sytuacja, w której zarówno zgłoszenie wygenerowane przez pojazd, jak również zgłoszenie wygenerowane przez moduł MNP zostaną przekazane do PLC, a stamtąd do Systemu Sterowania Ruchem (strefy C1/C2 oraz na obrazie trasy). Jeśli MNP otrzyma i zdąży zinterpretować komunikat o zgłoszeniu się pojazdu do sterownika PLC, to dodatkowy komunikat nie będzie wysyłany (taki wariant przedstawia diagram czasowy).


Poniższy diagram przedstawia komunikację związaną z sygnalizacją zjazdu tramwaju ze skrzyżowania.

<b>ZAMAWIAJĄCY:</b>  <b>Gmina Wrocław</b>	<b>Rozbudowa narzędzi informatycznych</b> <b>umowa TXU/TXXI/256/224/2018</b> <b>Dokumentacja powykonawcza</b>	<b>Numer sygnatury</b>
		<b>5434/05/2022</b>

Każde zgłoszenie wyjścia tramwaju ze skrzyżowania jest przekazywane do Systemu Sterowania Ruchem (z uwzględnieniem zmiany identyfikatorów entry).



Rysunek 7 Diagram wymiany danych - obsługa zgłoszenia opuszczenia przez tramwaj obszaru skrzyżowania

ZAMAWIAJĄCY:  <b>Gmina Wrocław</b>	Rozbudowa narzędzi informatycznych umowa TXU/TXXI/256/224/2018 Dokumentacja powykonawcza	Numer sygnatury 5434/05/2022
--	--	---------------------------------

## 6 Podłączenie do systemu sterowania ruchem Gertrude

### 6.1 Komunikacja GTR

Protokół komunikacyjny używany do podłączenia sterownika sygnalizacji do systemu sterowania ruchem przedstawiony został w dokumentacji powykonawczej dla zadania Inwestycyjnego: Wykonanie Inteligentnego Systemu Transportu w zakresie Projektu pn. Zintegrowany System Transportu Szynowego w aglomeracji i we Wrocławiu.

Sposób przesyłania danych opisano w dokumencie „Załącznik 07 Dokumentacji Powykonawczej Podsystemu ITS Gertrude – Protokół transmisji pomiędzy Podsystemem ITS Gertrude a sterownikami sygnalizacji świetlnej” natomiast proces podłączenia i potwierdzenia tożsamości sterowników sygnalizacji w dokumencie „Zabezpieczenia transmisji pomiędzy Podsystemem sterowania ruchem Gertrude a sterownikami sygnalizacji świetlnej.”

### 6.2 Autoryzacja GTR - opis wiadomości XYZ

Poniżej przedstawiono wiadomości uwierzytelniające wymieniane pomiędzy systemem sterowania ruchem a sterownikiem przed uruchomieniem przesyłania danych.

Zapytanie wysyłane przez system Gertrude (Wiadomość X – uwierzytelnienie) ma format:


TEDI	STX (editable ex ENQ de TEDI)	Początek tekstu	1 bajt
TEDI	rgsb or s	Adres	1 lub 4 bajty
DIASER	Message Type	‘X’	1 bajt
DIASER	Text liczby zapisane w formacie hex	klucz msg X	32 bajty
TEDI	ETX (editable)	Koniec tekstu	1 bajt
TEDI	BCC	Suma kontrolna	1 bajt

Przykładowa zawartość / kodowanie msg X (dane pokazujące format zapisu)

‘220102D3040506C708090A4B0C0D0E0F101C1213F415161748191A1B1C1D1E2F’

Sterownik sygnalizacji w odpowiedzi na wiadomość 'X' musi odpowiedzieć wiadomością 'Y' (Wiadomość Y – uwierzytelnienie) z kluczem autoryzacji (klucz msg Y) odpowiadającym zapytaniu serwera (klucz msg X) zgodnie z poniższym formatem:

TEDI	STX (editable ex ENQ de TEDI)	Początek tekstu	1 bajt
TEDI	rgsb or s	Adres	1 lub 4 bajty
DIASER	Message Type	‘Y’	1 bajt
DIASER	Text liczby zapisane w formacie hex	klucz msg y	32 bajty
TEDI	ETX (editable)	Koniec tekstu	1 bajt

<b>ZAMAWIAJĄCY:</b>  <b>Gmina Wrocław</b>	Rozbudowa narzędzi informatycznych umowa TXU/TXXI/256/224/2018 Dokumentacja powykonawcza	Numer sygnatury
		5434/05/2022

TEDI	BCC	Suma kontrolna	1 bajt
------	-----	----------------	--------

Przykładowa zawartość / kodowanie msg Y (dane pokazujące format zapisu)

'000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E2F'

W odpowiedzi na Wiadomość Y system sterowania ruchem wysyła do sterownika odpowiedź (Wiadomość Z – uwierzytelnienie) w formacie.


TEDI	STX (editable ex ENQ de TEDI)	Początek tekstu	1 bajt
TEDI	rgsb or s	Adres	1 lub 4 bajty
DIASER	Message Type	'Z'	1 bajt
DIASER	Text liczby zapisane w formacie hex	Zawartość msg Z	16 bajtów
TEDI	ETX (editable)	Koniec tekstu	1 bajt
TEDI	BCC	Suma kontrolna	1 bajt

Wysłanie 'Z' przez system Gertrude nie powoduje odpowiedzi przez sterownik.

Przykładowa zawartość / kodowanie msg Z (dane pokazujące format zapisu)

'1A1A121F1415C61718191A1B1C1D1E2F'

Po poprawnie zakończonym procesie weryfikacji następuje uruchomienie przesyłania danych z systemu sterowania ruchem do sterownika.

ZAMAWIAJĄCY:  <b>Gmina Wrocław</b>	Rozbudowa narzędzi informatycznych umowa TXU/TXXI/256/224/2018 Dokumentacja powykonawcza	Numer sygnatury 5434/05/2022
--	--	---------------------------------

## 7 Dane konfiguracyjne

Informację na temat danych konfiguracyjnych serwisów oraz ustawień sieciowych i haseł dostępowych przekazuje administrator systemu.

Poniżej przedstawiono zakres danych konfiguracyjnych.

1. „MNPserver” adres i port serwisu uwierzytelniającego MNP służącego od rejestrowania metryk oraz obsługi komunikacji MNP tcp
2. „GTRfiles” zasób IP (ftp) skąd należy pobrać pliki uwierzytelniające dla GTR
3. „MNPfiles” zasób IP (ftp) skąd należy pobrać pliki uwierzytelniające dla MNP

## 8 Terminy i wyrażenia użyte w dokumencie

**TLC (traffic light controller) lub PLC** - skrót określający sterownik sygnalizacji ulicznej lub inne urządzenie podlegające uwierzytelnianiu i/lub komunikacji szyfrowanej.

**Gertrude / GTR** - system sterowania ruchem eksploatowany w terenie (określa protokół i/lub urządzenie – serwer)

**MNP** - Moduł Nadawania Priorytetów, nazywany również modułem tras alternatywnych (MTA) system prowadzenie pojazdów transportu publicznego po wyznaczonych trasach.

**DIASER** - protokół komunikacyjny pomiędzy ITS a TLC

**Mertyka** - unikalny ciąg liczb nadawany i zdefiniowany dla danej grupy urządzeń wg dostawcy urządzeń.

MSG-X treść wiadomości pobranej z serwisu zawiera 16 liczb.

MSG-Y treść wiadomości pobranie z pliku zawierającej 16 liczb.

MSG-Z treść wiadomości kończącej uwierzytelnianie zawiera 8 liczb.

Serwis usługa serwerowa świadcząca obsługę metryki, uwierzytelniania, oraz pliki.

**?** - wartość w opisie danych/ramkach lub treści wiadomości, oznacza wartość bez znaczenia, jednakże musi być w zakresie opisanego formatu danych.

**n** - Parametr-zmienna definiowana w algorytmie liczba definiująca sposoby obliczeń dla AES.

**k** - Parametr-zmienna definiowana w algorytmie liczba definiująca sposoby obliczeń dla macierzy.

**x,y** - współrzędne liczb w macierzy wg układu kartezjańskiego

**C** - ciąg 8 liczb określający położenie odpowiedzi dla MSG-Y.

**X** - zmienna wyliczeniowa definiująca offset odpowiedzi dla MSG-Y za ciągiem "C".