

**Zabezpieczenia transmisji pomiędzy
Podsystemem sterownia ruchem Gertrude
a sterownikami sygnalizacji świetlnej
(obowiązuje dla wersji aplikacji nie starszej niż 12.02)**

Numer sygnatury
DAT/KCZ/11403/09/2018

Przygotowano dla:	Zarząd Dróg i Utrzymania Miasta ul. Długa 49, 53-633 Wrocław
Wersja:	1.0
Ostatnio zmodyfikowano:	21-09-2018
Autor:	Krzysztof Czarniecki WASKO S.A. ul. Berbeckiego 6, 44-100 Gliwice

Metryka dokumentu

Tytuł dokumentu:	Zabezpieczenia transmisji pomiędzy Podsystemem sterownia ruchem Gertrude a sterownikami sygnalizacji świetlnej		
Autor(rzy):	Krzysztof Czarnecki	Numer wersji dokumentu:	1.0
Adres mailowy autora(ów):	K.Czarnecki@wasko.pl		
Klauzula poufności:	Tak	Data stworzenia dokumentu:	21-09-2018

Historia dokumentu

Nr wersji	Data wersji	Autor zmiany	Komentarz/Uwagi/Zakres zmian
1.0	21-09-2018	Krzysztof Czarnecki	Utworzenie dokumentu

Spis treści

1	Informacje podstawowe	4
2	Opis działania	5
2.1	Weryfikacja tożsamości.....	6

Spis tabel

Tabela 1	Zapytanie o autoryzację sterownika	6
Tabela 2	Potwierdzenie tożsamości	6
Tabela 3	zapytanie o autoryzację systemu	6

1 Informacje podstawowe

W dokumencie przedstawiono proces podłączenia i potwierdzenia tożsamości sterowników sygnalizacji ulicznej do systemu sterowania ruchem oraz innych zabezpieczeń mających na celu zapewnienie bezpieczeństwa komunikacji. pomiędzy podsystemem sterowania ruchem a sterownikami sygnalizacji ulicznej.

Mechanizmy kontroli mają na celu potwierdzenie, że podłączane do produkcyjnie uruchomionego systemu urządzenie jest w pełni kompatybilne i nie powoduje ryzyka zaburzeń lub awarii w pracy systemu sterowania ruchem w efekcie których może wystąpić zagrożenie dla uczestników ruchu.

Protokół transmisji pomiędzy Podsystemem ITS Gertrude a sterownikami sygnalizacji świetlnej oraz ich znaczenie nie ulegają zmianie.

Informacje wrażliwe niosące ryzyko uzyskania nieautoryzowanego dostępu takie jak metody odszyfrowania danych, struktury komunikatów autoryzacji zostały w dokumencie pominięte. Dostęp do tych informacji jest możliwy po podpisaniu stosownej umowy o zachowaniu poufności (non-disclosure agreement – NDA) z producentem systemu:

GERTRUDE SAEM

9, rue de Ségur

33000 Bordeaux, France

Tél : +33 (0) 556 993 020

Mail : contact@gertrude.fr

Site : www.gertrude.fr

2 Opis działania

W celu dokonania autoryzacji urządzenia należy z serwera systemu sterowania ruchem pobrać pliku autoryzacji zawierający m.in. pytania i spodziewane odpowiedzi używane do weryfikacji tożsamości strony podłączającej się (sterownik sygnalizacji ulicznej).

W pliku zapisywane są możliwe kody autoryzacyjne pytanie – odpowiedź oraz dane zabezpieczenia transmisji.

Charakterystyka pliku autoryzacji:

1. Plik jest generowany na nowo nie częściej niż co 15 minut. W przypadku gdy w udostępnianym zasobie znajduje się więcej plików autoryzacji, wówczas należy użyć najnowszego.
2. Plik nie posiada zadeklarowanej długości (zmienna)
3. Plik jest skompresowany
4. Dane w pliku są zaszyfrowane zmiennym hasłem
5. Plik zawiera informacje niezbędne do przeprowadzenia uwierzytelnienia i zabezpieczenia (szyfrowania) transmisji danych pomiędzy systemem i sterownikiem. W zależności od metody zabezpieczeń narzuconym przez serwer sterownia ruchem i dotyczą one:
 - a. dane pytań i spodziewanych odpowiedzi (faza uwierzytelnienia). Kody autoryzacyjne to ciąg 16 liczb oddzielanych przecinkami, w pliku znajduje się min. 800 tys. możliwych kodów autoryzacyjnych.
 - b. dane metody kodowania transmisji ECC (eliptic curve crypograh) kody map ECC dla fazy kodowania/dekodowania - odczyt wg indeksu i długości map.
 - c. dane metody kodowania transmisji AES256 (metoda kodowania transmisji) dane kluczy 256 bitowych (faza kodowania) odczyt wg indeksu i długości
 - d. dane kluczy kodowania transmisji wg standardu RSA (klucz prywatny, publiczny) odczyt wg indeksu i długości kluczy
 - e. dane kluczy dla metody kodowania transmisji Trivium - odczyt wg indeksu i długości kluczy

2.1 Weryfikacja tożsamości

Poniżej przedstawiono strukturę komunikatów wykorzystywanych do weryfikacji urządzeń

Zapytanie: zapytanie systemu o potwierdzenie tożsamości sterownika

TEDI	STX	Początek tekstu	1 bajt
TEDI	rgsb or s	Adres	1 lub 4 bajty
DIASER	Message Type	88	1 bajt
DIASER	Message	Teść zapytania format	n bajtów
TEDI	ETX	Koniec tekstu	1 bajt
TEDI	BCC	Suma kontrolna	1 bajt

Tabela 1 Zapytanie o autoryzację sterownika

Odpowiedź: Odpowiedz sterownika na zapytanie systemu o potwierdzenie tożsamości sterownika:

TEDI	STX	Początek tekstu	1 bajt
TEDI	rgsb or s	Adres	1 lub 4 bajty
DIASER	Message Type	88	1 bajt
DIASER	Message	Teść zapytania format	n bajtów
TEDI	ETX	Koniec tekstu	1 bajt
TEDI	BCC	Suma kontrolna	1 bajt

Tabela 2 Potwierdzenie tożsamości

Zapytanie: Poniżej przedstawiono strukturę komunikatu wykorzystywanego do weryfikacji systemu sterowania ruchem:

TEDI	STX	Początek tekstu	1 bajt
TEDI	rgsb or s	Adres	1 lub 4 bajty
DIASER	Message Type	90	1 bajt
DIASER	Message	Teść zapytania format	n bajtów
TEDI	ETX	Koniec tekstu	1 bajt
TEDI	BCC	Suma kontrolna	1 bajt

Tabela 3 zapytanie o autoryzację systemu

n-oznacza zmienną liczbę bajtów (ustawiana dynamicznie) typowo 32 bajty

Przykład:

Poniżej przedstawiono przykładowy format zapytania/odpowiedzi (przykład kodowania) :

Struktura wiadomości *[STX][R][G][S][B][Message][ETX][BCC]*

kodowanie message przykład:

*21F**02111567805**348245*22FA340F*

kodowanie odpowiedzi message

*41A*0*21AC534421*3*48*45*540A4*2*