

Standard wymiany danych dla Urzędów rejestrujących

Wersja 1.4

1 Spis treści

Standard wymiany danych dla Urzędów rejestrujących	1
1 Spis treści	1
2 Definicje	2
2.1 Terminologia z zakresu dziedziny problemu	2
2.2 Terminy technologiczne	2
3 Przyjęte założenia	3
3.1 Ogólna koncepcja wymiany informacji	3
3.2 Założenia dotyczące roli Urzędów rejestrujących	3
3.3 Założenia dotyczące przyjętych technologii	4
3.4 Założenia dotyczące bezpieczeństwa	5
3.5 Założenia dotyczące dostępności	5
4 Wymagania na Urządzenia rejestrujące	5
4.1 Zapewnienie komunikacji	5
4.2 Zapewnienie autentyczności dowodu	6
4.3 Parametry Urządzenia	6
4.4 Obsługiwane zdarzenia	8
4.5 Kontrola warunków pracy Urządzenia	9
4.5.1 Synchronizacja czasu	9
4.5.2 Zgłoszenia stanu pracy	9
4.5.3 Ustawienia parametrów pracy Urządzenia	9
4.5.4 Wykrywanie funkcjonalności Urządzenia	9
5 Wykorzystanie infrastruktury PKI	9
5.1 Sposób tworzenia sygnatury dowodu	10
6 Wymagania na centralę	10
7 Opis protokołu	10
7.1 Warstwa sieciowa	11
7.1.1 Urządzenie w trybie off-line	12
7.2 Warstwa protokołu transportowego	12
7.3 Składnia zdalnych wywołań	13
7.3.1 Alerty, zlecenia i kwerendy	13
7.3.2 Pobieranie dowodu	14
8 Definicje komunikatów	15
8.1 Format dowodu	15
8.1.1 Struktura dowodu	16
8.1.2 Format manifestu	16
8.1.3 Wytworzenie dowodu	20
8.1.4 Weryfikacja sygnatury dowodu	20
8.1.5 Pliki natywne dowodu, inne obrazy i filmy	20
8.2 Alerty	21
8.2.1 Zgłoszenie obecności dowodu	21
8.2.2 Zgłoszenie przekroczenia wartości parametru	21
8.2.3 Zgłoszenie naruszenia integralności Urządzenia	22
8.2.4 Zgłoszenie przepełnienia bufora	22
8.2.5 Zgłoszenie restartu Urządzenia	22

8.2.6	Dostarczanie informacji statystycznej.....	23
8.2.7	Inne zgłoszenia.....	24
8.3	Odpowiedzi do kwerend.....	24
8.3.1	Wykrywanie funkcjonalności Urządzenia	24
8.3.2	Zapytanie o parametr.....	28
8.4	Zlecenia	28
8.4.1	Format podstawowy	29
9	Scenariusze użycia	30
9.1	Zapytanie o właściwości Urządzenia	30
9.2	Obsługa dowodu.....	31
9.3	Zgłoszenie stanu pracy Urządzenia/alertu	32
9.4	Odpytanie o stan parametrów	33
9.5	Modyfikacja parametru pracy Urządzenia	33
9.6	Obsługa informacji statystycznych.....	35
10	Zasady weryfikacji zgodności ze standardem.....	36

2 Definicje

2.1 Terminologia z zakresu dziedziny problemu

Urządzenie rejestrujące – w niniejszym dokumencie każde Urządzenie wykorzystywane do wykrywania i rejestrowania wykroczeń popełnianych przez uczestników ruchu drogowego. W czasie powstawania obecnej wersji dokumentu znane były trzy typy Urządzeń rejestrujących: Urządzenia do pomiaru prędkości chwilowej (tak zwane fotoradary), Urządzenia do pomiaru prędkości odcinkowej oraz Urządzenia do wykrywania przejazdu na czerwonym świetle. Urządzenia rejestrujące przesyłają do centrali przetwarzania dowody wykrytych i zarejestrowanych wykroczeń.

Dowód – zbiór informacji dokumentujących fakt zaistnienia naruszenia. Dowód jest przesyłany przez Urządzenia do centrali przetwarzania. Następnie jest wykorzystywany w postępowaniu przedprocesowym oraz ewentualnie w sądzie.

Centrala przetwarzania – (również w krótszej formie jako „centrala”) system informatyczny przeznaczony do gromadzenia i przetwarzania dowodów dostarczanych przez Urządzenia rejestrujące. Rolą centrali jest wykrycie sprawy naruszenia udokumentowanego dowodem.

Dostawca Urządzenia rejestrującego – producent Urządzenia rejestrującego. Dostawca nie ma dostępu do Urządzenia i przetwarzanych na nim danych podczas normalnej eksploatacji. Dostawca ustawia pewne elementy Urządzenia i jako jedyny ma możliwość ich zmiany.

Administrator Urządzenia rejestrującego – osoba konfiguruje Urządzenie rejestrujące i odpowiadająca za jego właściwą pracę. Ustawia parametry pracy Urządzenia w czasie jego normalnej eksploatacji. Nie posiada praw umożliwiających zmianę niektórych parametrów Urządzenia (np. klucza do podpisywania).

2.2 Terminy technologiczne

RSA – Algorytm umożliwiający realizację kryptografii asymetrycznej. Sposób użycia opisany jest w standardzie PKCS#1.

JSON – Tekstowy format danych. Opisany w standardzie RFC 4627.

OpenVPN – projekt realizacji wirtualnej sieci prywatnej bazujący w zakresie bezpieczeństwa na protokole TLS (tak zwany SSL VPN). OpenVPN to zarówno protokół komunikacji jak i realizujące go oprogramowanie na licencji GPL. Strona WWW: <http://openvpn.net/>.

OpenSSL – projekt implementacji algorytmów kryptograficznych. Strona WWW: <http://www.openssl.org/>.

3 Przyjęte założenia

Niniejsze opracowanie opisuje wymagania na Urządzenie rejestrujące i centralę przetwarzania w zakresie funkcjonalności obsługiwanych przez obie strony. Szczególna uwaga przyłożona jest do Urządzeń rejestrujących co wynika z faktu, że to właśnie one są odpowiedzialne za wykrycie naruszenia i wytworzenie na to dowodu. Jednocześnie, Urządzenia rejestrujące posiadają stosunkowo niewielką moc obliczeniową (komputery *embedded*), są wytwarzane przez różnych producentów oraz docelowo zlokalizowane w terenie (przy drogach i na skrzyżowaniach). Koncepcja musi uwzględniać zatem zarówno rolę jak i ograniczenia tych Urządzeń.

W kolejnych sekcjach niniejszego rozdziału przedstawiono założenia przyjęte do wypracowania standardu wymiany danych dla Urządzeń rejestrujących.

3.1 Ogólna koncepcja wymiany informacji

Przyjmuje się, że Urządzenie komunikuje się z centralą za pośrednictwem tunelu VPN.

Komunikacja wewnątrz tunelu realizowana jest w oparciu o protokół HTTP 1.1 w konwencji REST.

Strony (centrala i Urządzenie) przekazują sobie komunikaty w formacie JSON. Specyfikacja komunikatów pozwala Urządzeniu przysyłać alerty do centrali a centrali wykonywać zlecenia zmian konfiguracyjnych Urządzenia oraz kwerendy do Urządzenia.

Centrala może również pobierać dowody wykroczeń pobierając je metoda HTTP GET z Urządzenia a następnie zlecając ich usunięcie metodą HTTP DELETE.

Dowody naruszeń są udostępniane centrali w formacie archiwum 7-zip zawierającym opis zdarzenia i materiały dowodowe – zdjęcia i ewentualnie filmy.

W celu zapewnienia integralności dowodu wszystkie pliki są podpisane prywatnym (niejawnym) kluczem Urządzenia.

Proces dostarczenia dowodu z Urządzenia do centrali jest wieloetapowy:

- W momencie wykrycia naruszenia Urządzenie stara się wysłać do centrali „alert” informujący o tym fakcie (HTTP POST z Urządzenia na centralę),
- Centrala niezwłocznie po odebraniu alertu próbuje pobrać dowód w razie potrzeby wznowiając transmisję od miejsca, w którym ta została przerwana ewentualną awarią (HTTP GET z centrali do Urządzenia),
- Centrala po kompletnym pobraniu dowodu informuje Urządzenie o tym, że dowód może być już usunięty (HTTP DELETE z centrali do Urządzenia).

3.2 Założenia dotyczące roli Urządzeń rejestrujących

Przyjmuje się, że Urządzenia rejestrujące wykrywają sytuację na drodze kwalifikującą się jako określonego rodzaju naruszenie. Urządzenie rejestruje dowód tego naruszenia w skład którego wchodzi zdjęcie lub zdjęcia sytuacji na drodze oraz informacja opisująca zobrazowaną sytuację, w tym data i czas zdarzenia czy zarejestrowana prędkość. Fakt pojawienia się nowego dowodu (dowód – czyli obrazy i informacja opisująca) jest niezwłocznie zgłaszany do centrali przetwarzania. Ta podejmuje próbę pobrania dowodu.

Urządzenie buforuje uzyskane dowody do czasu potwierdzenia przez centralę ich pobrania. W przypadku przepełnienia bufora Urządzenie przestaje gromadzić kolejne dowody zgłaszając podczas wykrycia naruszenia alerty z informacją o utracie dowodu do centrali.

Przyjmuje się, że Urządzenia działają bez bezpośredniego nadzoru i muszą w związku z tym zgłaszać automatycznie do centrali przetwarzania wszystkie problemy wymagające interwencji człowieka. Urządzenia muszą również odpowiadać centrali przetwarzania na zadane zapytania i wykonywać przesłane polecenia (np. zmiana wartości parametru).

Pojedyncze paczki danych (komunikaty, dowody wykroczeń) nie stanowią informacji niejawnej w rozumieniu obowiązujących w RP przepisów prawa.

3.3 Założenia dotyczące przyjętych technologii

Urządzenia rejestrujące wytwarzane są przez różnych producentów i z wykorzystaniem różnych technologii. W związku z tym opracowana koncepcja wymiany danych powinna wymagać rozwiązań, które przez swą prostotę i uniwersalność mogą być przez każdego z producentów zaimplementowane zbliżonym nakładem pracy. Przyjęte rozwiązania są niezależne od platformy sprzętowo-programowej i mogą być zrealizowane z wykorzystaniem ogólnodostępnych nieodpłatnych bibliotek lub samodzielnej implementacji.

Komunikacja bazuje na popularnych protokołach i formatach danych, takich jak HTTP/1.1 czy JSON. W związku z tym, że komunikacja może odbywać się po sieciach bezprzewodowych o stosunkowo niewielkich przepustowościach a ponadto rozliczanych proporcjonalnie do ilości przetransferowanych danych, kluczowe jest minimalizowanie rozmiaru transferowanych danych. Dane są więc kompresowane tam gdzie ma to sens za pomocą algorytmu Deflate (RFC 1951) lub LZMA (patrz <http://7-zip.org/7z.html>). Dane w formatach realizujących kompresję (np. JPEG) nie powinny być ponownie kompresowane metodą Deflate lub LZMA aby nie obciążać niepotrzebnie procesora Urządzenia.

Tam gdzie potrzebne jest archiwum plików (patrz format dowodu) zastosowano 7z (patrz <http://7-zip.org/7z.html>). Kontener w tym formacie umożliwia stosowanie wielu typów kompresji, w tym LZMA¹.

Elementy rozwiązania wymagające kryptografii bazują na popularnych i ogólnie dostępnych algorytmach. Istnieją gotowe implementacje umożliwiające ich nieodpłatne użycie w komercyjnych rozwiązaniach.

Do zawiązania tunelu VPN stosowane jest oprogramowanie OpenVPN. Umożliwia ono realizację wirtualnej sieci pomiędzy Urządzeniami a centralą. Zaletą wybranego podejścia jest obecność pakietu na wielu platformach (otwarte źródła i licencja GPL umożliwiają przenoszenie go na kolejne) oraz prawidłowa obsługa różnych trybów pracy sieci (np. NAT, firewall, zmienne adresy IP) a także stosunkowo mały narzut na rozmiar transmitowanych danych i ich opóźnienie.

Przyjęto, że do wykonania operacji wszystkich kryptograficznych wystarczający jest pakiet oprogramowania OpenSSL (OpenVPN bazuje w zakresie kryptografii na OpenSSL). Zaprezentowane w dokumencie przykłady składania czy weryfikacji podpisu posługują się wręcz uruchamianymi z linii poleceń komendami programu openssl. Biblioteka OpenSSL umożliwia delegowanie operacji kryptograficznych do urządzeń sprzętowych (kart kryptograficznych lub HSM) z wykorzystaniem dedykowanych implementacji silników (engine) lub poprzez interfejs PKCS#11.

Unika się wykorzystania formatu danych XML ponieważ szereg możliwości tego języka jest w opisywanym zastosowaniu nadmiarowy a powoduje często konieczność stosowania złożonych i niepotrzebnie konsumujących zasoby interpreterów.

W trakcie pracy nad dokumentem przyjęto, że implementacja na większości platform sprzętowych i operacyjnych możliwa jest z wykorzystaniem następujących pakietów:

- OpenVPN w wersji 2.2 (realizacja tunelu VPN),
- OpenSSL w wersji 0.9.8 (realizacja usług kryptograficznych),
- LZMA SDK w wersji 9.20 (obsługa algorytmów kompresji i archiwum 7z),
- Python w wersji 3.2 (implementacja kodu, obsługa protokołu http i formatu JSON).

Nie istnieje wymaganie zastosowania żadnego z powyższych komponentów programistycznych, ale wykorzystanie trzech pierwszych pozycji jest rekomendowane.

¹ Poza przewagą technologiczną, kontener 7z ma jaśniejszą sytuację licencyjną niż popularny format ZIP.

3.4 Założenia dotyczące bezpieczeństwa

Cały ruch pomiędzy Urządzeniami rejestrującymi a Systemem Centralnym odbywa się w szyfrowanym tunelu VPN. Urządzenia rejestrujące nie udostępniają żadnych usług sieciowych poza siecią wykreowaną w ramach VPN. Oznacza to, że tylko centrala przetwarzania może nawiązywać połączenia do Urządzenia.

Istnienie VPN gwarantuje integralność i poufność transmisji bez względu na wykorzystywane protokoły – protokoły nie muszą więc dostarczać niezależnie mechanizmów integralności i poufności transmisji.

Każdy dowód jest kryptograficznie podpisany przez Urządzenie kluczem prywatnym przechowywanym w Urządzeniu.

Urządzenie jest skonstruowane w ten sposób, że bez jego uszkodzenia lub pozostawienia trwałych śladów nie jest możliwe pozyskanie klucza prywatnego lub użycie klucza prywatnego w sposób inny niż jako integralna składowa procesu wytworzenia dowodu.

Klucz publiczny (odpowiedni dla klucza prywatnego) jest udostępniany przez Urządzenie i stanowi jego (równoległy do numeru seryjnego) unikatowy identyfikator.

Centrala generuje certyfikat dla klucza każdego Urządzenia przeznaczonego do pracy. Certyfikat poza kluczem publicznym Urządzenia zawiera informacje takie jak numer seryjny Urządzenia, planowana lokalizacja Urządzenia i okres pracy Urządzenia w danym miejscu. Certyfikat jest później wznawiany lub wycofywany jeśli Urządzenie zmienia lokalizację.

Urządzenie nigdy nie otrzymuje i nie przetwarza w żaden sposób certyfikatu. Nie musi więc znać formatu ani szczegółów dotyczących jego zawartości.

Nowo wprowadzane Urządzenia muszą mieć inne klucze niż używane kiedykolwiek w przeszłości (klucze nie mogą się powtarzać).

Niezależnie od kluczy służących podpisywaniu dowodów naruszeń Urządzenia otrzymają (w postaci plików) klucze do nawiązywania tunelu VPN.

3.5 Założenia dotyczące dostępności

Protokół zakłada, że od żadnego elementu systemu (centrala, Urządzenie) nie wymaga się dostępności przekraczającej 99,9%. Oznacza to, że komponenty muszą poprawnie obsługiwać awarie drugiej strony czy też jej niedostępność.

Produkcyjny system założy maksymalne rozmiary dla komunikatów i dowodów. Komunikaty większe od założonego limitu będą odrzucane. Limit zostanie dobrany tak, aby nie przeszkadzał w normalnej pracy systemu.

4 Wymagania na Urządzenia rejestrujące

4.1 Zapewnienie komunikacji

Urządzenia i centrala starają się utrzymywać działające połączenie sieciowe. Komunikacja realizowana jest wewnątrz tunelu VPN.

Przewiduje się jednak, że w skutek różnych awarii komunikacja sieciowa może być przerwana. W związku z tym:

- Urządzenia rejestrujące posiadają bufor, w którym przechowywane są wytworzone dowody. Dowód jest usuwany z bufora dopiero po potwierdzeniu przez centralę jego prawidłowego pobrania lub po przekroczeniu pojemności bufora.
- Po odzyskaniu połączenia Urządzenie raportuje błędne stany, które miały miejsce podczas braku dostępności centrali. Zakłada się przy tym, że Urządzenie buforuje tylko jeden – ostatni

– komunikat określonego typu (przykład: jeśli podczas niedostępności centrali miało miejsce kilkukrotne przekroczenie rozmiaru bufora spowodowane tym, że powstawał kilkukrotnie dowód, to centrala po odzyskaniu połączenia jest informowana o tym fakcie tylko raz).

- Proces pobierania dowodu jest zorganizowany w ten sposób, że możliwe jest wznowianie transferu (pobieranie metodą HTTP GET i obsługa rozdziału 14.35 w RFC 2616 – Nagłówki „Range”).
- Urządzenie przechowuje ustaloną liczbę nieprzesłanych alertów danego typu i wysyła je niezwłocznie po odzyskaniu połączenia.

4.2 Zapewnienie autentyczności dowodu

Każdy wytworzony przez Urządzenie dowód jest podpisany prywatnym kluczem Urządzenia. Klucz jest niedostępny w żaden sposób dla administratora Urządzenia.

Centrala zarządza listami aktywnych Urządzeń (czyli aktywnych kluczy).

Urządzenie utrzymuje licznik wytworzonych dowodów. Każdy dowód jest oznaczony unikalnym dla tego Urządzenia identyfikatorem. Możliwe jest wykrycie luk w sekwencji dowodów.

4.3 Parametry Urządzenia

Urządzenie musi obsługiwać no najmniej następujące parametry:

Nazwa	Znaczenie	Warianty wartości	Zapis	Wymagalność:		
				W – wymagany	X – nie występuje	
				miar-punktow	miar-odcinko	czerwone-swiatlo
rodzaj	Typ Urządzenia. Możliwe wartości, to <ul style="list-style-type: none"> • “miar-punktowy”, • “miar-odcinkowy” i • “czerwone światło”. 	NIE	NIE	W	W	W
numer-seryjny	Numer seryjny Urządzenia	NIE	NIE	W	W	W
lokalizacja	Identyfikator lokalizacji Urządzenia. Wartość wprowadzana przez administratora.	NIE	TAK	W	W	W
gps	Sentencja GPBGA zgodna z formatem NMEA-183 opisująca pozycję Urządzenia odczytaną z GPS.	NIE	NIE	W	W	W
limit	Limit prędkości w miejscu pracy Urządzenia (w km/h).	TAK	TAK	W	W	X

	Największa dopuszczalna prędkość.					
próg	Próg wyzwalacza Urządzenia (w km/h). Najmniejsza prędkość traktowana jako naruszenie.	TAK	TAK	W	W	X
temp	Temperatura pracy Urządzenia. Urządzenie generuje alerty jeśli temperatura przekroczy parametr temp-min lub temp-max.	NIE	NIE	W	X	X
temp-min	Minimalna dopuszczalna temperatura pracy Urządzenia.	NIE	TAK	W	X	X
temp-max	Maksymalna dopuszczalna temperatura pracy Urządzenia.	NIE	TAK	W	X	X
klucz	Klucz publiczny (RSA) w formacie PEM	NIE	NIE	W	W	W
limit-alertów	Liczba alertów każdego typu, która ma być zbuforowana na Urządzeniu w sytuacji, gdy nie ma połączenia z centralą.	NIE	TAK	W	W	W
następny-id	Kolejny identyfikator dowodu do nadania	NIE	NIE	W	W	W
statystyki	Włączenie lub wyłączenie gromadzenia informacji o przejeżdżających pojazdach. Wartość „tak” oznacza włączenie”, „nie” – wyłączenie. Urządzenie przesyła dane o pojazdach z częstotliwością od kwadransa do godziny regulowaną automatycznie przez Urządzenie w zależności od ruchu i obciążenia łącza.	NIE	TAK	W	W	X
dowody	Liczba dowodów pozostających do nadania	NIE	NIE	W	W	W
aktywny	Oznaczenie stanu urządzenia – faktu rejestracji pomiarów. W przypadku wartości „false”: <ul style="list-style-type: none"> • Urządzenie nie może dokonywać pomiarów i nie może zbierać danych statystycznych. 	NIE	TAK	W	W	W

	<ul style="list-style-type: none"> • Urządzenie musi obsługiwać wszystkie kwerendy i zlecenia. 					
opóźnienie	Czas opóźnienia rozpoczęcia rejestracji od momentu zapalenia się czerwonego światła na sygnalizatorze.	NIE	TAK	X	X	W
opis-kierunku-t-p	Opis kierunku „tył” – „przód” dla pomiaru odcinkowego np.: „Warszawa – Gdańsk” Inicjalnie na urządzeniu musi zostać ustawiona wartość zgodnie z zapisami w Centrali.	NIE	TAK	X	W	X
opis-kierunku-p-t	Opis kierunku „przód” – „tył” dla pomiaru odcinkowego np.: „Gdańsk – Warszawa” Inicjalnie na urządzeniu musi zostać ustawiona wartość zgodnie z zapisami w Centrali.	NIE	TAK	X	W	X

Każdy parametr spoza powyższego zbioru jest rozszerzeniem producenta i musi rozpoczynać się od znaków „x-”, np. hipotetyczne „x-cpuload” – obciążenie procesora Urządzenia.

„TAK” w kolumnie „Warianty wartości” oznacza, że można skonfigurować wartość w różnych wariantach zależnie od czasu, kierunku lub kategorii pojazdu.

4.4 Obsługiwane zdarzenia

Urządzenie potrafi rozpoznać co najmniej następujące zdarzenia:

- Przepełnienie bufora Urządzenia – sytuacja, w której nieodbierane dowody zapełniają całą dostępną przestrzeń bufora,
- Naruszenie integralności Urządzenia – sytuacja, w której wykrywana jest dowolne zdarzenie rodzące podejrzenie, że integralność Urządzenia została naruszona.
- Restart Urządzenia – każde uruchomienie Urządzenia skutkuje wysłaniem informacji o tym do centrali.

4.5 Kontrola warunków pracy Urządzenia

4.5.1 Synchronizacja czasu

System działa w oparciu o czas UTC.

Urządzenie może posiadać własne źródło czasu (bazujące na wzorcu rozgłaszanym radiowo). Jeśli nie posiada, musi synchronizować czas z centralą w oparciu protokół NTP (RFC 1305). Centrala wystawia adresy co najmniej dwu serwerów NTP. Urządzenie musi posiadać funkcje umożliwiające konfigurację serwerów NTP.

Synchronizacja czasu odbywa się w tunelu VPN.

Centrala posiada niezawodne źródło czasu (np. wzorzec czasu z GUM).

4.5.2 Zgłoszenia stanu pracy

Każda sytuacja awaryjna lub wskazująca na nieprawidłowe lub podejrzanе zachowanie dowolnego elementu Urządzenia rejestrującego jest zgłaszane do centrali.

Urządzenia posiadają listę parametrów pracy wraz z konfigurowalnymi progami poprawności pracy. Przekroczenie dozwolonych wartości skutkuje przesłaniem alertu do centrali.

4.5.3 Ustawienia parametrów pracy Urządzenia

Urządzenie udostępnia funkcjonalność umożliwiającą zdalną zmianę jego parametrów z centrali.

Urządzenie, w zależności od swojego typu, udostępnia właściwą listę parametrów.

4.5.4 Wykrywanie funkcjonalności Urządzenia

Jedna z funkcji Urządzenia udostępnia całą informację o Urządzeniu. Informacja obejmuje:

- Typ Urządzenia,
- Listę ustawianych parametrów pracy,
- Rozszerzenia producenta Urządzenia.

5 Wykorzystanie infrastruktury PKI

System wykorzystuje infrastrukturę PKI na dwa sposoby:

- Uwierzytelnianie w tunelu VPN,
- Sygnatura cyfrowa pod dowodem naruszenia,

Do obu trybów wykorzystuje się rozdzielna pary kluczy RSA.

System (Urządzenia i centrala) stosuje klucze o długości 2048 bitów i funkcję skrótu SHA-2 (256 bitów). Sygnatury realizowane są zgodnie z PKCS#1 w wersji 1.5.

Na potrzeby uwierzytelniania w tunelu VPN centrala utrzymuje minimalną infrastrukturę niezbędną do wygenerowania certyfikatu CA oraz generuje klucze i certyfikaty dla poszczególnych Urządzeń.

Klucze i certyfikaty Urządzenia są przygotowane w postaci plików w formatach obsługiwanych przez OpenVPN. Administrator instaluje je na Urządzeniu podczas jego konfiguracji.

Para kluczy do składania i weryfikacji sygnatury pod dowodem obsługiwana jest w inny sposób:

- Urządzenie posiada unikatowy klucz prywatny przechowywany na Urządzeniu w sposób uniemożliwiający jego pozyskanie skopiowanie lub użycie,
- Urządzenie zwraca klucz publiczny jeśli otrzyma właściwe polecenie,
- Urządzenie podpisuje każdy dowód kluczem prywatnym zgodnie z wymaganym formatem.

Klucze do podpisów są nierozdzielnie związane z Urządzeniem. Ten sam klucz na dwu Urządzeniach traktowany jest jako usterka Urządzeń uniemożliwiająca ich wykorzystanie.

Administrator ani osoby postronne nie mogą uzyskać jakiegokolwiek dostępu do klucza prywatnego bez pozostawienia trwałych śladów takiej operacji lub uszkodzenia Urządzenia.

Zaleca się, aby Urządzenie przechowywało klucz prywatny na dedykowanym komponencie technicznym spełniającym wymagania Urządzeń zgodnych z FIPS 140-2 poziom 3 lub adekwatny profil Common Criteria.

5.1 Sposób tworzenia sygnatury dowodu

Sygnatura tworzona jest na dowodzie jako skrót SHA-256 zaszyfrowany kluczem RSA 2048 bitów zgodnie z PKCS#1 w wersji 1.5.

Poprawne wykonanie sygnatury demonstruje poniższy przykład:

```
openssl dgst -sha256 -sign prywatny.key -out sygnatura manifest
```

Gdzie:

- openssl dgst – polecenie wykonania sygnatury pakietu openssl,
- -sha256 – instrukcja użycia dla skrótu algorytmu SHA-256,
- -sign prywatny.key – instrukcja złożenia podpisu kluczem zawartym lub wskazanym w pliku prywatny.key,
- -out sygnatura – umieszczenie sygnatury we wskazanym pliku,
- manifest – nazwa pliku, dla którego wykonana jest sygnatura.

Centrala może zweryfikować poprawność tak wykonanej sygnatury poleceniem:

```
openssl dgst -verify publiczny.key -sha256 -signature sygnatura manifest
```

6 Wymagania na centralę

Centrala dostarcza następujących usług:

- Serwery (co najmniej dwa) dla tuneli VPN zapewniające adresację Urządzeń,
- Serwery (co najmniej dwa) DNS,
- Serwery (co najmniej dwa) NTP,
- Funkcjonalność CA generowania i certyfikowania kluczy na potrzeby tunelu VPN.
- Usługa przyjmowania alertów (serwer HTTP).

Centrala musi obsługiwać cały opisany tu protokół.

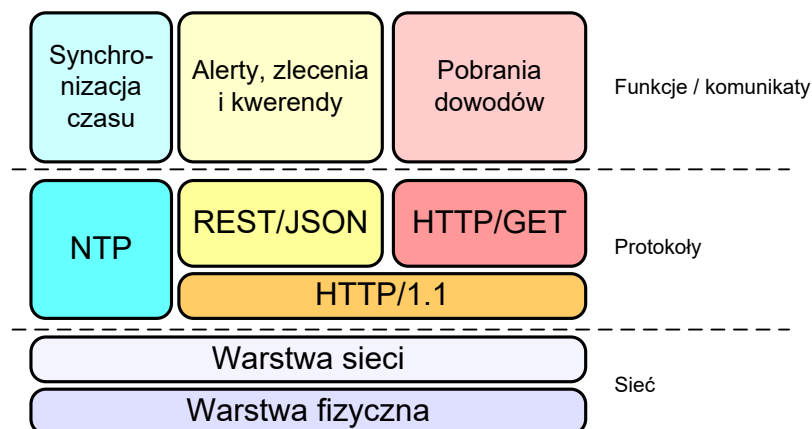
Centrala utrzymuje konfigurację każdej lokalizacji, w której umieszczono lub planuje się umieszczenie Urzędu rejestrującego.

Każde Urządzenie niezwłocznie po uruchomieniu informuje o tym centralę. Centrala powinna odpytać Urządzenie o jego konfigurację i zweryfikować czy jest poprawna. Jeśli nie, centrala ustawia parametry pracy Urzędu. Centrala weryfikuje również poprawność konfiguracji przekazanej wraz z dowodem.

7 Opis protokołu

Protokół komunikacyjny pomiędzy Urządzeniem rejestrującym a centralą został zdefiniowany z wykorzystaniem opisu warstw w podziale na trzy grupy: sieć, protokoły i funkcje/komunikaty.

Struktura protokołów została zobrazowana w poniższym diagramie:



Kolejne rozdziały specyfikują poszczególne warstwy.

7.1 Warstwa sieciowa

Urządzenie rejestrujące posiada połączenie z centralą zrealizowane w dowolnej technologii przy czym wymaga się, aby:

- Połączenie zapewniało dostępność protokołu IP i UDP.
- Umożliwiało zainicjowanie wymiany pakietów UDP z Urządzenia do centrali,
- Umożliwiało przesyłanie pakietów UDP z centrali do Urządzenia jeśli nie minął określony czas od inicjalnego transferu Urządzenie-centrala lub kolejnych transferów².

Centrala przetwarzania wystawia jeden lub kilka adresów IP z którymi łączą się Urządzenia.

W celu zabezpieczenia poufności i integralności transmisji wykorzystywane będzie szyfrowany tunel VPN. Poza zagadnieniami związanymi z bezpieczeństwem zastosowanie zapewni właściwą adresację Urządzeń i ich dostępność z centrali na poziomie sieci.

Realizacja tunelu VPN oparta jest o udostępniane w postaci źródłowej oprogramowanie OpenVPN. Za przyjęciem takiego rozwiązania stoi przede wszystkim jego niezależność od systemu operacyjnego i platformy sprzętowej.

Konfiguracja Urządzenia rejestrującego w zakresie tunelu VPN musi umożliwiać łatwe zmiany wykonywane przez administratora Urządzenia stąd treść plików konfiguracyjnych nie może podlegać homologacji czy zatwierdzeniu typu.

Minimalistyczny przykładowy plik konfiguracyjny tunelu OpenVPN wygląda następująco:

```
remote <adres IP punktu dostępowego centrali>
client
port 1194
cipher aes-128-cbc
dev tun0
```

```
ca certyfikat-ca.crt
cert certyfikat-Urządzenia.crt
key klucz-prywatny-Urządzenia.pem
```

Centrala dostarcza pliki certyfikatów i kluczy dla Urządzenia. Konfigurację wykonuje administrator. Wzmiankowany klucz służy do uwierzytelniania tunelu VPN i nie może być tym samym kluczem, który zostanie użyty do składania sygnatury pod danymi wchodzącymi w skład dowodu.

Pole CN certyfikatu zawiera sieciową nazwę Urządzenia. Central jest skonfigurowana w ten sposób, że serwery DNS zamieniają tę nazwę na adres IP Urządzenia w tunelu VPN.

Klucz prywatny może być przechowywany jako plik.

Administrator może sterować całością konfiguracji OpenVPN – może zmienić każdy jej aspekt. Dokumentacja Urządzenia specyfikuje wymagane elementy konfiguracji (np. skrypty uruchamiane po nawiązaniu połączenia tunelu).

Interfejs Urządzenia umożliwia wgranie (upload) plików certyfikatów i kluczy do Urządzenia oraz ustawienie konfiguracji.

Centrala nadaje adresy IP wszystkim Urządzeniom w ramach tunelu. Wszystkie usługi centrali i cała komunikacja z centralą odbywa się na bazie adresacji wewnątrz tunelu IP.

IP nadawane Urządzeniom w ramach adresacji tunelu VPN są stałe. Przykładowa minimalistyczna konfiguracja OpenVPN po stronie centrali może wyglądać następująco:

² Dopuszcza się zatem istnienie zapory ogniowej lub analogicznych mechanizmów bezpieczeństwa, które uniemożliwiają nawiązanie komunikacji do Urządzenia ale dopuszczają ruch w obie strony jeśli zostanie zainicjowany przez Urządzenie oraz transmisja ma miejsce odpowiedni często.

```
proto udp
dev tun0
link-mtu 1500
port 1194
```

```
ca certyfikat-ca.crt
cert certyfikat-centrali.crt
key klucz-centrali.pem
```

```
dh dh1024.pem
```

```
server 10.128.0.0 255.255.0.0 ; przykładowa adresacja VPN
topology subnet
```

```
cipher AES-128-CBC
opt-verify cipher
```

```
ifconfig-pool-persist ipp.txt
keepalive 120 300
```

Centrala dostarcza serwer DNS dzięki czemu korzystanie z adresów IP (poza konfiguracją OpenVPN) nie jest wymagane.

Urządzenie musi dostarczać mechanizmy umożliwiające konfigurację co najmniej takich elementów jak adresy serwerów DNS i synchronizacji czasu.

7.1.1 Urządzenie w trybie off-line

Od wersji 1.4 SWD nie przewiduje się wykorzystania urządzeń w trybie off-line.

7.2 Warstwa protokołu transportowego

Protokół wymiany zrealizowany jest w oparciu o koncepcję REST. Oznacza to, że komunikaty pomiędzy Urządzeniem a centralą są przesyłane w oparciu o protokół http/1.1, z zastosowaniem odpowiednich do zadania metod (GET, POST, DELETE).

Na potrzeby wymiany danych przyjmuje się następujące założenia:

- Połączenia może nawiązywać zarówno Urządzenie jak i centrala – obie strony wystawiają zatem usługi http na ustalonym porcie,
- Co do oprogramowania serwera i klienta http zakłada się minimalną implementację:
 - Stosuje się wyłącznie metody GET i POST,
 - Nie jest używana ani obsługiwana funkcja Expect: 100-continue (RFC 2616, rozdział 14.20),
 - Wszystkie połączenia są zamykane (brak „keep-alive” – nagłówki „Connection: close”),
 - Komunikaty JSON przesyłane są z „Content-type” równym „application/json”,
 - Dowody przesyłane są z „Content-type” równym „application/x-7z-compressed”,
 - Dla komunikatów JSON stosowana jest kompresja (Nagłówek Content-encoding: gzip),
- Serwer i klient (w celu oszczędzania transmisji) przesyłają tylko niezbędne nagłówki.
- Obsługiwane jest wznowianie transferu dla metody GET (RFC 2616, Rozdział: 14.3 Byte Ranges).

- Nagłówek „Host” zawiera nazwę sieciową Urządzenia (wartość pola CN certyfikatu Urządzenia wykorzystywanego w VPN).

7.3 Składnia zdalnych wywołań

Wywołania przyjmują obejmują dwie postaci:

- Alerty, zlecenie i kwerendy,
- Pobieranie dowodu.

Pierwszy typ jest wykorzystywany do zmiany parametrów Urządzenia, odpytywania Urządzenia lub zgłaszania przez Urządzenie awarii czy wygenerowania nowego dowodu.

Drugi typ jest metodą pobierania dowodu.

7.3.1 Alerty, zlecenia i kwerendy

Alerty to mechanizm powiadamiania centrali przez Urządzenie o zaistnieniu określonego faktu.

Zlecenia, to polecenia centrali przekazywane do Urządzenia w celu zmiany lub ustawienia typu pracy Urządzenia.

Kwerendy, to zapytania centrali kierowane do Urządzenia w celu pozyskania określonej informacji (np. zapytanie o aktualne ograniczenie prędkości ustawione na Urządzeniu).

Dwa pierwsze typy realizowane są metodą HTTP POST. Kwerendy realizowane są poprzez HTTP GET.

Wszystkie żądania posiadają następujące cechy:

- Treść żądań lub odpowiedzi przekazywana jest jako „application/json”.
- Treść jest kompresowana (Content-encoding oraz Accept-encoding: gzip),
- Połączenia są zamykane (Connection: close),
- Przesyłane są wyłącznie wymagane nagłówki.

Alerty realizowane są następująco:

- Urządzenie nawiązuje połączenie z centralą i wysyła następujące polecenie: **POST /Alert HTTP/1.1**
- Treścią alertu jest odpowiedni komunikat w formacie JSON.
- Serwer odpowiada statusem 200 (bez treści) jeśli przyjął alert. Centrala może również zwrócić inne statusy z grupy 4xx odpowiadające sytuacji (np. 400 jeśli komunikat jest niepoprawny). Możliwe jest również pojawienie się błędu z grupy 5xx jeśli w centrali ma miejsce jakiś rodzaj awarii.
- Urządzenie powinno ponawiać żądanie jeśli otrzymało błąd z grupy 5xx i nie ponawiać w aktualnej postaci jeśli otrzymało błąd z grupy 4xx.

Zlecenia realizowane są następująco:

- Centrala wysyła do Urządzenia polecenie: **POST /Zlecenie HTTP/1.1**
- W treści zlecenia jest odpowiedni komunikat w formacie JSON.
- Urządzenie odpowiada kodem 200 i odpowiednim komunikatem zwrotnym.
- Inne statusy oznaczają błąd przetwarzania. Centrala może automatycznie ponawiać żądanie jeśli status odpowiedzi Urządzenia należał do grupy 5xx.

Kwerendy realizowane są w następujący sposób:

- Centrala wysyła do Urzędu polecenie: **GET /Zapytanie/{id parametru} HTTP/1.1**
- Urządzenie zwraca status 200 i treść w postaci JSON, która zawiera odpowiednie wartości.
- Jeśli identyfikator parametru jest pusty (GET /Zapytanie lub GET /Zapytanie/), Urządzenie zwraca komunikat opisujący wszystkie dostępne parametry.

7.3.2 Pobieranie dowodu

Dowód jest zrealizowany jako archiwum 7-zip zawierające odpowiednie pliki. Centrala pobiera dowód wykonując na Urzędzie metodę GET a następnie oznacza go jako możliwy do usunięcia metodą DELETE.

Opis procedury pobrania dowodu:

- Centrala wykonuje na danym Urzędzie polecenie HTTP o następującej treści: **GET /Dowod/{x} HTTP/1.1**
- {x} jest w rzeczywistości identyfikatorem dowodu (czyli np. polecenie ma postać GET/Dowod/12345 HTTP/1.1).
- Polecenie zawiera następujące nagłówki HTTP:
 - Host: <nazwa Urzędu>,
 - Connection: close,
 - Accept : application/x-7z-compressed.
- Opcjonalnie polecenie może zawierać również nagłówek “Range” podając informację o bajtach do pobrania,
- Urządzenie odpowiada statusem 200 jeśli dowód o podanym id istnieje w buforze, pozostałe nagłówki, to:
 - Connection: close,
 - Content-type: application/x-7z-compressed,
 - Content-length: <rozmiar danych>
- Jeśli dowodu o podanym id nie ma w buforze Urzędu, zwraca ono status 404 – nie znaleziono. Odpowiedź nie musi zawierać jakiegokolwiek treści. Jeśli zawiera, centrala ją zignoruje.
- Strony zamykają połączenie.
- Po pobraniu kompletnego dowodu (z ewentualnymi wznowieniami transmisji), centrala informuje Urządzenie o tym, że dowód może być już usunięty przesyłając do Urzędu polecenie **DELETE /Dowod/{x} HTTP/1.1** gdzie {x} jest tym samym identyfikatorem, który był wykorzystany do pobrania dowodu. Urządzenie może usunąć z lokalnego bufora dane dowodu.

Szczegóły dotyczące całego procesu opisują kolejne rozdziały.

8 Definicje komunikatów

Komunikaty wymieniane pomiędzy centralą a Urzędem bazują na strukturach zgodnych ze standardem JSON (RFC 4627). Dodatkowo wprowadza się następujące zasady:

- Pierwszym elementem każdego obiektu jest pole „typ” opisuje typ i wersję komunikatu w postaci „typ.rozdzielony.kropkami:wersja”, np. „komunikat.błąd:1.0”,

- Czas jest zawsze czasem UTC i jest przedstawiany w następującej postaci: „RRRR-MM-DD gg:mm:ss.xxx”, gdzie:
 - RRRR – rok (np. 2011),
 - MM – miesiąc (01-styczeń, 12-grudzień),
 - DD – dzień (od 01 do 31),
 - gg – godzina (od 00 do 23),
 - mm – minuta (od 00 do 59),
 - ss – sekunda (od 00 do 59),
 - xxx – milisekundy (od 000 do 999) – może być zawsze 000 jeśli Urządzenie nie wspiera takiej dokładności ale musi zawsze wystąpić.
- W kilku miejscach występują pojęcia „godz-od” „godz-do” o formacie „gg:mm”. Jest to godzina i minuta wyrażona w aktualnej strefie czasowej. Oznacza to na przykład, że w ciągu doby może wystąpić dwukrotnie 02:15 – jeśli jest to akurat doba, w której ma miejsce zmiana czasu.
- Komunikaty kodowane są jako UTF-8.
- Kolejność pól w komunikatach jest nieokreślona. Istotne są nazwy i struktura.

8.1 Format dowodu

Dowód naruszenia ma szczególną postać, ponieważ oprócz informacji strukturalnej (struktury JSON) zawiera dodatkowe dane: zdjęcia oraz sygnaturę.

Dowód ma następujące cechy:

- Dowód jest zrealizowany jako archiwum 7-zip przechowujące wszystkie pliki wchodzące w skład dowodu.
- Głównym plikiem jest „manifest”. Zawiera on (w formacie JSON) informację o szczegółach dowodu. Każdy plik dowodu ma odpowiednią pozycję w manifestcie obejmującą jego nazwę i skrót SHA-256,
- Drugim istotnym plikiem jest plik „sygnatura” przechowujący podpis manifestu wykonany zgodnie z opisem w rozdziale 5.1.
- Każdy plik, który nie jest plikiem manifestu lub sygnatury oraz nie jest wzmiankowany w manifestcie powinien zostać odrzucony.
- Zdjęcia przechowywane są w formacie JPEG (ISO/IEC IS 10918-1 | ITU-T Recommendation T.81) lub PNG (RFC 2083).
- W skład dowodu może wchodzić plik natywny (typu „natywny”) z urządzenia rejestrującego na podstawie którego zostało utworzone zdjęcie lub zdjęcia (typu „zdjęcie”). Plik natywny jest elementem opcjonalnym.
- W skład dowodu mogą wchodzić pliki innych obrazów (typu „inny-obraz”) pochodzące z urządzenia typu „czerwone-światło” (lub innego, które uzupełnia materiał dowodowy dodatkowymi ujęciami), przedstawiające np. ujęcie pogładowe na całe skrzyżowanie. Dopuszczalne formaty plików obrazów typu „inny-obraz” są takie same jak dla plików typu „zdjęcie”.
- W skład dowodu mogą wchodzić pliki filmów (typu „film”) pochodzące z urządzenia typu „czerwone-światło” (lub innego, które uzupełnia materiał dowodowy sekwencją filmową) przedstawiające przejazd pojazdu dokonującego naruszenia. Nie specyfikuje się formatu

plików filmów, wymagane jest natomiast umieszczenie w polu „specyfikacja-filmu” informacji o kontenerze, kodeku wideo i kodeku audio (jeżeli występuje) np.: „Ogg/Theora/Vorbis” lub „Ogg/Theora” (w przypadku braku strumienia dźwięku).

- Niepomijalnym i najistotniejszym elementem Dowodu jest zdjęcie (typu „zdjęcie”), na którym uwidoczniiony jest numer rejestracyjny pojazdu, którym dokonywane jest naruszenie. Dowód bez tego zdjęcia nie będzie przetwarzany w systemie centralnym. Tym samym każdy poprawny Dowód zawierać musi co najmniej jeden plik typu „zdjęcie”.
- Zdjęcia tworzące sekwencje plików odpowiadających za różne zdarzenia dokumentujące jedno naruszenie muszą zawierać w sekcji „plik” pola „numer-sekwencji” i „numer-w-sekwencji” pozwalające na ich precyzyjną i powtarzalną identyfikację.

Dowód jest pobierany przez centralę z adresu <http://<Urządzenie>/Dowod/{id dowodu}>.

8.1.1 Struktura dowodu

Dowód jest archiwum 7-zip z następującą strukturą plików:

- Plik „manifest”,
- Plik „sygnatura”,
- Pozostałe pliki (tj. zdjęcia, filmy oraz pliki natywne z urządzenia rejestrującego).

8.1.2 Format manifestu

Manifest ma następującą postać:

```
{
  „typ”: „Dowód.Manifest:1.0”,
  „opis”: {
    „id”: <numer sekwencyjny dowodu>,
    „rodzaj”: („pomiar-punktowy” | „pomiar-odcinkowy” | „czerwone-światło”),
    „producent”: „<producent Urzędnika>”,
    „model”: „<model Urzędnika>”,
    „numer-seryjny”: „<numer seryjny Urzędnika>”,
    „lokalizacja”: „<identyfikator lokalizacji>”,
    „opis-lokalizacji”: „<opis miejsca wykrycia naruszenia>”,
    „gps”: „<lokalizacja z GPS w formacie NMEA>”,
    „czas-wjazdu”: „RRRR-MM-DD gg:mm:ss.xxx”,
    „czas”: „RRRR-MM-DD gg:mm:ss.xxx”,
    „czas-trwania-fazy”: „<wartość w milisekundach>”,
    „limit”: <wartość ograniczenia w km/h>,
    „próg”: <wartość progu w km/h>,
    „prędkość”: <zmierzona prędkość w km/h>,
    „kierunek”: („P” | „T”),
    „opis-kierunku”: „<opis kierunku wykrycia naruszenia>”,
    „opóźnienie”: <wartość czasu opóźnienia w milisekundach>,
    „pojazd”: {
      „marka”: „<rozpoznana marka pojazdu>”,
      „anpr”: „<rozpoznany numer rejestracyjny>”,
      „kategoria”: („ciężarowy” | „osobowy”)
    }
  },
  „informacja-o-limitach”: {
    „kategoria-ciężarowy-najazd”: <limit dla poj. ciężarowych na najazd>,
    „kategoria-ciężarowy-odjazd”: <limit dla poj. ciężarowych na odjazd>,
    „kategoria-osobowy-najazd”: <limit dla poj. Osobowych na najazd>,
    „kategoria-osobowy-odjazd”: <limit dla poj. Osobowych na odjazd>
  },
  „rozszerzenia”: [
    ...
  ]
}
```

```

    ]
  },
  „pliki”: [
    {
      „nazwa”: „<zdzecie.jpeg>”,
      „numer-sekwencji”: <numer sekwencji>,
      „numer-w-sekwencji”: <numer pliku w sekwencji>,
      „typ-pliku”: („natywny” | „zdjęcie” | „film” | „inny-obraz”),
      „specyfikacja-filmu”: „<kontener/kodek wideo/kodek audio>”,
      „czas”: „<RRRR-MM-DD gg:mm:ss.xxx>”,
      „gps”: „<lokalizacja z GPS w formacie NMEA>”,
      „obrys”: {
        „x1”: <lewy bok>,
        „y1”: <dolny bok>,
        „x2”: <prawy bok>,
        „y2”: <górny bok>
      }
      „skrót”: {
        „alg”: „SHA-256”,
        „wartość”: „d8d934a2fe58cd41496fb61648143...”}
    },
    {
      ... // inne pliki
    }
  ]
  „sygnatura”: „SHA256withRSA”
}

```

Informacje do struktury:

- Pola „typ”, „sygnatura” oraz „alg” są niezmiennie w tej wersji protokołu,
 - typ specyfikuje format i wersję manifestu,
 - alg specyfikuje algorytm funkcji skrótu i jest niezmienny dla danej wartości typ,
 - sygnatura specyfikuje algorytm podpisu – dla danej wartości „typ” „alg” jest zawsze jednakowy,
- Pole „id” zawiera numer sekwencyjny dowodu. Jest to liczba naturalna bez limitu na maksymalną wartość. Wymaga się, aby dla każdego Urzędnika generacja identyfikatorów rozpoczynała się od „1” i stanowiła ciągłą sekwencję bez luk. Id jest wartością numeryczną.
- Pole „rodzaj” mówi, czy dowód dotyczy pomiaru punktowego, odcinkowego czy też przejazdu na czerwonym świetle,
- Pole „producent” zawiera nazwę producenta Urzędnika,
- Pole „model” zawiera nazwę modelu Urzędnika,
- Pole „numer-seryjny” zawiera numer seryjny Urzędnika. Centrala utrzymuje szereg informacji powiązanych z numerem seryjnym Urzędnika, w tym informacje o legalizacji Urzędnika.
- Pole „lokalizacja” zawiera skonfigurowany przez administratora identyfikator lokalizacji. Centrala utrzymuje informacje dotyczące lokalizacji np. informacje o obowiązujących limitach prędkości i decyzje o ustawionym progu,
- Pole „opis-lokalizacji” zawiera dodatkowe informacje umożliwiające identyfikację kierunku w jakim zostało wykryte naruszenia np.: informacje o lokalizacji, kierunku, pasie jezdni. Pole jest

w szczególności istotne dla pomiaru punktowego i przejazdu na czerwonym świetle. Pole jest opcjonalne.

- Pole „gps” zawiera sentencję GPGLA w formacie NMEA-183 opisującą odczytaną z Urządzenia GPS aktualną w momencie tworzenia dowodu lokalizację Urządzenia wraz z pozostałymi informacjami wynikającymi z formatu sentencji (np. liczba satelitów); Pole jest opcjonalne gdy dowód dotyczy przejazdu na czerwonym świetle. Przykład: „\$GPGLA,123519,4807.038,N,01131.000,E,1,08,0.9,545.4,M,46.9,M,,*47”. Pole w sekcji „opis” oznacza lokalizację urządzenia, na którym nastąpiło wykrycie naruszenia przepisów ruchu drogowego. W przypadku pomiaru punktowego lub czerwonego światła jest to ta sama wartość, która pojawia się potem w sekcji „plik”. W przypadku pomiaru odcinkowego jest to lokalizacja urządzenia ustawionego na wyjeździe z odcinka.
- Pole „czas” w sekcji „opis” wskazuje moment zarejestrowania faktu dokumentującego wykrycie naruszenia. W przypadku pomiaru punktowego lub czerwonego światła jest to moment w czasie, gdy wykonano zdjęcie. W przypadku pomiaru odcinkowego jest to moment w czasie, gdy zarejestrowano pojazd opuszczający mierzony odcinek.
- Pole „czas-wjazdu” w sekcji „opis” wskazuje moment wjazdu na odcinek w przypadku pomiaru odcinkowego. Pole nie występuje dla pomiaru punktowego i dla przejazdu na czerwonym świetle.
- Pole „czas-trwania-fazy” występuje tylko dla urządzenia dla którego pole „rodzaj” jest równe „czerwone-światło”.
- Pola „limit” i „próg” nie występują jeśli „rodzaj” równe jest „czerwone-światło”; pole „prędkość” jest wtedy opcjonalne,
- Pola „limit”, „próg” i „prędkość” są polami numerycznymi,
- Pole „limit” oznacza ograniczenie prędkości na danym odcinku,
- Pole „próg” oznacza wartość powyżej której zmierzona prędkość zainicjować tworzenie dowodu (np. ograniczenie jest do 50km/h a limit 60km/h).
- Ustawienie wysokiej wartości dla pól „limit” i „próg” (np. 250km/h) należy interpretować jako rezygnację z chęci pomiaru prędkości w określonym kierunku. Konkretną wartość, dla której urządzenie przestaje rejestrować prędkość określa producent urządzenia a w systemie centralnym wykorzystuje Operator modułu Zarządzania Infrastrukturą.
- Pole „prędkość” jest zmierzoną (w przypadku pomiaru punktowego) lub wyliczoną (w przypadku pomiaru odcinkowego) w km/h prędkością pojazdu.
- Pole „kierunek” mówi o tym, czy zdjęcie zostało zrobione pojazdowi zbliżającemu się („P” – przód) czy oddalającemu („T” – tył). Pole jest opcjonalne gdy dowód dotyczy przejazdu na czerwonym świetle.
- Pole „opis-kierunku” występuje dla pomiaru odcinkowego i zawiera wartość przepisana z parametru Urządzenia: „opis-kierunku-p-t” lub „opis-kierunku-t-p” w zależności od obowiązującej w czasie wykrycia naruszenia wartości atrybutu „kierunek” parametru Urządzenia „limit” i „próg”.
Przykład: parametry „limit” i „próg” mają ustawiony atrybut „kierunek” = „P”; w przypadku wykrycia naruszenia pole „opis-kierunku” powinno zawierać wartość parametru „opis-kierunku-p-t”. Analogicznie dla pola „kierunek” = „T” pole „opis-kierunku” powinno zawierać wartość parametru „opis-kierunku-t-p”.
- Sekcja „informacja-o-limitach” zawiera cztery atrybuty:

- kategoria-ciężarowy-odjazd – z informacją o limicie prędkości dla pojazdów ciężarowych na odjazd,
- kategoria-ciężarowy-najazd – z informacją o limicie prędkości dla pojazdów ciężarowych na najazd,
- kategoria-osobowy-odjazd – z informacją o limicie prędkości dla pojazdów osobowych na odjazd,
- kategoria-osobowy-najazd – z informacją o limicie prędkości dla pojazdów osobowych na najazd.

Wartości wszystkich parametrów mają ten sam typ i znaczenie, co pole „limit” w sekcji „opis”.

Informacja jest wykorzystywana w centrali w przypadkach, gdy wykryta przez urządzenie kategoria pojazdu nie jest zgodna z informacją pochodzącą z CEPiK. Zarówno sekcja jak i atrybuty w niej są obowiązkowe dla urządzeń rejestrujących przekroczenie prędkości.

- Pole „opóźnienie” informuje o skonfigurowanym na urządzeniu rejestrującym czasie opóźnienia w rejestracji obecności pojazdu od momentu włączenia się czerwonego światła na sygnalizatorze. Czas prezentowany jest w milisekundach. Pole wymagane dla dowodów, jeśli „rodzaj” równy jest „czerwone-swiatło”.
- Pole „rozszerzenia” jest miejscem dla rozszerzeń producenta. Pole jest opcjonalne. Jeśli występuje rozszerzenia są interpretowane w kontekście wartości pól „producent” i „model”.
- Sekcja „pojazd” dotyczy zdolności rozpoznawania przez Urządzenie marki i typu oraz numeru rejestracyjnego (anpr) pojazdu. Sekcja „pojazd” jest wymagana dla każdego rodzaju Urządzenia. Pole „anpr” zawierające rozpoznany numer rejestracyjny jest wymagane. Pozostałe pola sekcji „pojazd” są opcjonalne.
- Dla każdego pliku liczona jest wartość skrótu SHA-256.
- Dla każdego pliku niezależnie dołączana jest informacja o czasie wykonania zdjęcia i lokalizacji geograficznej (gps) miejsca, w którym wykonano zdjęcie. Ma to przede wszystkim zastosowanie dla pomiaru odcinkowego lub gdy w ramach dowodu dostarczane jest kilka zdjęć. W przypadku pomiaru odcinkowego czasu i lokalizacje wykonania poszczególnych zdjęć są przebiegami odcinka drogi z nadmierną prędkością.
- Pole „typ-pliku” w sekcji „plik” jest opcjonalne. W przypadku braku pola przyjmowana jest wartość domyślna „zdjęcie”.
- Pole „specyfikacja-filmu” jest wymagane jeżeli pole „typ-pliku” równe jest „film”.
- Pola „gps”, „czas” i „obrys” w sekcji „plik” są wymagane dla każdego typu urządzenia rejestrującego wykroczenia.
- Pole „obrys” w sekcji „plik” definiuje prostokąt jednoznacznie wskazujący pojazd z jego numerem rejestracyjnym, dla którego wykryto naruszenie. Wartości osi X rosną z lewej do prawej, wartości osi Y z dołu do góry. Jednostką są piksele obrazu. „x2” musi być większe od „x1”. Analogicznie „y2” musi być większe od „y1”. Pole jest wymagane.
- Pola „numer-sekwencji” i „numer-w-sekwencji” w sekcji „plik” są wymagane jeżeli pliki dowodu naruszenia tworzą sekwencję różnych zdarzeń dokumentujących jedno naruszenie. Pole „numer-sekwencji” powinno zawierać numer kolejnej sekwencji plików a pole „numer-w-sekwencji” kolejny numer pliku w danej sekwencji. Wartości tych pól muszą być nieprzerwanym ciągiem kolejnych liczb począwszy od 1.

Centrala weryfikuje w dowodzie zgodność wszystkich pól z utrzymywaną konfiguracją oraz weryfikuje, czy pola posiadają prawdopodobne wartości (np. czy zmierzona prędkość jest w ogóle osiągalna dla pojazdów).

8.1.3 Wytworzenie dowodu

Dowód tworzony jest zgodnie z następującym algorytmem:

- Tworzony jest pusty folder do którego kopiuje się wszystkie pliki,
- Tworzony jest plik manifestu opisujący zdarzenie.
- Dla każdego zdjęcia, filmu lub pliku natywnego obliczany jest skrót SHA-256; nazwa pliku ze zdjęciem/filmem oraz odpowiedni skrót umieszczany jest w strukturze manifestu.
- Generowana jest sygnatura pliku manifest zgodnie z opisem w rozdziale 5.1.
- Wszystkie pliki w katalogu dodawane są do archiwum o nazwie równej identyfikatorowi zdarzenia.

Tak przygotowany dowód jest dostępny na Urzędzeniu pod adresem http://<Urządzenie>/Dowod/<numer_id>

8.1.4 Weryfikacja sygnatury dowodu

Weryfikacja jest procesem odwrotnym do wytworzenia.

Po rozpakowaniu archiwum następuje weryfikacja sygnatury pliku manifest zgodnie z opisem w 5.1 (Mechanizm sygnatury opisany jest w samym manifestie w polu „sygnatura”).

Po pozytywnej weryfikacji plik manifestu jest przetwarzany. Dla każdej pozycji plikowej liczy się skrót i porównuje z zapisanym w manifestie.

Pliki, których skróty są niezgodne z manifestem są odrzucane. Pliki w archiwum, których nie było w manifestie są odrzucane.

Odrzucenie co najmniej jednego pliku może stanowić powód do odrzucenia dowodu jako całości.

8.1.5 Pliki natywne dowodu, inne obrazy i filmy

W przypadku wystąpienia w dowodzie naruszenia plików natywnych, filmów lub innych obrazów (typ „natywny”, „film”, „inny-obraz), powstałych na urządzeniach rejestrujących, rola centrali sprowadza się do:

- weryfikacji skrótów (zgodnie z punktem 8.1.4)
- składowania tych plików w repozytorium plików dowodów naruszeń

Pliki typu „zdjęcie” analizowane są zgodnie z przyjętymi wymaganiami.

8.2 Alerty

Alerty wysyłane są przez Urządzenia do centrali metodą POST na adres <http://<centrala>/Alert>.

Wymagalność obsługi alertów w podziale na rodzaj urządzenia (W – wymagane, X – nie występuje):

Typ alertu	pomiar-punktowy	pomiar-odcinkowy	czerwone-swiatło
Zgłoszenie obecności dowodu	W	W	W
Zgłoszenie przekroczenia wartości parametru	W	W	X
Zgłoszenie naruszenia integralności Urządzenia	W	X	X
Zgłoszenie przepełnienia bufora	W	W	W
Zgłoszenie restartu urządzenia	W	W	W

Dostarczanie informacji statystycznej	W	W	X
Inne zgłoszenia	W	W	W

8.2.1 Zgłoszenie obecności dowodu

Gdy Urządzenie wygeneruje dowód informacja o jego istnieniu jest zgłaszana do centrali. Realizowane jest to następującym komunikatem:

```
{
  „typ”: „Nowy.Dowód:1.0”,
  „producent”: „<nazwa producenta Urządzenia>”,
  „model”: „<nazwa modelu Urządzenia>”,
  „numer-seryjny”: „<numer seryjny Urządzenia>”,
  „id”: <identyfikator dowodu>,
  „czas”: „RRRR-MM-DD gg:mm:ss.xxx”
}
```

Centrala odpowie na ten alert pobraniem dowodu a następnie zleceniem usunięcia dowodu.

Przykład:

```
{„typ”: „Nowy.Dowód:1.0”, „producent”: „ABC”,
„model”: „ABC-124”, „numer-seryjny”: „1234-234-12”, „id”: „1045”,
„czas”: „2015:04:12 23:59.000”}
```

8.2.2 Zgłoszenie przekroczenia wartości parametru

Alert jest generowany, gdy Urządzenie wykryje przekroczenie wartości parametru pracy (np. temperatura nie mieści się w akceptowanym zakresie):

```
{
  „typ”: „Przekroczenie.parametru:1.0”,
  „producent”: „<nazwa producenta Urządzenia>”,
  „model”: „<nazwa modelu Urządzenia>”,
  „numer-seryjny”: „<numer seryjny Urządzenia>”,
  „czas”: „RRRR-MM-DD gg:mm:ss.xxx”,
  „parametr”: „<nazwa parametru>”,
  „wartość”: „<wartość parametru>”
}
```

Przykład:

```
{“typ”: „Przekroczenie.parametru:1.0”, „producent”: „ABC”,
„model”: „ABC-124”, „numer-seryjny”: „1234-234-12”,
„czas”: „2001:12:24 22:45:23.123”, „parametr”: „temp”, „wartość”: „85”}
```

Parametry opisano w rozdziale 4.3.

8.2.3 Zgłoszenie naruszenia integralności Urządzenia

Alert jest generowany, gdy nastąpi jakiegokolwiek zdarzenie stwarzające podejrzenie, że naruszono integralność Urządzenia:

```
{
  „typ”: „Naruszenie.Integralności:1.0”,
  „producent”: „<nazwa producenta Urządzenia>”,
  „model”: „<nazwa modelu Urządzenia>”,
  „numer-seryjny”: „<numer seryjny Urządzenia>”,
  „czas”: „RRRR-MM-DD gg:mm:ss.xxx”,
}
```

```

    „info”: “<opcjonalnie dodatkowa informacja>”
  }
  Przykład
  {“typ”: “Naruszenie.Integralności:1.0”, „producent”: „ABC”,
    „model”: „ABC-124”, „numer-seryjny”: „1234-234-12”,
    „czas”: “2012-01-13 19:35:17.000”, „info”: “Otwarcie obudowy”}

```

Pole „info” jest opcjonalne a jego wartość czysto informacyjna – centrala nie powinna próbować go przetwarzać automatycznie.

8.2.4 Zgłoszenie przepełnienia bufora

Jeśli centrala nie pobiera zbyt długo dowodów z Urządzenia lub nie zleca ich usuwania, może dojść do zapelnienia bufora. Jeśli w takim momencie wygenerowany zostanie nowy dowód, to nie da się go umieścić w buforze. W tej sytuacji dowód jest usuwany a do centrali przesyłany alert o przepełnieniu.

Komunikat ma następującą postać:

```

{
  „typ”: “Przepełnienie.Bufora:1.0”,
  „producent”: „<nazwa producenta Urządzenia>”,
  „model”: „<nazwa modelu Urządzenia>”,
  „numer-seryjny”: „<numer seryjny Urządzenia>”,
  „czas”: “RRRR-MM-DD gg:mm:ss.xxx”,
  „utracono”: <id>
}

```

Pole „utracono” jest opcjonalne i może zawierać najwyższy z identyfikatorów utraconych dowodów.

Przykład:

```

{“typ”: “Przepełnienie.Bufora:1.0”, „producent”: „ABC”,
  „model”: „ABC-124”, „numer-seryjny”: „1234-234-12”,
  „czas”: “2012-05-13 14:12:14.000”, „utracono”: 10234}

```

8.2.5 Zgłoszenie restartu Urządzenia

Urządzenie rejestrujące niezwłocznie po uruchomieniu wysyła do centrali alert informujący o tym fakcie.

Komunikat ma następującą postać:

```

{
  „typ”: “Uruchomienie:1.0”,
  „producent”: „<nazwa producenta Urządzenia>”,
  „model”: „<nazwa modelu Urządzenia>”,
  „numer-seryjny”: „<numer seryjny Urządzenia>”,
  „czas”: “RRRR-MM-DD gg:mm:ss.xxx”,
  „przyczyna”: („planowane włączenie” | „automatyczny restart” | „restart po awarii”)
}

```

Pole „przyczyna” może nie wystąpić jeśli przyczyna jest nieznana.

8.2.6 Dostarczanie informacji statystycznej

Jeśli w Urządzeniu ustawiono parametr „statystyki” na wartość „tak”, Urządzenie rejestruje czas i prędkość każdego przejeżdżającego pojazdu (o ile urządzenie gromadzi informacje o prędkościach pojazdów).

Urządzenie generuje komunikat z listą zarejestrowanych przejazdów w następującym formacie:

```
{
  "typ": "Informacja.Statystyczna:1.0",
  "producent": "<nazwa producenta Urządzenia>",
  "model": "<nazwa modelu Urządzenia>",
  "numer-seryjny": "<numer seryjny Urządzenia>",
  "czas": "RRRR-MM-DD gg:mm:ss.xxx",
  "statystyki": [
    {
      "czas": "RRRR-MM-DD gg:mm:ss.xxx",
      "prędkość": "<prędkość>",
      "kierunek": ("P" | "T"),
      "kategoria": ("ciężarowy" | "osobowy")
    },
    ...
  ]
}
```

Tablica „statystyki” zawiera informację o czasie i zmierzonej lub oszacowanej prędkości pojazdu. Pole prędkość, kierunek i kategoria muszą wystąpić jeśli Urządzenie posiada techniczną możliwość do ich określenia.

Urządzenie przesyła do centrali na tyle często, żeby rozmiar tablicy „statystyki” nie przekroczył 1000 pozycji i nie rzadziej niż raz na godzinę.

Przykład:

```
{
  "typ": "Informacja.Statystyczna:1.0",
  "producent": "ABC",
  "model": "RDR/1.0",
  "numer-seryjny": "1234-1234",
  "czas": "2001-01-02 12:14:24.123",
  "statystyki": [
    {
      "czas": "2001-01-02 10:15:17.120",
      "prędkość": "62",
      "kierunek": "P",
      "kategoria": "osobowy"
    },
    {
      "czas": "2001-01-02 10:16:35.743",
      "prędkość": "84",
      "kierunek": "T",
      "kategoria": "ciężarowy"
    }
  ],
}
```

8.2.7 Inne zgłoszenia.

Urządzenie może zgłaszać również inne zdarzenia. Ich semantyka nie jest jednak ustalona standardem. Format takiego zgłoszenia jest następujący:

```
{
  "typ": "Ogólne.Zgłoszenie:1.0",
  "producent": "<nazwa producenta Urządzenia>",
  "model": "<nazwa modelu Urządzenia>",
  "numer-seryjny": "<numer seryjny Urządzenia>",
  "czas": "RRRR-MM-DD gg:mm:ss.xxx",
  "klasa": ("info" | "uwaga" | "awaria")
}
```

```

    „info”: “<opcjonalnie dodatkowa informacja>”
    „parametry”: [
        {
            „nazwa”: „<”,
            „wartość”: „<”
        },
        ...
    ]
}

```

Przykład (Urządzenie z akcelerometrem wykrywając uderzenie):

```

{
    „typ”: „Ogólne.Zgłoszenie:1.0”, „producent”: „ABC”,
    „model”: „ABC-124”, „numer-seryjny”: „1234-234-12”,
    „czas”: „2012-05-13 14:12:14.000”, „klasa”: „uwaga”, „info”: „Uderzenie”,
    „parametry”: [{ „nazwa”: „przeciążenie”, „wartość”: „95G”}]
}

```

8.3 Odpowiedzi do kwerend

Wymagalność obsługi kwerend w podziale na rodzaj urządzenia (W – wymagane, X – nie występuje):

Typ kwerendy	pomiar-punktowy	pomiar-odcinkowy	czerwone-światło
Wykrywanie funkcjonalności Urządzenia	W	W	W
Zapytanie o parametr	W	W	W

8.3.1 Wykrywanie funkcjonalności Urządzenia

Wykrywanie funkcjonalności jest realizowane poprzez przesłanie polecenie GET na adres <http://<Urządzenie>/Zapytanie>.

Urządzenie zwraca wówczas komunikat następującej postaci:

```

{
    „typ”: „Odp.Rozpoznanie:1.0”,
    „producent”: „<producent Urządzenia>”,
    „model”: „<model Urządzenia>”,
    „czas”: „<bieżący czas na Urządzeniu>”,
    „rodzaj”: („pomiar-punktowy” | „pomiar-odcinkowy” | „czerwone-światło”),
    „klucz”: [
        „-----BEGIN PUBLIC KEY-----”,
        „MIIBIjANBgkqhkiG9w0BAQEFAAOCA...”,
        „K4TfIGcXvQ0L7Q6Vb7FpEH4GiQrb...”,
        ...
        „8wIDAQAB=”,
        „-----END PUBLIC KEY-----”
    ],
    „parametry”: [
        {
            „nazwa”: „<”,
            „format”: („num” | „str” | „bool”),
            „jednostka”: „<jednostka>”,
            „wartość”: <”,
            „ro”: (true | false),
            „opis”: „<Wyjaśnienie znaczenia parametru>”,
            „zmiany-wartości”: {

```

```

    „dozwolone”: (true | false),
    „lista”: [
    {
        „kategoria”: („ciężarowy” | „osobowy”)
        „kierunek”: („P” | „T”)
        „godz-od”: „gg:mm”,
        „godz-do”: „gg:mm”,
        „wartość”: <wartość>
    },
    ...
    ]
    }
    }
    „roszerzenia”: [
    ]
}

```

Uwagi:

- Pole „klucz” zawiera kolejne linijki klucza publicznego RSA w formacie PEM.
- Pole „rozszerzenia” jest opcjonalne a jego zawartość zależy od producenta.
- Wartość pola „rodzaj” zależy od typu Urządzenia.
- Parametr może być typu numerycznego (num), znakowego (str) lub prawda/fałsz (boolean, w JSON wyrażane jako true/false). Mówi o tym pole „format”.
- Jednostka ma wyłącznie charakter opisowy i jest opcjonalna.
- Pole „ro” (Read Only) oznacza, że wartość jest tylko do odczytu (true) lub, że centrala może je również modyfikować (false).
- Pole „opis” jest opcjonalne ale zalecane.
- Struktura „zmiany-wartości” ma szczególne znaczenie. Występuje i ma pole „dozwolone” równe true jeśli wartość parametru może być ustawiana ze zmianami w czasie, kierunku kategorii pojazdu. Takie ustawienie oznacza, że poza podstawową wartością w zadanych przedziałach czasu obowiązuje dodatkowa wartość. Przedziały czasowe dla tego samego typu pojazdu nie mogą zachodzić na siebie. Jeśli „godz-od” jest późniejsze niż „godz-do”, to traktowane jest to jako przejście przez północ (przypadek typu 23:00 do 01:00). Pole „kierunek” jest opcjonalne gdy rodzaj urządzenia zwracającego komunikat to „czerwone-światło”. Jeżeli zmiany wartości parametru nie obejmują pełnej doby, w brakujących przedziałach czasu obowiązuje podstawowa wartość określona za pomocą pola „wartość” w definicji parametru. W przypadku pomiaru odcinkowego, pole „kierunek”, występujące w ramach zmiany wartości dla parametrów „limit” i „próg”, powinno być interpretowane następująco: „P” – przód – tył; „T” – tył – przód.

Interpretacja przedziałów czasowych dla struktury „zmiany-wartości”

Przedział czasowy dla struktury „zmiany-wartości” określony za pomocą pól „godz-od”, „godz-do” powinien być interpretowany przez urządzenie jako przedział lewostronnie domknięty:

[godz-od, godz-do + 1 minuta)

Przykłady.:

dla „godz-od” = 12:00, „godz-do” = 23:59 przedział czasowy w którym obowiązuje wartość to [12:00, 00:00)

dla następujących po sobie strukturach zmiany wartości: „godz-od” = 12:05, „godz-do” = 12:12, „wartość” = 50 i „godz-od” = 12:13, „godz-do” = 12:15, „wartość” = 50 przedział czasowy w którym obowiązuje wartość to [12:05, 12:16)

Godzina wyrażona w formacie „godz-od” lub „godz-do” powinna być interpretowana przez urządzenie jako wartość „gg:mm:ss.xxx” gdzie liczba sekund „ss” równa się „00” i liczba milisekund „xxx” równa się „000” np.: dla godziny „12:00” rzeczywista wartość jest równa „12:00:00.000”.

Przykład:

```
{
  "typ": "Odp.Rozpoznanie:1.0",
  "czas": "1970-02-12 01:13:14.124",
  "rodzja": "pomiar-punktowy",
  "klucz": [
    "-----BEGIN PUBLIC KEY-----",
    "MIIBIjANBgkqhkiG9w0BAQEFAAOCA...",
    "K4TflGcXvQ0L7Q6Vb7FpEH4GiQrb...",
    "...",
    "8wIDAQAB=",
    "-----END PUBLIC KEY-----"
  ],
  "parametry": [
    {
      "nazwa": "numer-Urządzenia",
      "format": "string",
      "wartość": "<numer seryjny Urządzenia>",
      "ro": true,
      "opis": "Numer seryjny Urządzenia"
    },
    {
      "nazwa": "temp",
      "format": "num",
      "wartość": 25,
      "jednostka": "C",
      "ro": true,
      "opis": "Bieżąca temperatura pracy Urządzenia"
    },
    {
      "nazwa": "temp-min",
      "format": "num",
      "wartość": -5,
      "jednostka": "C",
      "ro": false,
      "opis": "Minimalna akceptowalna temperatura pracy"
    },
    {
      "nazwa": "temp-max",
      "format": "num",
      "wartość": 80,
      "jednostka": "C",
      "ro": false,
      "opis": "Maksymalna akceptowalna temperatura pracy"
    }
  ]
}
```



```

    },
    {
        „nazwa”: „limit”,
        „format”: „num”,
        „wartość”: 50,
        „jednostka”: „km/h”,
        „ro”: false,
        „opis”: „Dopuszczalna prędkość”,
        „zmiany-wartości”: {
            „dozwolone”: true,
            „lista”: [
                {
                    „godz-od”: „23:00”,
                    „godz-do”: „04:00”,
                    „wartość”: 60
                }
            ]
        }
    }
},
{
    „nazwa”: „próg”,
    „format”: „num”,
    „jednostka”: „km/h”,
    „wartość”: 61,
    „ro”: false,
    „opis”: „Minimalna prędkość dla naruszenia”
    „zmiany-wartości”: {
        „dozwolone”: true,
        „lista”: [
            {
                „godz-od”: „23:00”,
                „godz-do”: „04:00”,
                „wartość”: 71
            }
        ]
    }
}
},
{
    „nazwa”: „aktywny”,
    „format”: „bool”,
    „wartość”: true,
    „ro”: false,
    „opis”: „Oznaczenie stanu urządzenia – faktu rejestracji pomiarów”
}
]
}

```

8.3.2 Zapytanie o parametr

Zapytania o parametr Urządzenia realizowane są przez centralę poprzez wysłanie zapytania GET na adres `http://<Urządzenie>/Zapytanie/{nazwa-parametru}`

Odpowiedź ma następującą postać:

```

{
    „typ”: „Odp.Parametr:1.0”,
    „nazwa”: „<nazwa parametru>”,
    „format”: („num” | „str” | „bool”),
    „jednostka”: „<jednostka>”,
    „wartość”: „<wartość parametru>”,

```

```

    „ro”: (true | false)
    „opis”: „<Wyjaśnienie znaczenia parametru>”
    „zmiany-wartości”: {
        „dozwolone”: (true | false),
        „lista”: [
            {
                „godz-od”: „gg:mm”,
                „godz-do”: „gg:mm”,
                „kategoria”: („ciężarowy” | „osobowy”)
            }
        ]
    }
    „kierunek”: („P” | „T”),
    „wartość”: <wartość>
    ...
}

```

Zawartość pól jest analogiczna do opisu w poprzednim rozdziale. Dodatkowe parametry Urządzenia (rozszerzenia) powinny zachowywać ten sam format.

Przykład:

```

{
    „typ”: „Odp.Parametr:1.0”,
    „nazwa”: „limit”,
    „format”: „num”,
    „wartość”: 50,
    „jednostka”: „km/h”,
    „ro”: false,
    „opis”: „Dopuszczalna prędkość”
    „zmiany-wartości”: {
        „dozwolone”: true,
        „lista”: [
            {
                „godz-od”: „23:00”,
                „godz-do”: „04:00”,
                „wartość”: 60
            }
        ]
    }
}

```

8.4 Zlecenia

Wymagalność obsługi zleceń w podziale na rodzaj urządzenia (W – wymagane, X – nie występuje):

Typ zlecenia	miar-punktowy	miar-odcinkowy	czerwone-swiatło
Format podstawowy	W	W	W

8.4.1 Format podstawowy

Zlecenia do Urządzenia są realizowane przez centralę poprzez przesłanie na adres <http://<Urządzenie>/Zlecenie> komunikatu z treścią zlecenia.

Urządzenie odpowiada kodem 200 jeśli przyjęło i wykonało zlecenie lub błędy z grupy 4xx lub 5xx.

Zlecenie ma następującą postać:

```

{

```

```

„typ”: „Zmiana.Parametru:1.0”,
„parametry”: [
  {
    „typ”: „Zmiana.Parametru:1.0”,
    „nazwa”: „<nazwa parametru>”,
    „wartość”: <wartość parametru>,
    „zmiany-wartości”: [
      {
        „godz-od”: „gg:mm”,
        „godz-do”: „gg:mm”,
        „kategoria”: („ciężarowy” | „osobowy”),
        „kierunek”: („P” | „T”),
        „wartość”: <wartość>
      },
      [...]
    ]
  },
  [...]
]
}

```

Komunikat w polu „parametry” jest więc w praktyce listą zleceń: w ten sposób można jednym poleceniem zmienić kilka parametrów (np. limit i próg jednocześnie). Urządzenie musi przyjąć wszystkie parametry z komunikatu lub wszystkie odrzucić. Dzięki temu na przykład limit i próg zostaną albo jednocześnie zmienione, albo żaden z nich nie zostanie zmieniony.

Przykład:

```

{
  „typ”: „Zmiana.Parametru:1.0”,
  „parametry”: [
    {
      „nazwa”: „limit”,
      „wartość”: 50,
      „zmiany-wartości”: [
        {„godz-od”: „23:00”, „godz-do”: „04:00”, wartość: 60}
      ]
    },
    {
      „nazwa”: „próg”,
      „wartość”: 61,
      „zmiany-wartości”: [
        {„godz-od”: „23:00”, „godz-do”: „04:00”, wartość: 71},
        {„godz-od”: „14:00”, „godz-do”: „18:00”, wartość: 81},
      ]
    }
  ]
}

```

9 Scenariusze użycia

Poniżej przedstawiono typowe przebiegi komunikacji pomiędzy Urządzeniem a centralą.

Tabele demonstrują polecenia HTTP jak również nagłówki HTTP i treść komunikatów.

Nagłówki wskazują fakt kompresji danych, ale w dokumencie zademonstrowano treść po dekompresji.

9.1 Zapytanie o właściwości Urządzenia

Przykład demonstruje odpytanie Urządzenia o jego parametry.

C->U	GET /Zapytanie HTTP/1.1 Accept: application/json Accept-encoding: gzip Connection: close Host: urzadzenie-x
U->C	HTTP/1.1 200 OK. Content-Type: application/json Content-encoding: gzip Content-length: xxx Connection: close
	<pre> { "typ": "Odp.Rozpoznanie:1.0", "czas": "1970-02-12 01:13:14.124", "rodzja": "pomiar-punktowy", "klucz": ["-----BEGIN PUBLIC KEY-----", "MIIBIjANBgkqhkiG9w0BAQEFAAOCA...", "K4TflGcXvQ0L7Q6Vb7FpEH4GiQrb...", "...", "8wIDAQAB=" "-----END PUBLIC KEY-----"], "parametry": [{ "nazwa": "numer-Urządzenia", "format": "string", "wartość": "1234-234-12345", "ro": true, "opis": "Numer seryjny Urządzenia" }, { "nazwa": "temp", "format": "num", "wartość": 25, "jednostka": "C", "ro": true, "opis": "Bieżąca temperatura pracy Urządzenia" }, { "nazwa": "temp-min", "format": "num", "wartość": -5, "jednostka": "C", "ro": false, "opis": "Minimalna akceptowalna temperatura pracy" }, { "nazwa": "temp-max", </pre>

	Content-type: application/gzip Content-length: xxxx Connection: close Host: centrala
	{„typ”: „Nowy.Dowód:1.0”, „id”: „1045”, „czas”: „2015:04:12 23:59.000”}
C->U	HTTP/1.1 200 OK. Connection: close
C->U	GET /Dowod/1045 HTTP/1.1 Accept: application/x-7z-compressed Connection: close Host: Urządzenie-x
U->C	HTTP/1.1 200 OK Content-length: xxx Content-type: application/x-7z-compressed Connection: close ... bajty archiwum dowodu ...
C->U	DELETE /Dowod/1045 HTTP/1.1 Connection: close Host: Urządzenie-x
U->C	HTTP/1.1 200 OK Connection: close

9.3 Zgłoszenie stanu pracy Urządzenia/alertu

Urządzenie zgłasza do centrali alert.

U->C	POST /Alert HTTP/1.1 Accept: application/json Accept-encoding: gzip Content-type: application/gzip Content-length: xxxx Connection: close Host: centrala {“typ”: “Przekroczenie.parametru:1.0”, „producent”: „ABC”, „model”: „ABC-124”, „numer-seryjny”: „1234-234-12”, „czas”: „2001:12:24 22:45:23.123”, “parametr”: “temp”,
------	---

	"wartość": "85"}
C->U	HTTP/1.1 200 OK. Connection: close

9.4 Odpytanie o stan parametrów

Scenariusz demonstruje operację pobrania wartości parametru z Urządzenia.

C->U	GET /Zapytanie/limit HTTP/1.1
	Accept: application/json Accept-encoding: gzip Connection: close Host: Urządzenie-x
U->C	HTTP/1.1 200 OK Content-length: xxx Content-type: application/json Content-encoding: gzip Connection: close
	<pre>{ „typ”: „Odp.Parametr:1.0”, „nazwa”: „limit”, „format”: „num”, „wartość”: 50, „jednostka”: „km/h”, „ro”: false, „opis”: „Dopuszczalna prędkość” „zmiany-wartości”: { „dozwolone”: true, „lista”: [{ „godz-od”: „23:00”, „godz-do”: „04:00”, „wartość”: 60 }] } }</pre>

9.5 Modyfikacja parametru pracy Urządzenia

W tym scenariuszu pobiera się wartość parametrów limit i próg a następnie ustawia ponownie ich wartości w Urządzeniu.

C->U	GET /Zapytanie/limit HTTP/1.1
	Accept: application/json Accept-encoding: gzip Connection: close

	Host: Urządzenie-x
U->C	<p>HTTP/1.1 200 OK</p> <p>Content-length: xxx</p> <p>Content-type: application/json</p> <p>Content-encoding: gzip</p> <p>Connection: close</p>
	<pre> { „typ”: „Odp.Parametr:1.0”, „nazwa”: „limit”, „format”: „num”, „wartość”: 50, „jednostka”: „km/h”, „ro”: false, „opis”: „Dopuszczalna prędkość” „zmiany-wartości”: { „dozwolone”: true, „lista”: [{ „godz-od”: „23:00”, „godz-do”: „04:00”, „wartość”: 60 }] } } </pre>
C->U	<p>GET /Zapytanie/próg HTTP/1.1</p> <p>Accept: application/json</p> <p>Accept-encoding: gzip</p> <p>Connection: close</p> <p>Host: Urządzenie-x</p>
U->C	<p>HTTP/1.1 200 OK</p> <p>Content-length: xxx</p> <p>Content-type: application/json</p> <p>Content-encoding: gzip</p> <p>Connection: close</p>
	<pre> { „typ”: „Odp.Parametr:1.0”, „nazwa”: „próg”, „format”: „num”, „wartość”: 61, „jednostka”: „km/h”, „ro”: false, „opis”: „Wyzwalacz” „zmiany-wartości”: { „dozwolone”: true, „lista”: [</pre>

	<pre> „godz-od”: „23:00”, „godz-do”: „04:00”, „wartość”: 71 }] } </pre>
C->U	<p>POST /Zlecenie HTTP/1.1</p> <p>Accept: application/json</p> <p>Accept-encoding: gzip</p> <p>Content-type: application/gzip</p> <p>Content-length: xxxx</p> <p>Connection: close</p> <p>Host: Urządzenie-x</p> <pre> { „typ”: „Zmiana.Parametru:1.0”, „parametry”: [{ „nazwa”: „limit”, „wartość”: 50, „zmiany-wartości”: [{„godz-od”: „23:00”, „godz-do”: „04:00”, wartość: 60}] }, { „nazwa”: „próg”, „wartość”: 61, „zmiany-wartości”: [{„godz-od”: „23:00”, „godz-do”: „04:00”, wartość: 71}, {„godz-od”: „14:00”, „godz-do”: „18:00”, wartość: 81},] }] } </pre>
U->C	<p>HTTP/1.1 200 OK.</p> <p>Connection: close</p>

9.6 Obsługa informacji statystycznych

U->C	<p>POST /Alert HTTP/1.1</p> <p>Accept: application/json</p> <p>Accept-encoding: gzip</p> <p>Content-type: application/gzip</p> <p>Content-length: xxxx</p>
------	--

	Connection: close
	Host: centrala
	<pre>{ "typ": "Ogólne.Zgłoszenie:1.0", "producent": "ABC", "model": "RDR/1.0", "numer-seryjny": "1234-1234", "czas": "2001-01-02 12:14:24.123", "statystyki": [{ "czas": "2001-01-02 10:15:17.120", "prędkość": "62" }, { "czas": "2001-01-02 10:16:35.743", "prędkość": "84" }] }</pre>
C->U	HTTP/1.1 200 OK. Connection: close

10 Zasady weryfikacji zgodności ze standardem

Na potrzeby weryfikacji poprawności zgodności Urządzenia ze standardem przygotowane zostanie oprogramowanie symulujące pracę centrali.

Test Urządzenia obejmuje wykonanie kilku przebiegów na podstawie scenariuszy przedstawionych w rozdziale 9 rozszerzonych o sytuacje awaryjne – np. niedostępność, przerwy w komunikacji lub restart w trakcie przetwarzania.

Urządzenie działające poprawnie z symulatorem zostanie zaklasyfikowane jako poprawne.

Poprawność centrali będzie testowana w oparciu o Urządzenia, które przeszły testy z symulatorem.