DZIENNIK USTAW
RZECZYPOSPOLITEJ POLSKIEJ

Warszawa, dnia 9 listopada 2026 r.

Poz. 1475

ROZPORZĄDZENIE
RADY MINISTRÓW

z dnia 29 października 2026 r.

w sprawie wymagań technicznych i eksploatacyjnych dla interfejsów

Na podstawie art. 46 ust. 2 ustawy z dnia 12 lipca 2024 r. – Prawo komunikacji elektronicznej (Dz. U. poz. 1221, z 2025 r. poz. 637 i 820 oraz z 2026 r. poz. 252, 815 i 1296) zarządza się, co następuje:

§ 1. 1. Rozporządzenie określa wymagania techniczne i eksploatacyjne dla interfejsów, o których mowa w art. 43 ust. 5 ustawy z dnia 12 lipca 2024 r. – Prawo komunikacji elektronicznej, zwanej dalej „ustawą", umożliwiających zapewnienie warunków technicznych i organizacyjnych dostępu i utrwalania, o których mowa w art. 43 ust. 1 pkt 1 ustawy, oraz przygotowanie technicznych i organizacyjnych warunków udostępniania danych, o których mowa w art. 45 ust. 1 ustawy, oraz ich udostępniania.

2. Wymagania, o których mowa w ust. 1, są określone w załączniku nr 1 do rozporządzenia.

§ 2. W przypadku interfejsów LI HI stosowanych na podstawie umów, o których mowa w art. 43 ust. 5 ustawy, zawartych przed dniem wejścia w życie rozporządzenia, w zakresie usług telekomunikacyjnych objętych tymi umowami, stosuje się wymagania, o których mowa w § 1 ust. 1, określone w załączniku nr 2 do rozporządzenia, jednak niedłużej niż 36 miesięcy od dnia wejścia w życie rozporządzenia.

§ 3. Rozporządzenie wchodzi w życie z dniem 11 listopada 2026 r.[1)]

Prezes Rady Ministrów: *D. Tusk*

---

1) Niniejsze rozporządzenie było poprzedzone rozporządzeniem Rady Ministrów z dnia 20 stycznia 2012 r. w sprawie wymagań technicznych i eksploatacyjnych dla interfejsów umożliwiających wykonywanie zadań i obowiązków na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego (Dz. U. poz. 200 oraz z 2019 r. poz. 2135), które traci moc zgodnie z art. 104 pkt 26 ustawy z dnia 12 lipca 2024 r. – Przepisy wprowadzające ustawę – Prawo komunikacji elektronicznej (Dz. U. poz. 1222 oraz z 2026 r. poz. 252).

Załączniki do rozporządzenia Rady Ministrów
z dnia 29 października 2026 r. (Dz. U. poz. 1475)

Załącznik nr 1

WYMAGANIA TECHNICZNE I EKSPLOATACYJNE DLA INTERFEJSÓW

1. Przepisy ogólne

Wymagania techniczne i eksploatacyjne dla interfejsów uznaje się za spełnione, gdy interfejsy zapewniają realizację obowiązków, o których mowa w art. 43 ust. 1 pkt 1 oraz art. 45 ust. 1 ustawy z dnia 12 lipca 2024 r. – Prawo komunikacji elektronicznej (Dz. U. poz. 1221, z 2025 r. poz. 637 i 820 oraz z 2026 r. poz. 252, 815 i 1296), zwanej dalej „ustawą”.

Dopuszcza się stosowanie do interfejsów wymagań określonych w dokumentach w wersjach innych niż wskazane w pkt 2, jeżeli interfejsy spełniające te wymagania zapewniają realizację obowiązków, o których mowa w art. 43 ust. 1 pkt 1 oraz art. 45 ust. 1 ustawy, w stopniu niemniejszym niż w przypadku wymagań określonych w dokumentach w wersjach wskazanych w załączniku.

2. Wykaz dokumentów

2.1. Wykaz dokumentów powoływanych w załączniku:

[1] ETSI TS 101 671 V3.11.1 Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic, zwany dalej „ETSI TS 101 671”;

[2] ETSI TS 102 232-1 V3.2.1 Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 1: Handover specification for IP delivery, zwany dalej „ETSI TS 102 232-1”;

[3] ETSI TS 102 232-3 (wersja wynikająca z zależności od wersji ETSI TS 102 232-1) Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 3: Service-specific details for internet access services, zwany dalej „ETSI TS 102 232-3”;

[4] ETSI TS 102 232-5 (wersja wynikająca z zależności od wersji ETSI TS 102 232-1) Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 5: Service-specific details for IP Multimedia Services, zwany dalej „ETSI TS 102 232-5”;

[5] ETSI TS 102 232-6 (wersja wynikająca z zależności od wersji ETSI TS 102 232-1) Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 6: Service-specific details for PSTN/ISDN services, zwany dalej „ETSI TS 102 232-6”;

[6] ETSI TS 102 232-7 (wersja wynikająca z zależności od wersji ETSI TS 102 232-1) Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 7: Service-specific details for Mobile Services, zwany dalej „ETSI TS 102 232-7”;

[7] ETSI TS 102 657 V1.7.1 Lawful Interception (LI); Retained data handling; Handover interface for the request and delivery of retained data, zwany dalej „ETSI TS 102 657”;

[8] ETSI ETS 300 927 Digital cellular telecommunications system (Phase 2+) (GSM); Numbering, addressing and identification (GSM 03.03 version 5.2.1 Release 1996), zwany dalej „ETSI ETS 300 927”;

[9] ETSI TS 102 280 V1.1.1 X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons (2004-03), zwany dalej „ETSI TS 102 280”;

[10] ETSI TS 133 108 V12.8.0 Universal Mobile Telecommunications System (UMTS); LTE; 3G security; Handover interface for Lawful Interception (LI), zwany dalej „ETSI TS 133 108”;

[11] ETSI TS 133 128 V18.15.0 Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G; Security; Protocol and procedures for Lawful Interception (LI); Stage 3, zwany dalej „ETSI TS 133 128”;

[12] IEEE 802.3-2022 IEEE Standard for Ethernet, zwany dalej „IEEE 802.3”;

[13] IETF RFC 0791 Internet Protocol, zwany dalej „IETF RFC 0791”;

[14] IETF RFC 0793 Transmission Control Protocol, zwany dalej „IETF RFC 0793”;

[15] IETF RFC 2315 Cryptographic Message Syntax, Version 1.5, zwany dalej „IETF RFC 2315”;

[16] IETF RFC 2460 Internet Protocol, Version 6 (IPv6) Specification, zwany dalej „IETF RFC 2460”;

[17] IETF RFC 5652 Cryptographic Message Syntax (CMS), zwany dalej „IETF RFC 5652”;

[18] IETF RFC 4291 Internet Protocol Version 6 (IPv6) Addressing Architecture, zwany dalej „IETF RFC 4291”;

[19] ITU-T X.680 Information Technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation, zwany dalej „ITU-T X.680”;

[20] ITU-T X.681 Information Technology – Abstract Syntax Notation One (ASN.1): Information object specification, zwany dalej „ITU-T X.681”;

[21] ITU-T X.682 Information Technology – Abstract Syntax Notation One (ASN.1): Constraint specification, zwany dalej „ITU-T X.682”;

[22] ITU-T X.683 Information Technology – Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specifications, zwany dalej „ITU-T X.683”;

[23] ITU-T X.690 Information Technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER), zwany dalej „ITU-T X.690”.

2.2. W przypadku gdy wykaz, o którym mowa w pkt 2.1, zawiera odesłanie do konkretnej wersji dokumentu, stosuje się wymagania wskazane w tej wersji dokumentu. Dopuszczalne jest spełnienie wymagań określonych w nowszej wersji dokumentu.

2.3. Dokumenty, o których mowa w pkt 2.1 w poz. [1]–[11], są dostępne na stronie Europejskiego Instytutu Norm Telekomunikacyjnych (ETSI): www.etsi.org.

2.4. Dokument, o którym mowa w pkt 2.1 w poz. [12], jest dostępny na stronie Instytutu Inżynierów Elektryków i Elektroników (IEEE): www.ieee.org.

2.5. Dokumenty, o których mowa w pkt 2.1 w poz. [13]–[18], są dostępne na stronie zespołu inżynierów ustanawiających standardy techniczne i organizacyjne w Internecie, Internet Engineering Task Force (IETF): www.ietf.org.

2.6. Dokumenty, o których mowa w pkt 2.1 w poz. [19]–[23], są dostępne na stronie Międzynarodowego Związku Telekomunikacyjnego (ITU): www.itu.int.

3. Akronimy

Użyte w załączniku akronimy oznaczają:

1) ADMF – system przedsiębiorcy telekomunikacyjnego umożliwiający realizację dostępu do komunikatów elektronicznych i związanych z nimi danych, o których mowa w art. 43 ust. 1 pkt 1 oraz art. 45 ust. 1 ustawy (Administration Function);
2) ASCII – kod przyporządkowujący liczby z zakresu od 0 do 127 literom alfabetu angielskiego, cyfrom, znakom przestankowym i innym symbolom oraz poleceniom sterującym (American Standard Code for Information Interchange);
3) ASN.1 – znormalizowaną notację stosowaną do opisu struktur danych (Abstract Syntax Notation One), zdefiniowaną w ITU-T X.680 [19], ITU-T X.681 [20], ITU-T X.682 [21] i ITU-T X.683 [22];
4) BER – sposób kodowania informacji zapisanej przy użyciu ASN.1 do postaci transmitowanej w sieciach telekomunikacyjnych (Basic Encoding Rules), zgodny z ITU-T X.690 [23];
5) CA – urząd certyfikacji (Certificate Authority);
6) CC – treść komunikatu elektronicznego (Content of Communication);
7) CDMA – wielodostęp z podziałem kodowym (Code Division Multiple Access);
8) CMS – standard zabezpieczania wiadomości (Cryptographic Message Syntax), zdefiniowany w IETF RFC 5652 [17];
9) CS – komutację kanałów (Circuit Switched) umożliwiającą uzyskiwanie dostępu do danych głosowych, generowanych w sieciach stacjonarnych oraz 2G i 3G;
10) DER – sposób kodowania informacji zapisanej przy użyciu ASN.1 (Distinguished Encoding Rules), zdefiniowany w ITU-T X.690 [23];
11) DF – funkcję dostarczającą dane do LEMF (Delivery Function);
12) ESN – indywidualny numer identyfikujący telekomunikacyjne urządzenie końcowe używane w ruchomej publicznej sieci telefonicznej wykorzystującej technologię CDMA (Electronic Serial Number);
13) IMEI – indywidualny międzynarodowy numer identyfikujący telekomunikacyjne urządzenie końcowe używane w ruchomej publicznej sieci telefonicznej (International Mobile Equipment Identity);
14) IMSI – międzynarodowy numer przydzielony karcie identyfikującej użytkownika w ruchomej publicznej sieci telefonicznej (International Mobile Subscriber Identity);
15) IRI – informacje powiązane z komunikatem elektronicznym i związanymi z nim danymi, o których mowa w art. 43 ust. 1 pkt 1 ustawy (Intercept Related Information);
16) ISDN – cyfrową sieć telekomunikacyjną z integracją usług (Integrated Services Digital Network);
17) LEA – uprawnione podmioty, o których mowa w art. 43 ust. 1 pkt 1 lit. a ustawy (Law Enforcement Agency);
18) LEMF – system monitorowania LEA umożliwiający dostęp do komunikatów elektronicznych i związanych z nimi danych, o których mowa w art. 43 ust. 1 pkt 1 oraz art. 45 ust. 1 ustawy (Law Enforcement Monitoring Facility);
19) LIID – identyfikator obiektu monitorowanego (Lawful Interception Identifier);
20) LOGIN – nazwę użytkownika logującego się do sieci telekomunikacyjnej, używaną w procesie jego uwierzytelnienia;
21) MAC – sprzętowy adres karty sieciowej (Media Access Control);

22) MEID – unikalny numer identyfikujący telekomunikacyjne urządzenie końcowe używane w ruchomej publicznej sieci telefonicznej wykorzystującej technologię CDMA, zastępujący ESN (Mobile Equipment Identifier);
23) MF – funkcję pośredniczącą dostosowującą dane będące przedmiotem monitorowania, pochodzące z sieci przedsiębiorcy telekomunikacyjnego, do formatu wymaganego przez interfejs (Mediation Function);
24) MSISDN – numer przydzielony użytkownikowi końcowemu ruchomej publicznej sieci telefonicznej z integracją usług (Mobile Subscriber Integrated Services Digital Network);
25) PSTN – publiczną komutowaną sieć telefoniczną (Public Switched Telephone Network);
26) SMS – krótką wiadomość tekstową (Short Message Service);
27) TCP – protokół komunikacji w sieci komputerowej (Transmission Control Protocol), zdefiniowany w IETF RFC 0793 [14];
28) WAN – rozległą sieć komputerową (Wide Area Network);
29) VoIP – telefonię internetową (Voice over IP).

4. Definicje

Użyte w załączniku określenia oznaczają:

1) interfejs LI HI (Lawful Interception Handover Interface) – elektroniczny, zdalny i oparty na protokole komunikacyjnym IP interfejs między ADMF a LEMF, umożliwiający realizację dostępu do komunikatów elektronicznych i związanych z nimi danych, o których mowa w art. 43 ust. 1 pkt 1 ustawy, w którego skład wchodzą:

a) interfejs HI1 – styk umożliwiający dwukierunkową wymianę informacji między LEMF a ADMF, wykorzystywany przez LEMF do przesyłania żądań, a przez ADMF głównie do przesyłania notyfikacji zdarzeń lub stanu realizacji żądań, realizujący także inne funkcje, opisane w pkt 10,
b) interfejs HI2 – styk umożliwiający jednokierunkowe, w kierunku od ADMF do LEMF, przesyłanie informacji związanych z objętymi monitorowaniem komunikatami elektronicznymi i związanymi z nimi danymi, o których mowa w art. 43 ust. 1 pkt 1 ustawy, związanych ze świadczoną publicznie dostępną usługą telekomunikacyjną oraz treści SMS,
c) interfejs HI3 – styk umożliwiający jednokierunkowe, w kierunku od ADMF do LEMF, przesyłanie informacji objętych monitorowaniem;

2) interfejs HI A-B – elektroniczny, zdalny i oparty na protokole komunikacyjnym IP interfejs służący do dostarczania przez przedsiębiorcę telekomunikacyjnego do LEA danych, o których mowa w art. 45 ust. 1 ustawy, w którego skład wchodzą:

a) interfejs HI A – styk służący do realizowania funkcji administracyjnych polegających na przesyłaniu i obsłudze żądań przekazywanych w obu kierunkach między LEMF a ADMF,
b) interfejs HI B – styk służący do przekazywania przez ADMF wyników żądań składanych za pośrednictwem interfejsu HI A;

3) obiekt monitorowany – osobę wskazaną w postanowieniu sądu wydanym na podstawie wniosku albo zarządzenia organu nadzorującego LEA wydanego na podstawie odrębnych przepisów;

4) buforowanie – magazynowanie danych przez zespół urządzeń przedsiębiorcy telekomunikacyjnego do czasu ich przekazania do LEMF;

5) monitorowanie – dostęp do komunikatów elektronicznych i związanych z nimi danych, o których mowa w art. 43 ust. 1 pkt 1 ustawy.

5. Wymagania ogólne dla interfejsu LI HI

5.1. W warstwie fizycznej jest stosowany interfejs standardu Ethernet 100/1000BASE-T, zgodny z IEEE 802.3 [12]. Po akceptacji obu stron dopuszcza się również stosowanie interfejsu światłowodowego. Do obsługi każdego z LEA jest przewidziany oddzielny port w standardzie Ethernet.

5.2. Protokołem warstwy sieciowej interfejsu LI HI jest protokół IPv4, zgodny z IETF RFC 0791 [13], lub protokół IPv6, zgodny z IETF RFC 2460 [16] i IETF RFC 4291 [18]. Stosuje się publiczne adresy IP.

5.3. Sieć między ADMF a LEMF jest siecią wydzieloną (w ramach WAN), za którą odpowiada LEA. Wyboru protokołu, o którym mowa w pkt 5.2, dostosowania przesyłanych informacji oraz szyfrowania sygnału na łączach WAN dokonuje LEA.

5.4. Szyfrowanie transmisji realizuje się poza interfejsem LI HI na poziomie warstwy łącza danych lub warstwy sieciowej.

5.5. W celu identyfikacji obiektów monitorowanych wykorzystuje się niepowtarzalny dla każdego obiektu monitorowanego LIID.

5.6. Dla każdej usługi w ramach danego kryterium wyboru, o którym mowa w pkt 6.4, jest przydzielany odrębny LIID. W przypadku monitorowania więcej niż jednej usługi w ramach tego samego kryterium wyboru dla każdej kolejnej usługi nadaje się unikalny LIID.

5.7. LEMF w żądaniach interfejsu LI HI używa poniżej zdefiniowanego formatu LIID. LIID składa się z dwóch członów: LEAID (LEA Identifier) + SEQ (kolejny niepowtarzalny numer żądania). LIID jest utworzone z 17 znaków numerycznych ASCII od 0 do 9, w tym 2 cyfr określających LEAID oraz 15 cyfr wskazujących numer SEQ, zgodnie z tabelą nr 1. Wartość LEAID jest przydzielona każdemu LEA, zgodnie z tabelą nr 2.

Tabela nr 1

LIID
LEAID + SEQ
2 cyfry + 15 cyfr
Np. 01000300056043015

Tabela nr 2

LEAID		
Wartość	LEA	Opis
00	LEMF operatora	Przedsiębiorca telekomunikacyjny
01	ABW	Agencja Bezpieczeństwa Wewnętrznego
02	POLICJA	Policja
03	SKW	Służba Kontrwywiadu Wojskowego
04	ZW	Żandarmeria Wojskowa

05	SG	Straż Graniczna
06	KAS	Krajowa Administracja Skarbowa
07	CBA	Centralne Biuro Antykorupcyjne
08	SOP	Służba Ochrony Państwa
09	BNW	Biuro Nadzoru Wewnętrznego

5.8. Dopuszcza się wykorzystanie jednego portu do obsługi więcej niż jednego LEA. Wykorzystanie takiego rozwiązania ustala się na etapie uzgadniania zasad współpracy za pomocą interfejsu między przedsiębiorcą telekomunikacyjnym a zainteresowanymi LEA.

5.9. Interfejs LI HI przekazuje do LEMF bez zbędnej zwłoki komunikaty elektroniczne i związane z nimi dane, o których mowa w art. 43 ust. 1 pkt 1 ustawy. Dla interfejsu LI HI jest stosowane 72-godzinne buforowanie.

5.10. Po skutecznym przekazaniu do LEMF komunikatów elektronicznych i związanych z nimi danych, o których mowa w art. 43 ust. 1 pkt 1 ustawy, ADMF usuwa je ze swoich zasobów.

6. Wymagania dla interfejsu HI1

6.1. Interfejs HI1 zapewnia:

1) przekazywanie do ADMF żądań w zakresie włączania, modyfikacji i wyłączania monitorowania obiektów monitorowanych oraz zapytań o status obserwacji;
2) przekazywanie od ADMF do LEMF informacji o statusie realizacji zleceń i zapytań oraz informacji o występowaniu awarii;
3) możliwość realizacji podstawowych testów diagnostycznych tego interfejsu;
4) w pełni automatyczną realizację zleceń przekazywanych od LEMF, bez udziału pracowników przedsiębiorcy telekomunikacyjnego.

6.2. W celu aktywacji każdego zlecenia monitorowania LEA określa:

1) LIID;
2) obiekt monitorowany;
3) monitorowaną usługę telekomunikacyjną;
4) zakres monitorowania;
5) okres monitorowania.

6.3. Interfejs HI1 zapewnia następujące kryteria wyboru obiektu monitorowanego w sieciach telekomunikacyjnych, stosownie do rodzaju sieci:

1) numer abonenta PSTN/ISDN/MSISDN/VoIP;
2) IMSI;
3) IMEI o długości 15 cyfr, zgodny z ETSI ETS 300 927 [8];
4) LOGIN;

5) adres IP;

6) MAC;

7) ESN albo MEID.

6.4. Interfejs HI1 zapewnia następujące kryteria wyboru monitorowanych usług telekomunikacyjnych, stosownie do rodzaju sieci:

1) połączenia głosowe oraz wiadomości tekstowe;

2) transmisję danych, w tym wiadomości multimedialne.

Dopuszcza się zapewnienie dodatkowych kryteriów wyboru monitorowanych usług telekomunikacyjnych zgodnie z ustaleniami zawartymi w umowie, o której mowa w art. 43 ust. 5 ustawy.

6.5. Przez zakres monitorowania LEA wskazuje jeden z dwóch zakresów odnoszących się do danych:

1) IRI oraz opcjonalnie treści SMS;

2) IRI + CC.

6.6. Wysyłanie zleceń aktywacji następuje w chwili rzeczywistego uruchamiania monitorowania albo z wyprzedzeniem. Maksymalne wyprzedzenie ustala się na etapie uzgadniania zasad współpracy za pomocą interfejsu. W zleceniu aktywacji określa się czas zakończenia monitorowania.

6.7. Zlecenie modyfikacji monitorowania obejmuje czas wyłączenia monitorowania.

6.8. ADMF przesyła do LEMF informację o czasie faktycznego wykonania zlecenia aktywacji, dezaktywacji albo modyfikacji monitorowania. W przypadku błędu w trakcie wykonywania zlecenia przesyła informację o fakcie pojawienia się błędu lub braku możliwości wykonania zlecenia.

6.9. ADMF w odpowiedzi na pytanie o status obserwacji nie przesyła żadnych danych identyfikujących obiekt monitorowany poza LIID.

6.10. Zlecenia wystawiane przez użytkownika LEMF, z wyjątkiem weryfikacji stanu obserwacji, są podpisywane elektronicznie.

6.11. Formatem stosowanego podpisu elektronicznego żądań interfejsu HI1 jest CMS. Na potrzeby stosowania podpisu elektronicznego są wykorzystywane certyfikaty określone w ETSI TS 102 280 [9], z uwzględnieniem wymagań technicznych dla certyfikatów, o których mowa w ustawie z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. z 2024 r. poz. 1725 oraz z 2026 r. poz. 252), oraz Infrastruktury Klucza Publicznego, będącej systemem kryptograficznym, w którego skład wchodzą urzędy certyfikacyjne, użytkownicy certyfikatów (subskrybenci) oraz oprogramowanie i sprzęt (Public Key Infrastructure).

6.12. Szczegółowa struktura interfejsu HI1 jest przedstawiona w pkt 10.

6.13. Za zgodą LEA dopuszcza się pracę interfejsu HI1 w trybie półautomatycznym, w którym pracownik przedsiębiorcy telekomunikacyjnego spełniający wymagania określone w art. 43 ust. 9 ustawy, po odebraniu zlecenia od LEMF wykonuje prace niezbędne do przygotowania sieci przedsiębiorcy telekomunikacyjnego do realizacji zlecenia. Czas na przeprowadzenie tych prac nie przekracza 24 godzin.

7. Wymagania dla interfejsu HI2

7.1. Informacje związane z objętymi monitorowaniem komunikatami elektronicznymi i związanymi z nimi danymi, o których mowa w art. 43 ust. 1 pkt 1 ustawy, dotyczące świadczonej publicznie dostępnej usługi telekomunikacyjnej są przekazywane do LEMF niezwłocznie, jednak niepóźniej niż 10 minut od zakończenia przekazu.

7.2. Przesyłanie do LEMF informacji związanych z objętymi monitorowaniem komunikatami elektronicznymi i związanymi z nimi danymi, o których mowa w art. 43 ust. 1 pkt 1 ustawy, dotyczących świadczonej usługi telekomunikacyjnej odbywa się z wykorzystaniem TCP, zgodnie z ETSI TS 102 232-1 [2], łącznie z mechanizmem potwierdzania PDU (Protocol Data Unit) i zaleceniami dotyczącymi TCP.

7.3. Połączenia TCP są inicjowane w kierunku od ADMF do LEMF.

7.4. Zawartość strumieni (zawierających IRI) jest kodowana z wykorzystaniem ASN.1/BER zgodnie z:

1) ETSI TS 102 232-1 [2] oraz ETSI TS 102 232-7 [6] lub ETSI TS 133 108 [10] albo ETSI TS 133 128 [11] w odniesieniu do usług świadczonych w sieciach ruchomych oraz usług transmisji pakietowej świadczonych w sieciach ruchomych;
2) ETSI TS 102 232-1 [2] oraz ETSI TS 102 232-6 [5] lub ETSI TS 101 671 [1] w odniesieniu do usług świadczonych w stacjonarnej publicznej sieci telekomunikacyjnej oraz ruchomej publicznej sieci telekomunikacyjnej w technologii 2G/3G;
3) ETSI TS 102 232-1 [2] i ETSI TS 102 232-3 [3] w odniesieniu do usług dostępu do internetu w stacjonarnej publicznej sieci telekomunikacyjnej;
4) ETSI TS 102 232-1 [2] i ETSI TS 102 232-5 [4] w odniesieniu do usług VoIP.

7.5. Specyfikacja interfejsu HI2 jest rozszerzona o parametr ExtendedPartyIdentity. Specyfikacja struktur danych w ASN.1 opisujących format tego parametru jest przedstawiona w pkt 11.

7.6. Wartości parametrów IRI definiuje się w formatach (np. ISDN user part, DSS1, MAP, IP) zalecanych przez dotyczące ich ETSI, w tym ETSI TS 101 671 [1], ETSI TS 102 232-1 [2], ETSI TS 102 232-3 [3], ETSI TS 102 232-5 [4], ETSI TS 102 232-6 [5] i ETSI TS 102 232-7 [6].

7.7. Po skutecznym przekazaniu rekordów IRI ADMF usuwa związane z nimi dane ze swoich zasobów.

7.8. Interfejs HI2 nie wymaga stosowania podpisu elektronicznego.

8. Wymagania dla interfejsu HI3

8.1. Rozpoczęcie przekazywania do LEMF komunikatów elektronicznych i związanych z nimi danych, o których mowa w art. 43 ust. 1 pkt 1 ustawy, objętych monitorowaniem następuje niepóźniej niż 10 minut od zakończenia przekazu.

8.2. Korelacja między rekordami IRI (w interfejsie HI2) a przekazywaną CC (w interfejsie HI3) odbywa się z wykorzystaniem LIID, a w przypadku usług sieci z komutacją kanałów – również parametru CIN (Communication Identity Number).

8.3. Do przekazywania informacji objętych monitorowaniem stosuje się odpowiednio:

1) ETSI TS 102 232-1 [2] i ETSI TS 102 232-6 [5] w odniesieniu do usług telekomunikacyjnych świadczonych w ruchomej publicznej sieci telekomunikacyjnej oraz w stacjonarnej publicznej sieci telekomunikacyjnej;
2) ETSI TS 102 232-1 [2] oraz ETSI TS 102 232-3 [3] albo ETSI TS 133 128 [11] w odniesieniu do usług dostępu do internetu;
3) ETSI TS 102 232-1 [2] oraz ETSI TS 102 232-5 [4] albo ETSI TS 133 128 [11] w odniesieniu do usług VoIP.

8.4. Komunikaty elektroniczne i związane z nimi dane, o których mowa w art. 43 ust. 1 pkt 1 ustawy, wysyłane i odbierane przez obiekt monitorowany ADMF przesyła do LEMF w czasie rzeczywistym z wykorzystaniem TCP.

8.5. LEA może zwrócić się do przedsiębiorcy telekomunikacyjnego o dostarczenie kodeków umożliwiających prawidłowy odbiór połączeń głosowych i wideo.

8.6. Po skutecznym przekazaniu do LEMF komunikatów elektronicznych i związanych z nimi danych, o których mowa w art. 43 ust. 1 pkt 1 ustawy, ADMF usuwa je ze swoich zasobów.

8.7. Interfejs HI3 nie wymaga stosowania podpisu elektronicznego.

9. Wymagania dla interfejsu HI A-B

9.1. Interfejs ADMF jest dostępny w jednym punkcie (jednej lokalizacji) dla wszystkich LEA. Do obsługi każdego z LEA jest przewidziany oddzielny port w standardzie Ethernet.

9.2. W warstwie fizycznej jest stosowany interfejs standardu Ethernet 100/1000BASE-T, zgodny z IEEE 802.3 [12].

9.3. Protokołem warstwy sieciowej interfejsu HI A-B jest protokół IPv4, zgodny z IETF RFC 0791 [13], lub protokół IPv6, zgodny z IETF RFC 2460 [16] i IETF RFC 4291 [18]. Stosuje się publiczne adresy IP.

9.4. Interfejs HI A-B wymaga stosowania podpisu elektronicznego.

9.5. Realizacja interfejsu HI A-B jest zgodna z ETSI TS 102 657 [7].

9.6. Do komunikacji w interfejsie HI A-B stosuje się wariant określony w pkt 7.3 ETSI TS 102 657 [7], w którym:

1) w warstwie transportowej jest stosowany TCP;
2) jest stosowane kodowanie elementów informacyjnych z wykorzystaniem ASN.1/BER.

9.7. Wartość parametru CSPID (Communications Service Provider Identifier) odpowiada numerowi danego przedsiębiorcy telekomunikacyjnemu w rejestrze przedsiębiorców telekomunikacyjnych.

9.8. Pole countryCode w parametrze RequestID przyjmuje oznaczenie „PL”.

9.9. Pole authorisedOrganisationID w parametrze RequestID przyjmuje wartość LEAID przypisaną danemu LEA w tabeli nr 2 w pkt 5.7.

9.10. Nie stosuje się niżej wymienionych rozwiązań opcjonalnych:

1) priorytetów dla obsługi żądań skierowanych przez LEA RequestPriority, zgodnie z pkt A.2.2.1 Aneksu A w ETSI TS 102 657 [7];
2) mechanizmu multi-part delivery, zgodnie z pkt 5.1.7 w ETSI TS 102 657 [7];
3) trybu Authorized-Organization-initiated, zgodnie z pkt 5.3 w ETSI TS 102 657 [7].

9.11. Nie wykorzystuje się elementów informacyjnych wymienionych w tabeli nr 3.

Tabela nr 3

Numer tabeli w ETSI TS 102 657 [7]	Nazwa pola
Table A.12: IndividualInfo parameters	dateOfBirth
	gender
	identificationNumber
	authenticationInfo
	profession
Table B.3: TelephonyBillingDetails parameters	subscriberID
	serviceID
	billingAddress
	billingIdentifier
	billingRecords
Table B.4: BillingRecords parameters	time
	place
	amount
	currency
	method
Table B.11: Location parameters	postalLocation
	extendedLocation
Table D.3: MultimediaBillingDetails parameters	subscriberID
	serviceID
	billingAddress
	billingIdentifier
	billingRecords
Table D.4: MultimedaBillingRecords parameters	time
	place
	amount
	currency
	method
Table E.3: NAserviceUsage parameters	octetsDownloaded
	octetsUploaded

Table E.8: NABillingDetails parameters	billingAddress
	billingIdentifier
	billingRecords

10. Struktura interfejsu HI1

10.1. Warstwa transportowa:

1) jest stosowany TCP;
2) połączenia TCP są zestawiane w kierunkach:
   a) od ADMF/MF/DF do LEMF (HI1LEMFOperations),
   b) od LEMF do ADMF/MF/DF (HI1ADMFOperations);
3) w ramach jednego połączenia TCP jest wysyłana jedna wiadomość warstwy aplikacyjnej (żądanie, alarm), która jest potwierdzana przez drugą stronę (potwierdzenie otrzymania żądania, alarmu).

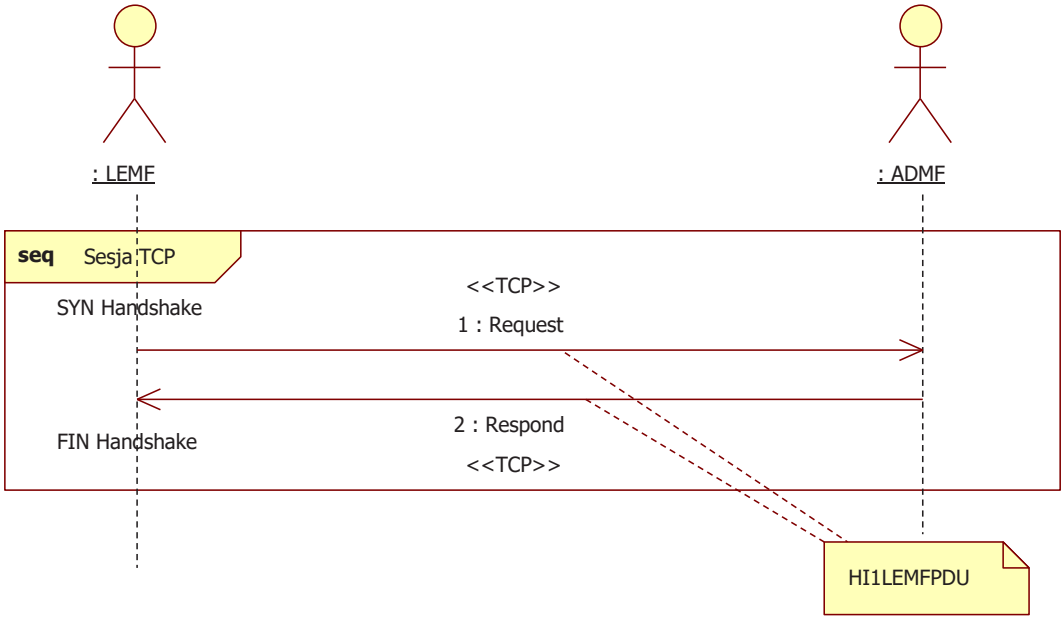
10.2. Warstwa aplikacyjna: wysyłane wiadomości są zdefiniowane w ASN.1 i są kodowane w standardzie BER lub DER.

10.2.1. Opis:

1) przeznaczenie: przesyłanie zleceń aktywacji, dezaktywacji i modyfikacji, zapytań o status zlecenia, alarmów oraz raportów, w tym o statusie interfejsu;
2) są stosowane dwa protokoły zdefiniowane w ASN.1:
   a) HI1LEMFOperations – protokół przeznaczony do operacji inicjowanych przez LEMF,
   b) HI1ADMFOperations – protokół przeznaczony do przesyłania alarmów i powiadomień wysyłanych przez ADMF;
3) protokoły HI1LEMFOperations i HI1ADMFOperations są całkowicie od siebie niezależne;
4) obsługa każdego z żądań jest realizowana w ramach jednej sesji TCP;
5) każde żądanie jest potwierdzane przez drugą stronę.

10.2.2. Protokół HI1LEMFOperations:

1) żądania przesyłane przez LEMF:
   a) żądania proste:
      – Hello,
      – ListRequest,
   b) żądania podpisane:
      – Activate,
      – Modificate, z wyjątkiem włączania/wyłączania trybu online,
      – Deactivate;
2) każde żądanie przesłane przez LEMF (Request) jest potwierdzane przez ADMF elementem informacyjnym LEMF (Respond), zgodnie ze schematem przedstawionym na rysunku 1;



Rysunek 1. Schemat obsługi żądań

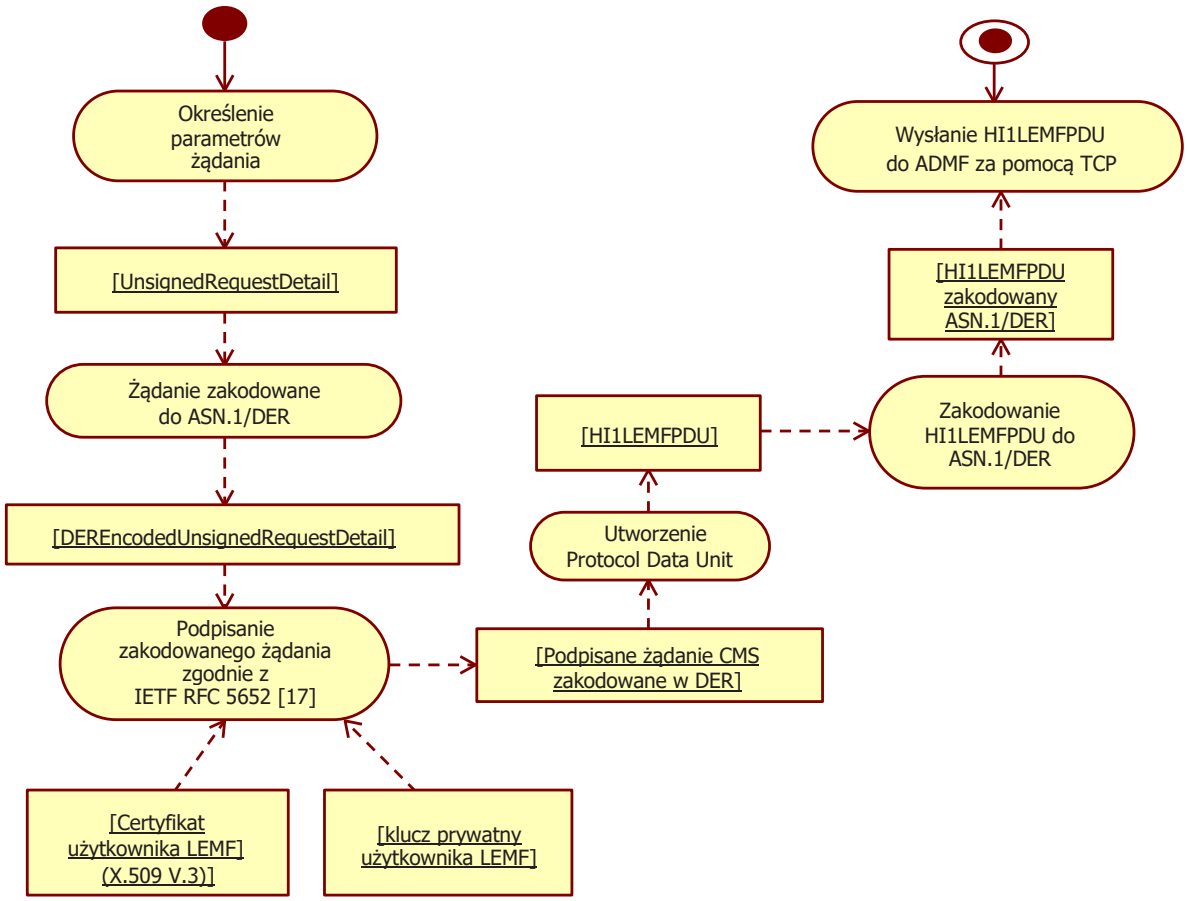
3) LEMF czeka na odpowiedź 10 sekund, a po upływie tego czasu uznaje wysłaną wiadomość za utraconą;
4) nad harmonogramem aktywacji i dezaktywacji czuwa LEMF; dopuszcza się przesłanie zlecenia aktywacji z wyprzedzeniem, przy czym zlecenie aktywacji ma określony czas zakończenia monitorowania, a przesunięcie momentu zakończenia monitorowania ponad ten czas wymaga zlecenia modyfikacji;
5) ADMF przesyła do LEMF informacje o założeniu lub zdjęciu monitorowania w elementach sieci przedsiębiorcy telekomunikacyjnego;
6) LEMF ma możliwość zadania zapytania (ListRequest) służącego do weryfikacji statusu monitorowania;
7) zlecenie dezaktywacji oznacza niezwłoczne zakończenie wskazanej obserwacji, a w przypadku obserwacji, która się jeszcze nie rozpoczęła – jej niezrealizowanie, przy czym fakt założenia tej obserwacji odnotowuje się w logach systemu;
8) modyfikacji podlegają jedynie zlecenia, które się nie zakończyły; modyfikować można czas zakończenia monitorowania, a po rozpoczęciu monitorowania czas startu nie może być już modyfikowany;
9) elementy informacyjne protokołu są podzielone na dwie grupy:
   a) Request – elementy informacyjne definiujące żądania wysyłane przez LEMF,
   b) Respond – elementy informacyjne stanowiące odpowiedzi ADMF na otrzymane żądania LEMF;

10) między LEMF a ADMF są dopuszczalne następujące interakcje między:

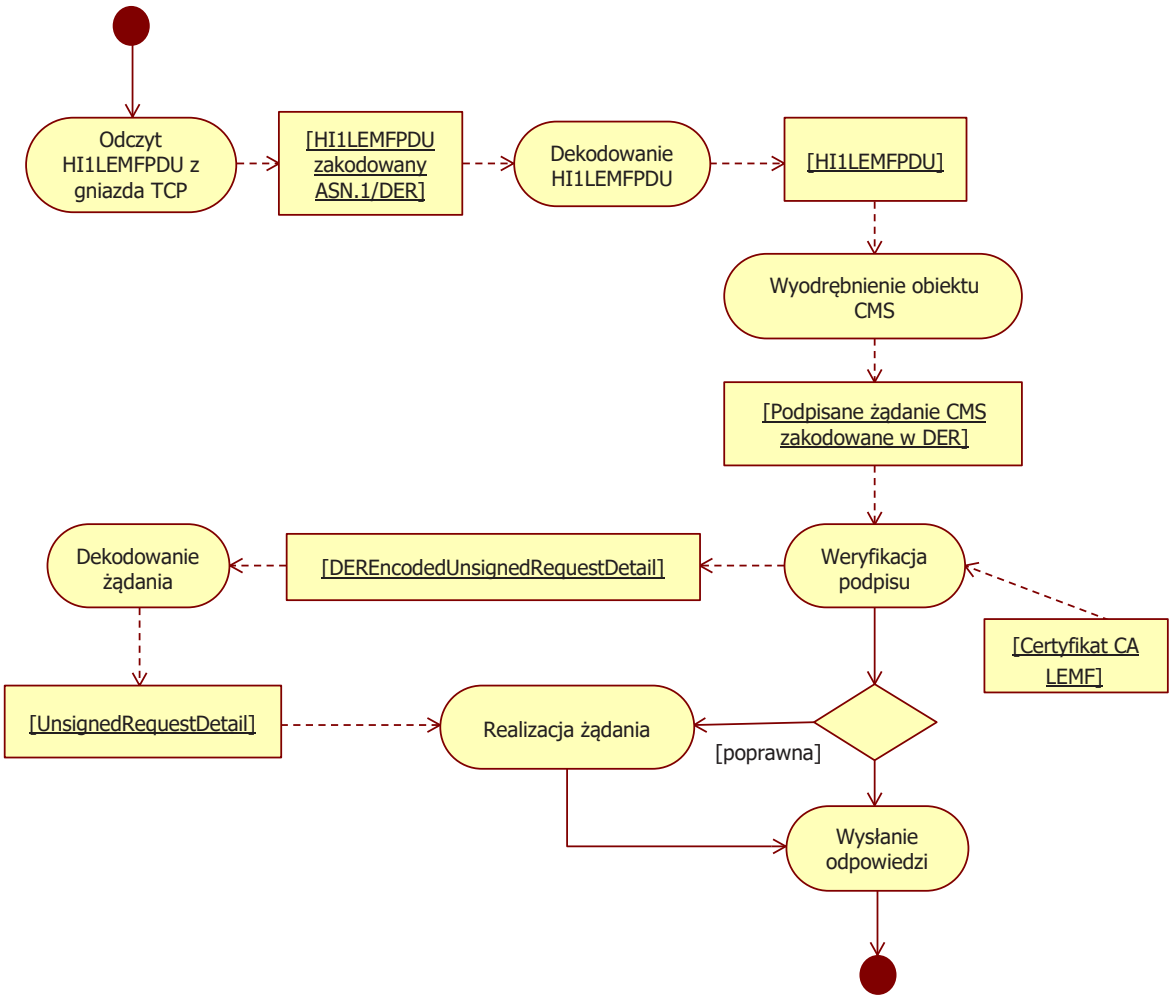
Tabela nr 4

Zapytanie LEMF	Odpowiedź ADMF	Alternatywna odpowiedź
SignedRequest	GeneralRespond	
HelloRequest	GeneralRespond	
ListRequest	ListRespond	GeneralRespond

11) żądania podpisane (SignedRequest) – sposób tworzenia i weryfikacji wiadomości podpisanych przedstawiono w formie diagramów aktywności na rysunkach 2 i 3.



Rysunek 2. Tworzenie żądania podpisanego



Rysunek 3. Weryfikacja żądania podpisanego

12) uwagi:

a) CMS – format binarny dokumentu z podpisem (z użyciem kodowania DER) stanowi podzbiór CMS; dokładna specyfikacja jest przedstawiona w IETF RFC 5652 [17],

b) identyfikator obiektu OID (Object Identifier) definiujący standard ma w notacji ASN.1 postać:

```
OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) modules(0) cms-
2004(24) }
```

c) struktura UnsignedRequestDetail, przedstawiona na rysunku 6, opisuje szczegóły żądania aktywacji, modyfikacji i dezaktywacji zlecenia; po zakodowaniu do postaci DER jest podpisywana zgodnie ze specyfikacją przedstawioną w IETF RFC 2315 [15],

d) monitorowaniu podlegają następujące usługi:

– CS (Mobile),

– PS (Packet Switched),

– InternetAccess,

– InternetTelephony,

– CS (Fixed).

10.2.3. Protokół HI1ADMFOperations:

1) żądania przesyłane przez ADMF:

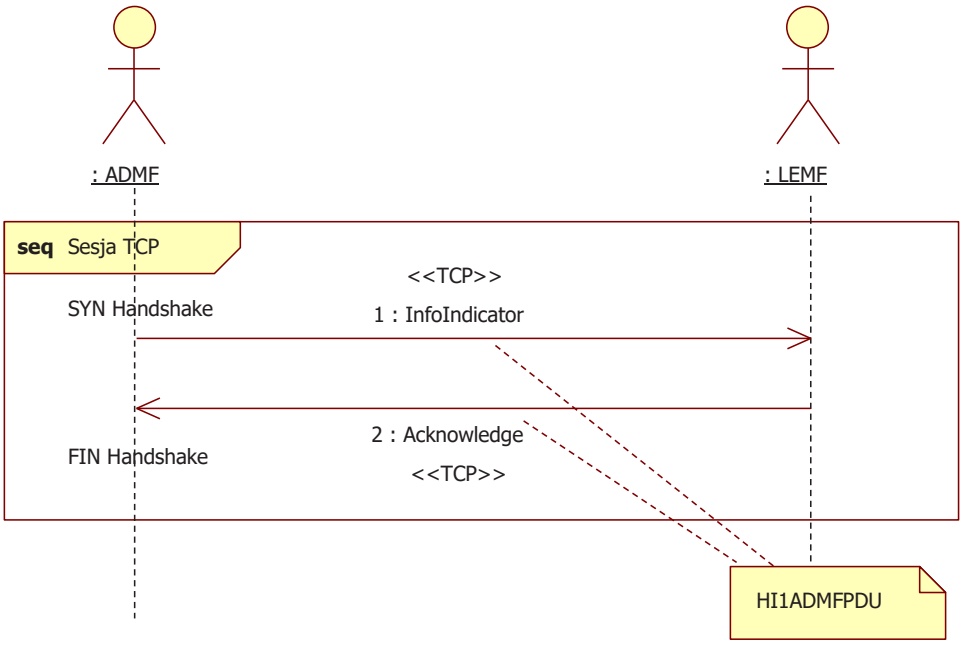
a) alarmy,

b) notyfikacje;

2) wiadomości są podzielone na dwie grupy, zgodnie ze schematem przedstawionym na rysunku 4:

a) InfoIndicator – elementy informacyjne definiujące alarmy i notyfikacje wysyłane przez ADMF,

b) Acknowledge – elementy informacyjne potwierdzające otrzymanie wiadomości przez ADMF;



Rysunek 4. Schemat obsługi żądań

3) między ADMF a LEMF są dopuszczalne następujące interakcje między:

Tabela nr 5

Wiadomość ADMF	Odpowiedź LEMF
HelloRequest	GeneralRespond
AlarmIndicator	GeneralRespond
NotificationIndicator	GeneralRespond

4) inne wymagania:

a) każde przesłane żądanie (InfoIndicator) jest potwierdzane przez LEMF (Acknowledge),

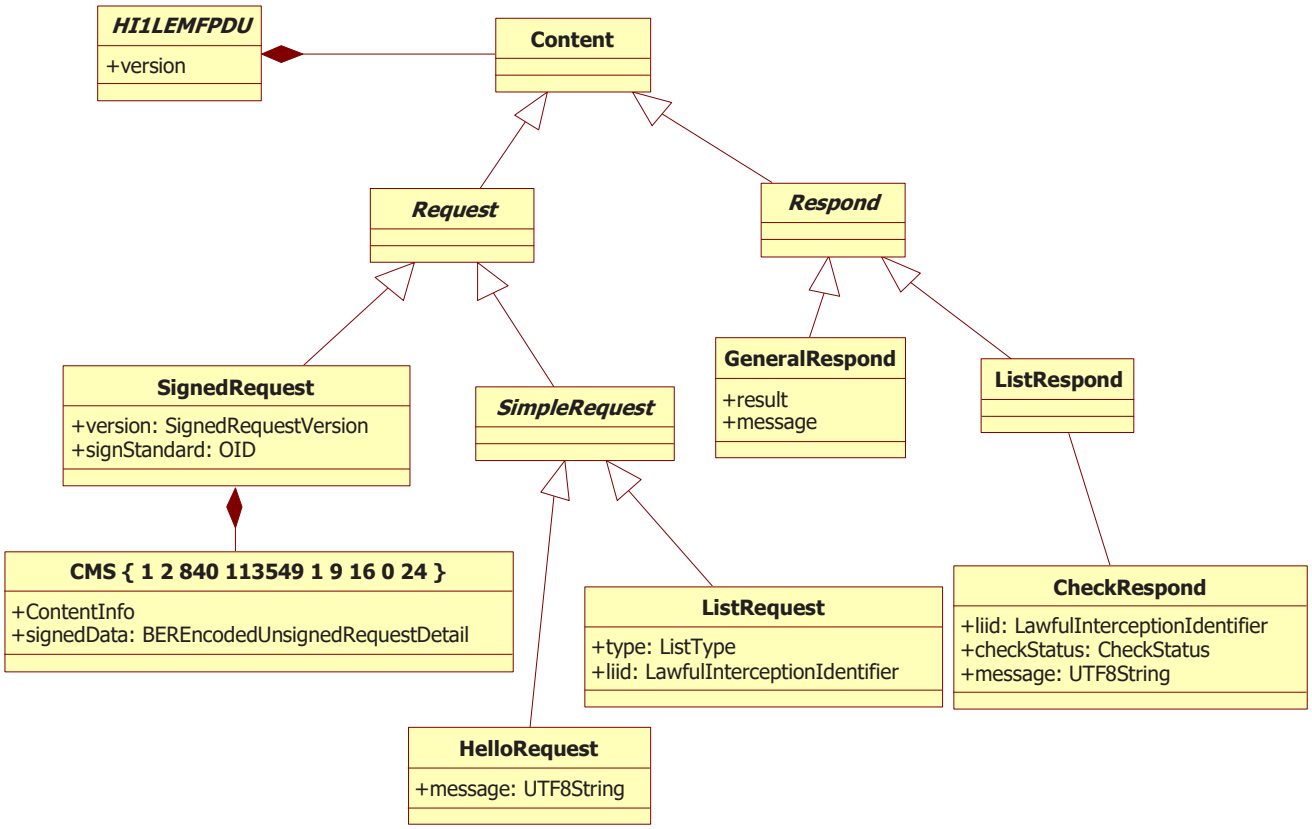
b) potwierdzenie jest realizowane w ciągu 5 sekund,

c) alarmy mają dwa stany: włączony i wyłączony (pole status),

d) żądanie wyłączające alarm może zawierać tylko jego identyfikator (identity).

10.3. Protokół HI1LEMFPDU

10.3.1. Struktura protokołu HI1LEMFPDU jest przedstawiona na rysunku 5.



Rysunek 5. Struktura protokołu HI1LEMFPDU

10.3.2. Specyfikacja ASN.1 dla protokołu HI1LEMFPDU

```
HI1LEMFOperations DEFINITIONS AUTOMATIC TAGS ::=
BEGIN
IMPORTS
  LawfulInterceptionIdentifier,
  TimeStamp
FROM
  UnsignedRequestDetail;

HI1LEMFPDU ::= SEQUENCE
{version [0] Version,
  content [1] Content,
  operator [2] UTF8String OPTIONAL,
  ...}

Version ::= ENUMERATED
{
  version1 (1),
  ...
}

Content ::= CHOICE
{
  request [1] Request,
  respond [2] Respond,
  ...
}

SignedRequest ::= SEQUENCE
{
  version [1] SignedRequestVersion,
  signStandard [2] OBJECT IDENTIFIER,
```

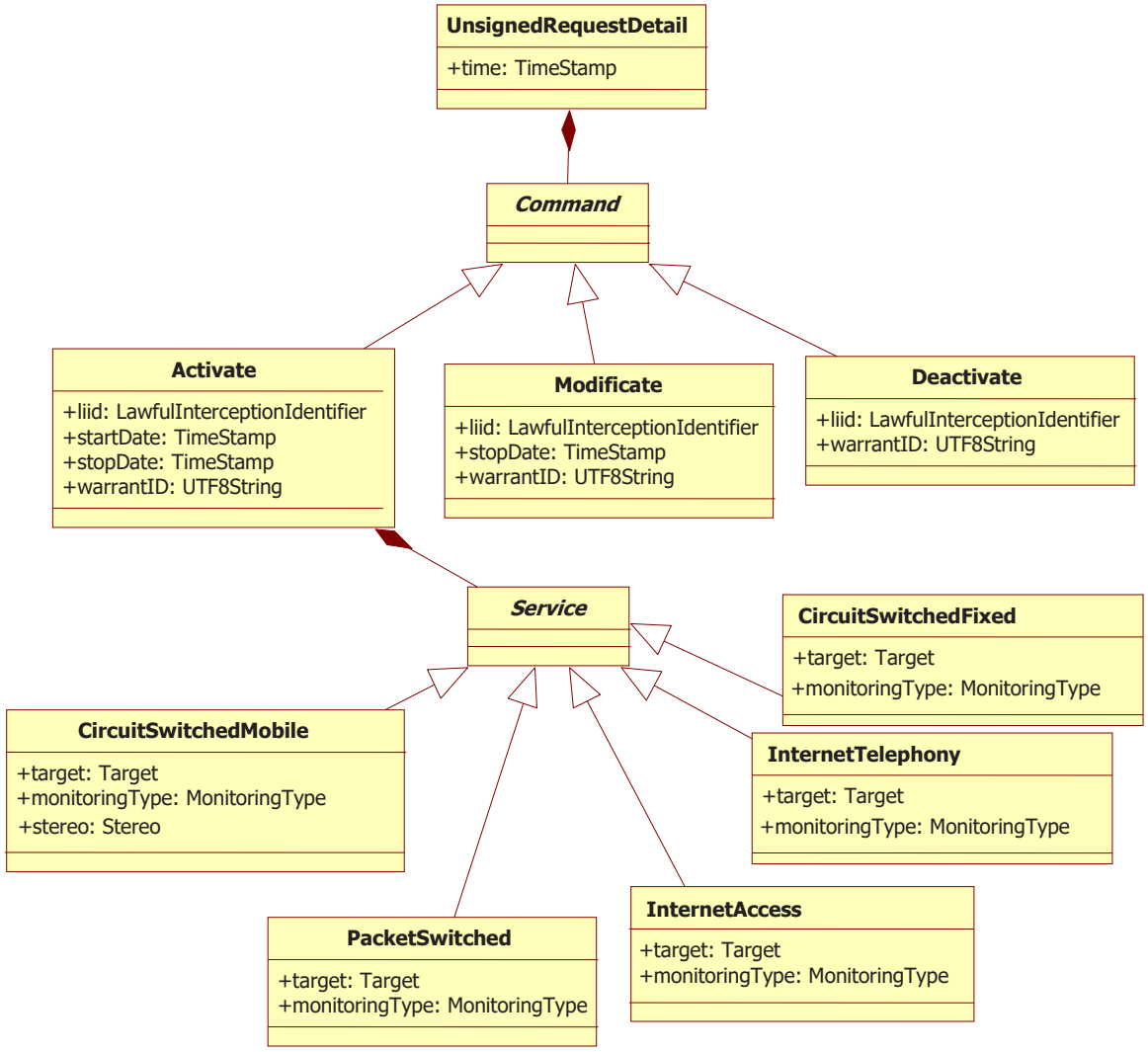
```
  -- CryptographicMessageSyntax2004 { iso(1) member-body(2)
us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) modules(0)
cms-2004(24)
  cmsDERSignedRequest  [3] OCTET STRING,
  -- cmsDERSignedRequest [3] ANY DEFINED BY signStandard
  ...
}

Request ::= CHOICE
{
  simpleRequest [1] SimpleRequest,
  signedRequest [2] SignedRequest,
  ...
}

SimpleRequest ::= CHOICE
{
  helloRequest [1] HelloRequest,
  listRequest [2] ListRequest,


SignedRequestVersion ::= ENUMERATED
{
  v1 (0),
  ...
}

HelloRequest ::= SEQUENCE
{
  message [1] UTF8String,
  ...
}

Respond ::= CHOICE
{
```

```
  generalRespond [1] GeneralRespond,
  listRespond [2] ListRespond,
  ...
}

GeneralRespond ::= SEQUENCE
{
  result [1] Result,
  message [2] UTF8String OPTIONAL,
  -- return Hello request message
  ...
}

Result ::= ENUMERATED
{
  ok (1),
  missing-parameter (2),
  unknown-parameter (3),
  unknown-parameter-value (4),
  incorrect-BER (5),
  badSignature (6),
  certificateExpired (7),
  unknownError (10),
  unsupportedService (11),
  ...
}

CheckRespond ::= SEQUENCE
{
  liid [1] LawfulInterceptionIdentifier,
  checkStatus [2] CheckStatus,
  message [3] UTF8String OPTIONAL,
  ...
}
```

```
CheckStatus ::= ENUMERATED
{
  notFound (0),
  waiting (1),  -- założone przez lemf, nie ma w cn (czeka na
zatwierdzenie lub )
  cnActivated (2), -- jest w cn
  unknown (3),
  deActivated (4), -- po dezaktywowaniu w cn
  ...
}

ListRequest ::= SEQUENCE
{
  type [1] ListType,
  liid [2] LawfulInterceptionIdentifier OPTIONAL,
  ...
}

ListRespond ::= SET OF CheckRespond

ListType ::= ENUMERATED
{
  all (1),
  specific (2),
  ...
}

END
```

10.4. UnsignedRequestDetail

10.4.1. Struktura UnsignedRequestDetail jest przedstawiona na rysunku 6.



Rysunek 6. Struktura UnsignedRequestDetail

10.4.2. Specyfikacja ASN.1 dla UnsignedRequestDetail

```
UnsignedRequestDetail DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

UnsignedRequestDetail ::= SEQUENCE
{
  time [1] TimeStamp,
  command [2] Command,
  operator [2] UTF8String OPTIONAL,
  ...
}
```

```
Command ::= CHOICE
{
  activate [1] Activate,
  deactivate [2] Deactivate,
  modificate [3] Modificate,
  ...
}

Activate ::= SEQUENCE
{
  lawfulInterceptionIdentifier [1]
LawfulInterceptionIdentifier,
  startTimestamp [2] TimeStamp,
  stopTimestap [3] TimeStamp,
  service [4] Service,
  warrantID [5] UTF8String,
  ...
}

Modificate ::= SEQUENCE
{
  lawfulInterceptionIdentifier [1]
LawfulInterceptionIdentifier,
  stopTimestap [3] TimeStamp,
  warrantID [5] UTF8String,
  ...
}

Deactivate ::= SEQUENCE
{
  lawfulInterceptionIdentifier [1]
LawfulInterceptionIdentifier,
  warrantID [5] UTF8String OPTIONAL,
  ...
}
```

```
Service ::= CHOICE
{
  circuitSwitchedMobile [1] CircuitSwitchedMobile,
  packetSwitched [2] PacketSwitched,
  wifi [3] WIFI, -- not used
  xdsl [4] XDSL, -- not used
  internetAccess [5] InternetAccess,
  internetTelephony [6] InternetTelephony,
  circuitSwitchedFixed [7] CircuitSwitchedFixed,
  generic [8] GenericService, - stosuje się jako podstawowy
sposób przekazywania identyfikatorów celu

  ...
}

GenericService ::= SEQUENCE
{
  identityType [1] UTF8String (SIZE(1..20)),
  identityValue [2] UTF8String,
  service [3] UFT8String OPTIONAL,
  ...
}

CircuitSwitchedMobile ::= SEQUENCE
{
  target [1] Target,
  monitoringType [2] MonitoringType,
  stereo [5] Stereo,
  ...
}

Stereo ::= ENUMERATED
{
  off (0),
```

```
  on (1)
}

PacketSwitched ::= SEQUENCE
{
  target [1] Target,
  monitoringType [2] MonitoringType,
  ...
}

WIFI ::= SEQUENCE
{
  target [1] Target,
  ...
}

XDSL ::= SEQUENCE
{
  target [1] Target,
  ...
}

InternetAccess::= SEQUENCE
{
  target [1] Target,
  monitoringType [2] MonitoringType,
  ...
}

InternetTelephony ::= SEQUENCE
{
  target [1] Target,
  monitoringType [2] MonitoringType,
  ...
}
```

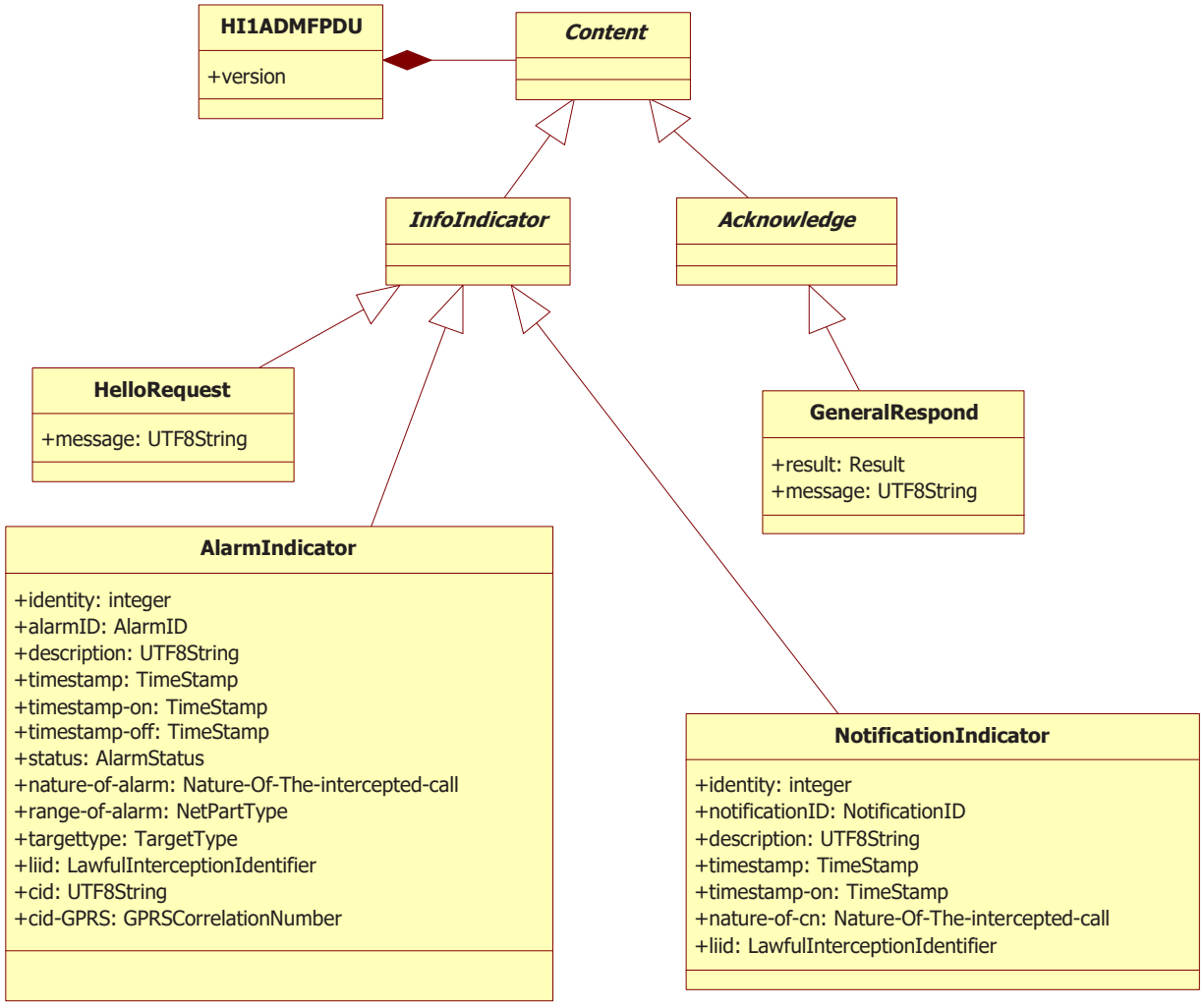
```
CircuitSwitchedFixed ::= SEQUENCE
{
  target [1] Target,
  monitoringType [2] MonitoringType,
  ...
}

Target ::= CHOICE
{
  mSISDN [1] MSISDN, -- wykorzystywany również jako numer
abonenta ISDN/PSTN lub telefonii internetowej(o ile jest to
numer zgodny z E.164)
  iMSI [2] IMSI,
  iMEI [3] IMEI,
  login [4] Login,
  iPAddress [5] IPAddress,
  mAC [6] MAC,
  eSN [7] ESN,
  ...
}

MSISDN ::= OCTET STRING (SIZE (1..9))
IMSI ::= OCTET STRING (SIZE (3..8))
IMEI ::= OCTET STRING (SIZE (8))
Login ::= OCTET STRING (SIZE (1..120))
IPAddress ::= OCTET STRING (SIZE (4))
MAC ::= OCTET STRING (SIZE (6))
ESN ::= OCTET STRING (SIZE (8))

SIPURL ::= UTF8String

MonitoringType ::= ENUMERATED
{
  iri (1),
```

```
  iriCC (2),
  ...
}

LawfulInterceptionIdentifier ::= OCTET STRING (SIZE (1..25))
-- It is recommended to use ASCII characters in " "0"…"9".
-- For subaddress option only "0"..."9" shall be used.
-- 17 znaków numerycznych ASCII
-- format: LEAID + TARGET(SEQ)
-- TARGET - (15 znaków) nadawany sekwencyjnie dla każdego
LEAID
-- LEAID -(2 znaki) 00 – LEMF operatora, 01 - ABW, 02 -
Policja, 03 - SKW, 04 - ZW, 05 - SG, 06 – KAS, 07 - CBA, 08-
SOP, 09 - BNW

TimeStamp ::= CHOICE
{
  -- The minimum resolution required is one second.
  -- "Resolution" is the smallest incremental change that can
be measured for time and
  -- is expressed with a definite number of decimal digits or
bits.
  localTime [0] LocalTimeStamp,
  utcTime [1] UTCTime
}

LocalTimeStamp ::= SEQUENCE
{
  generalizedTime [0] GeneralizedTime,
  -- The minimum resolution required is one second.
  -- "Resolution" is the smallest incremental change that can
be measured for time and
  -- is expressed with a definite number of decimal digits or
bits.

  winterSummerIndication [1] ENUMERATED
  {
```

```
    notProvided(0),
    winterTime(1),
    summerTime(2)
  }
}
END
```

10.5. Protokół HI1ADMFPDU

10.5.1. Struktura protokołu HI1ADMFPDU jest przedstawiona na rysunku 7.



Rysunek 7. Struktura protokołu HI1ADMFPDU

10.5.2. Specyfikacja ASN.1 dla protokołu HI1ADMFPDU

```
HI1ADMFOperations DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

IMPORTS
  LawfulInterceptionIdentifier,
  TimeStamp
FROM
UnsignedRequestDetail;
HI1ADMFPDU ::= SEQUENCE
{
  version [0] Version,
  content [1] Content
  operator [2] UTF8String OPTIONAL,
}

Version ::= ENUMERATED
{
  version1 (1),
  ...
}

Content ::= CHOICE
{
  info [0] InfoIndicator,
  acknowledge [1] Acknowledge,
  ...
}

InfoIndicator ::= CHOICE
{
  helloRequest [1] HelloRequest,
  alarm[2] AlarmIndicator,
  notification [3] NotificationIndicator,
```

```
  ...
}


HelloRequest ::= SEQUENCE
{
  message [1] UTF8String,
  ...
}


AlarmIndicator ::= SEQUENCE
{
  identity [0] INTEGER, -- numer pozwalający na jednoznaczną
identyfikację alarmu razem z timestamp-on
  alarmID [1] AlarmID,
  description [2] UTF8String OPTIONAL,       -- dodatkowe
informacje, opis, kod błędu (np. z alarmu z MSC), tzw. powód
  timestamp [3] TimeStamp,           -- czas wysłania alarmu
  timestamp-on [4] TimeStamp OPTIONAL,      -- czas
wystąpienia alarmowanego zdarzenia
  timestamp-off [5] TimeStamp OPTIONAL,     -- czas
wystąpienia zdarzenia odwrotnego do zdarzenia alarmowanego
  status [6] AlarmStatus OPTIONAL,    -- powstanie/ustanie
alarmu
  -- podobne nature-Of-The-intercepted-call z HI2 (jeżeli błąd
globalny to wszystkie service)
  nature-of-alarm  [7] Nature-Of-The-intercepted-call
OPTIONAL,
  range-of-alarm [8] NetPartType OPTIONAL,   -- dotyczy całej
sieci CN czy tylko jej części (np.: tylko jeden GGSN, jedna
centrala)
  targettype [9] TargetType OPTIONAL,     -- dotyczy
konkretnego LIID lub konkretnej sesji albo wszystkich
obserwacji
  liid [10] LawfulInterceptionIdentifier OPTIONAL,
  cid [11] UTF8String OPTIONAL,         -- z HI2 (chodzi o
wskazanie konkretnej rozmowy lub sesji)
  cid-GPRS [12] GPRSCorrelationNumber OPTIONAL,-- z HI2
(chodzi o wskazanie konkretnej rozmowy lub sesji)
  ...
```

```
}


Nature-Of-The-intercepted-call ::= ENUMERATED
{
  -- Nature of the intercepted "call":
  gSM-ISDN-PSTN-circuit-call(0),
  -- the possible UUS content is sent through the HI2 or HI3
"data" interface
  -- the possible call content call is established through the
HI3 "circuit" interface
  gSM-SMS-Message(1),
  -- the SMS content is sent through the HI2 or HI3 "data"
interface
  uUS4-Messages(2),
  -- the UUS content is sent through the HI2 or HI3 "data"
interface
  tETRA-circuit-call(3),
  -- the possible call content call is established through the
HI3 "circuit" interface
  -- the possible data are sent through the HI3 "data"
interface
  teTRA-Packet-Data(4),
  -- the data are sent through the HI3 "data" interface
  gPRS-Packet-Data(5),
  -- the data are sent through the HI3 "data" interface
  uMTS-circuit-call(6),
  -- the possible call content call is established through the
HI3 "circuit" interface
  -- the possible data are sent through the HI3 "data"
interface
  wIFI (11), -- not used
  xDSL (12), -- not used
  internetAccess (13),
  internetTelephony (14),
    ...
}
```

```
NotificationIndicator ::= SEQUENCE
{
  identity [0] INTEGER,     -- numer pozwalający na
jednoznaczną identyfikację alarmu razem z timestamp-on
  notificationID [1] NotificationID,
  description [2] UTF8String OPTIONAL,  -- dodatkowe
informacje, opis, kod błędu (np. z MSC), tzw. powód
  timestamp [3] TimeStamp,     -- czas wysłania powiadomienia
  timestampEvent [4] TimeStamp,    -- czas wystąpienia
zdarzenia, którego dotyczy powiadomienie
  liid [5] LawfulInterceptionIdentifier OPTIONAL,
  ...
}


AlarmID ::= ENUMERATED
{
  sm-buffer-overflow (0),     -- bufory wyjściowe w kierunku
LEMF przepełnione => IRI i/lub CC tracone (operator)
  lemf-hi3-online-delivery-failure (1),  -- problem z
monitoringiem online (LEMF)
  lemf-hi3-delivery-failure (2),  -- problem z zapisywaniem
danych HI3 (LEMF)
  lemf-hi2-delivery-failure (3),  -- problem z zapisywaniem
danych HI2 (LEMF)
  lemf-hi1-delivery-failure (4),  -- problem z monitoringiem
online (LEMF)
  sm-hi1-failure (5),   -- brak lub przeciążenie komunikacji z
CN na interfejsie HI1 (SM operatora)
  sm-hi2-failure (6),   -- brak lub przeciążenie komunikacji z
CN na interfejsie HI2 (SM operatora)
  sm-hi3-failure (7),   -- brak lub przeciążenie komunikacji z
CN na interfejsie HI3 (SM operatora)
  sm-hi3-online-failure (8), -- brak lub przeciążenie
komunikacji z CN na interfejsie HI3 (SM operatora)
  major-system-failure (9), -- poważne uszkodzenie SM =>
konieczne sprawdzenie spójności BD (SM operatora)
  -- zarządzanie obserwacjami prawidłowe, ale inne funkcje SM
mogą nie działać (np. część obserwacji stracona) (SM
operatora)
```

```
  minor-system-failure (10),
  cn-activation-error (11), -- obserwacja niezałożona w CN a
czas na nią (LIID obowiązkowy) (SM operatora)
  cn-deactivation-error (12),  -- obserwacja nieusunięta z CN a
czas na nią (LIID obowiązkowy) (SM operatora)
  major-cn-li-failure (13), -- po stronie CN LI całkowicie nie
funkcjonowało, BD obserwacji odbudowane w CN (SM operatora)
  minor-cn-li-failure (14), -- po stronie CN pewne funkcje LI
nie działały (SM operatora)
  manual-system-failure (15),  -- informacja wprowadzana
ręcznie: uszkodzenie w CN lub SM (SM operatora)
  manual-system-maintenance (20),-- informacja wprowadzana
ręcznie o pracach planowych w systemie SM operatora (SM
operatora)
  ...
}

AlarmStatus ::= ENUMERATED
{
  off (0),
  on (1),
  ...
}

NetPartType ::= ENUMERATED
{
  whole (1),
  part (2),
  ...
}

TargetType ::= ENUMERATED
{
  all (1),
  specific (2),
  ...
}
```

```
NotificationID ::= ENUMERATED
{
  target-activated (0),
  target-deactivated (1),
  target-modificated (2),
  ...
}

Acknowledge ::= CHOICE
{
  respond [0] GeneralRespond,
  ...
}

GeneralRespond ::= SEQUENCE
{
  result [1] Result,
  message [2] UTF8String OPTIONAL,
  ...
}

Result ::= ENUMERATED
{
  ok (1),
  missing-parameter (2),
  unknown-parameter (3),
  unknown-parameter-value (4),
  incorrect-BER (5),
  badSignature (6),
  certificateExpired (7),
  unknownError (10),
  ...
}

GPRSCorrelationNumber ::= OCTET STRING (SIZE(8..20))

END
```

11. Format parametru ExtendedPartyIdentity

```
PartyInformation ::= SEQUENCE
{
  ...
  partyExtendedIdentity [PRIVATE 1] PartyExtendedIdentity
OPTIONAL,
  ...
}

PartyExtendedIdentity ::= SEQUENCE
{
  subscriptionType [1] ENUMERATED
  {
    postpaid (0),
    prepaid  (1),
    ...
  } OPTIONAL,

  activationDate [2] TimeStamp OPTIONAL,
  deactivationDate [3] TimeStamp OPTIONAL,
  subscriber [4] Subscriber OPTIONAL,
  postalAddress [5] PostalAddress OPTIONAL,
  mailAddress [6] MailAddress OPTIONAL,
  ...
}

Subscriber ::= CHOICE
{
  company [1] Company,
  person [2] Person,
  ...
}
```

```
Company ::= SEQUENCE
{
  name [0] UTF8String,
  regon [1] OCTET STRING (SIZE (5)) OPTIONAL,
  -- BCD coded 9 digits
  -- F digit not used
  ...
}

Person ::= SEQUENCE
{
  firstName [0] UTF8String,
  surname [1] UTF8String,
  pesel  [2] OCTET STRING (SIZE (6)) OPTIONAL,
  -- BCD coded 11 digits
  -- F digit not used
  passportNumber [3] OCTET STRING (SIZE (7..14)) OPTIONAL,
  -- ASCII coded
  ...
}

PostalAddress ::= SEQUENCE
{
  street [1] UTF8String OPTIONAL,
  buildingNumber [2] OCTET STRING (SIZE (1..10)) OPTIONAL,
  -- ASCII coded: 10 char
  apartmentNumber [3] OCTET STRING (SIZE (1..10))
OPTIONAL,
  -- ASCII coded: 10 char
  postcode [4] OCTET STRING (SIZE (1..8)) OPTIONAL,
  city [5] UTF8String OPTIONAL,
  country [6] UTF8String OPTIONAL
}
```

Załącznik nr 2

WYMAGANIA TECHNICZNE I EKSPLOATACYJNE DLA INTERFEJSÓW

I. Dokumenty powołane

1. Wykaz dokumentów powołanych:

1.1. ETSI ES 201 671 V3.1.1 Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic, zwany dalej „ETSI ES 201 671”.

1.2. ETSI TS 102 232-1 V2.5.1 Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 1: Handover specification for IP delivery, zwany dalej „ETSI TS 102 232-1”.

1.3. ETSI TS 102 232-3 V2.2.1 Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 3: Service-specific details for internet access services, zwany dalej „ETSI TS 102 232-3”.

1.4. ETSI TS 102 232-5 V2.5.1 Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 5: Service-specific details for IP Multimedia Services, zwany dalej „ETSI TS 102 232-5”.

1.5. ETSI TS 102 232-6 V2.3.1 Lawful Interception (LI);Handover Interface and Service-Specific Details (SSD) for IP delivery;Part 6: Service-specific details for PSTN/ISDN services, zwany dalej „ETSI TS 102 232-6”.

1.6. ETSI ETS 300 927 Digital cellular telecommunications system (Phase 2+) (GSM); Numbering, addressing and identification (GSM 03.03 version 5.2.1 Release 1996), zwany dalej „ETSI ETS 300 927”.

1.7. ETSI TS 102 280 V1.1.1 X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons (2004-03), zwany dalej „ETSI TS 102 280”.

1.8. 802.3ab-1999 IEEE Standard for Information Technology – Telecommunications and information exchange between systems – Local and Metropolitan Area Networks – Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications – Physical Layer Parameters and Specifications for 1000 Mb/s Operation over 4 pair of Category 5 Balanced Copper Cabling, Type 1000BASE-T, zwany dalej „IEEE 802.3ab”.

1.9. IETF RFC 0791 Internet Protocol, zwany dalej „IETF RFC 0791”.

1.10. IETF RFC 0793 Transmission Control Protocol, zwany dalej „IETF RFC 0793”.

1.11. IETF RFC 0959 File Transfer Protocol, zwany dalej „IETF RFC 0959”.

1.12. IETF RFC 2315 Cryptographic Message Syntax, Version 1.5, zwany dalej „IETF RFC 2315”.

1.13. IETF RFC 2460 Internet Protocol, Version 6 (IPv6) Specification, zwany dalej „IETF RFC 2460”.

1.14. IETF RFC 3852 Cryptographic Message Syntax (CMS), zwany dalej „IETF RFC 3852”.

1.15. IETF RFC 3261 SIP: Session Initiation Protocol, zwany dalej „IETF RFC 3261”.

1.16. IETF RFC 4291 Internet Protocol, Version 6 (IPv6) Addressing Architecture, zwany dalej „IETF RFC 4291”.

1.17. ITU-T X.680 Abstract Syntax Notation One (ASN.1): Specification of basic notation, zwany dalej „ITU-T X.680”.

1.18. ITU-T X.681 Abstract Syntax Notation One (ASN.1): Information object specification, zwany dalej „ITU-T X.681”.

1.19. ITU-T X.682 Abstract Syntax Notation One (ASN.1): Constraint specification, zwany dalej „ITU-T X.682”.

1.20. ITU-T X.683 Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specifications, zwany dalej „ITU-T X.683”.

1.21. ITU-T X.690 ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER), zwany dalej „ITU-T X.690”.

2. Dokumenty, o których mowa w pkt 1.1–1.7, są dostępne na stronie Europejskiego Instytutu Norm Telekomunikacyjnych (ETSI): www.etsi.org.

3. Dokument, o którym mowa w pkt 1.8, jest dostępny na stronie Instytutu Inżynierów Elektryków i Elektroników (IEEE): www.ieee.org.

4. Dokumenty, o których mowa w pkt 1.9–1.16, są dostępne na stronie zespołu inżynierów ustanawiających standardy techniczne i organizacyjne w Internecie, Internet Engineering Task Force (IETF): www.ietf.org.

5. Dokumenty, o których mowa w pkt 1.17–1.21, są dostępne na stronie Międzynarodowego Związku Telekomunikacyjnego (ITU): www.itu.int.

II. Stosowane skróty

1. ADMF – system przedsiębiorcy telekomunikacyjnego umożliwiający realizację dostępu do wybranych treści przekazów telekomunikacyjnych (Administration Function).

2. ASCII – kod przyporządkowujący liczby z zakresu od 0 do 127 literom alfabetu angielskiego, cyfrom, znakom przestankowym i innym symbolom oraz poleceniom sterującym (American Standard Code for Information Interchange).

3. ASN.1 – znormalizowany zapis składni stosowany do opisu struktur danych przenoszonych przez wiadomości wymieniane między komunikującymi się elementami systemu (Abstract Syntax Notation One), zdefiniowany w ITU-T X.680, ITU-T X.681, ITU-T X.682 i ITU-T X.683.

4. BER – sposób kodowania informacji zapisanej przy użyciu ASN.1 do postaci transmitowanej w sieciach telekomunikacyjnych (Basic Encoding Rules), zgodny z ITU-T X.690.

5. CA – urząd certyfikacji (Certificate Authority).

6. CC – treść przekazu telekomunikacyjnego (Content of Communication).

7. CDMA – wielodostęp z podziałem kodowym (Code Division Multiple Access).

8. CMS – standard zabezpieczania wiadomości (Cryptographic Message Syntax), zdefiniowany w IETF RFC 3852.

9. CS – komutacja kanałów (Circuit Switched).

10. CSD – transmisja danych z wykorzystaniem komutacji łączy (Circuit Switched Data).

11. DER – sposób kodowania informacji (Distinguished Encoding Rules), zgodny z ITU-T X.690.

12. DF – funkcja dostarczająca dane do LEMF (Delivery Function).

13. ESN – indywidualny numer identyfikujący telekomunikacyjne urządzenie końcowe używane w ruchomej publicznej sieci telefonicznej wykorzystującej technologię CDMA (Electronic Serial Number).

14. FTP – protokół transferu plików (File Transfer Protocol), zdefiniowany w IETF RFC 0959.

15. GLIC – mechanizm przekazywania treści monitorowanej komunikacji do LEMF, dotyczący monitorowania transmisji danych pakietowych w sieciach ruchomych (GPRS LI Correlation).

16. IMEI – indywidualny międzynarodowy numer identyfikujący telekomunikacyjne urządzenie końcowe używane w ruchomej publicznej sieci telefonicznej (International Mobile Equipment Identity).

17. IMSI – międzynarodowy numer przydzielony karcie identyfikującej użytkownika w ruchomej publicznej sieci telefonicznej (International Mobile Subscriber Identity).

18. IRI – informacje związane z przekazem telekomunikacyjnym (Intercept Related Information).

19. ISDN – sieć cyfrowa z integracją usług (Integrated Services Digital Network).

20. LEA – podmiot uprawniony do monitorowania (Law Enforcement Agency).

21. LEMF – system monitorowania LEA umożliwiający dostęp do wybranych treści przekazów telekomunikacyjnych (Law Enforcement Monitoring Facility).

22. LIID – identyfikator obiektu monitorowanego (Lawful Interception Identifier).

23. LOGIN – nazwa użytkownika logującego się do sieci, używana w procesie jego uwierzytelnienia.

24. MAC – sprzętowy adres karty sieciowej (Media Access Control).

25. MEID – unikalny numer identyfikujący telekomunikacyjne urządzenie końcowe używane w ruchomej publicznej sieci telefonicznej wykorzystującej technologię CDMA, zastępujący ESN (Mobile Equipment Identifier).
26. MF – funkcja pośrednicząca dostosowująca dane będące przedmiotem monitorowania, pochodzące z sieci przedsiębiorcy telekomunikacyjnego, do formatu wymaganego przez interfejs (Mediation Function).
27. MSISDN – numer przydzielony użytkownikowi końcowemu ruchomej publicznej sieci telefonicznej z integracją usług (Mobile Subscriber Integrated Services Digital Network).
28. PKI – Infrastruktura Klucza Publicznego będąca systemem kryptograficznym, w którego skład wchodzą urzędy certyfikacyjne, użytkownicy certyfikatów (subskrybenci) oraz oprogramowanie i sprzęt (Public Key Infrastructure).
29. PSTN – publiczna komutowana sieć telefoniczna (Public Switched Telephone Network).
30. SIP – protokół sygnalizacyjny warstwy aplikacyjnej wykorzystywany do inicjowania, zarządzania oraz zakańczania sesji (połączenia telefonii internetowej, konferencji multimedialnej) (Session Initiation Protocol), zdefiniowany w IETF RFC 3261.
31. SMS – krótka wiadomość tekstowa (Short Message Service).
32. TCP – protokół komunikacji w sieci komputerowej (Transmission Control Protocol), zdefiniowany w IETF RFC 0793.
33. VoIP – telefonia internetowa (Voice over IP).
34. WAN – rozległa sieć komputerowa (Wide Area Network).

III. Określenia użyte w załączniku

1. Interfejs LI HI (Lawful Interception Handover Interface) – elektroniczny, zdalny i oparty na protokole komunikacyjnym IP interfejs między ADMF a LEMF, umożliwiający realizację dostępu do wybranych treści przekazów telekomunikacyjnych, w którego skład wchodzą:
   1) interfejs HI1 – styk umożliwiający dwukierunkową wymianę wiadomości między LEMF a ADMF, wykorzystywany przez LEMF do przesyłania żądań, a przez ADMF – głównie do przesyłania notyfikacji zdarzeń lub stanu realizacji żądań, realizujący także inne funkcje, opisane w pkt V;
   2) interfejs HI2 – styk umożliwiający jednokierunkowe, w kierunku od ADMF do LEMF, przesyłanie informacji związanych z objętymi monitorowaniem przekazami telekomunikacyjnymi oraz treści SMS;
   3) interfejs HI3 – styk umożliwiający jednokierunkowe, w kierunku od ADMF do LEMF, przesyłanie treści monitorowanych.
2. Obiekt monitorowany – obiekt wskazany w postanowieniu sądu wydanym na podstawie wniosku albo zarządzenia organu uprawnionego podmiotu wydanego na podstawie odrębnych przepisów.

3. Bufor – zespół urządzeń przedsiębiorcy telekomunikacyjnego odpowiedzialnych za magazynowanie danych do czasu ich przekazania do LEMF.

4. Monitorowanie – dostęp do przekazów telekomunikacyjnych i związanych z nimi danych, o których mowa w art. 43 ust. 1 pkt 1 lit. a ustawy z dnia 12 lipca 2024 r. – Prawo komunikacji elektronicznej (Dz. U. poz. 1221, z 2025 r. poz. 637 i 820 oraz z 2026 r. poz. 252, 815 i 1296), zwanej dalej „ustawą”.

5. Przekaz telekomunikacyjny – komunikat elektroniczny, o którym mowa w art. 2 pkt 19 ustawy.

IV. Interfejs LI HI

1. Wymagania ogólne

1.1. W warstwie fizycznej jest stosowany interfejs standardu Ethernet 100/1000BASE-T, zgodny z IEEE 802.3ab. Do obsługi każdego z LEA jest przewidziany oddzielny port w standardzie Ethernet.

1.2. Protokołem warstwy sieciowej interfejsu LI HI jest protokół IPv4, zgodny z IETF RFC 0791, lub IPv6, zgodny z IETF RFC 2460 i IETF RFC 4291. Stosuje się publiczne adresy IP.

1.3. Sieć między ADMF a LEMF jest siecią wydzieloną (w ramach WAN), za którą odpowiada LEA. Wyboru protokołu, o którym mowa w pkt 1.2, dostosowania przesyłanych informacji oraz szyfrowania sygnału na łączach WAN dokonuje LEA.

1.4. Szyfrowanie transmisji realizuje się poza interfejsem LI HI na poziomie warstwy łącza danych lub warstwy sieciowej.

1.5. W celu identyfikacji obiektów monitorowanych wykorzystuje się niepowtarzalny dla każdego obiektu monitorowanego LIID.

1.6. Dla każdej usługi w ramach danego kryterium wyboru, o którym mowa w pkt 2.4, jest przydzielany odrębny LIID. W przypadku monitorowania więcej niż jednej usługi w ramach tego samego kryterium wyboru dla każdej kolejnej usługi nadaje się unikalny LIID.

1.7. LEMF w wiadomościach interfejsu LI HI używa poniżej zdefiniowanego formatu LIID. LIID składa się z dwóch członów: LEAID (LEA Identifier) + SEQ (kolejny niepowtarzalny numer wiadomości). LIID jest utworzony z 17 znaków numerycznych ASCII od 0 do 9, w tym 2 cyfr określających LEAID oraz 15 cyfr wskazujących numer SEQ, zgodnie z tabelą nr 1. Wartość LEAID jest przydzielona każdemu LEA zgodnie z tabelą nr 2.

Tabela nr 1

LIID
LEAID + SEQ
2 cyfry + 15 cyfr
Np. 01000300056043015

Tabela nr 2

LEAID		
Wartość	LEA	Opis
00	LEMF operatora	Przedsiębiorca telekomunikacyjny
01	ABW	Agencja Bezpieczeństwa Wewnętrznego
02	POLICJA	Policja
03	SKW	Służba Kontrwywiadu Wojskowego
04	ZW	Żandarmeria Wojskowa
05	SG	Straż Graniczna
06	MF	Ministerstwo Finansów
07	CBA	Centralne Biuro Antykorupcyjne
08	SOP	Służba Ochrony Państwa
09	BNW	Biuro Nadzoru Wewnętrznego

1.8. Dopuszcza się wykorzystanie jednego portu do obsługi więcej niż jednego LEA. Wykorzystanie takiego rozwiązania ustala się na etapie uzgadniania zasad współpracy przez interfejs między przedsiębiorcą telekomunikacyjnym a zainteresowanymi LEA.

2. Wymagania dla interfejsu HI1

2.1. Interfejs HI1 zapewnia:

1) przekazywanie do ADMF zleceń w zakresie włączania, modyfikacji i wyłączania monitorowania obiektów monitorowanych oraz zapytań o status obserwacji;
2) przekazywanie od ADMF do LEMF informacji o statusie realizacji zleceń i zapytań oraz informacji o występowaniu awarii;
3) możliwość realizacji podstawowych testów diagnostycznych tego interfejsu;
4) w pełni automatyczną realizację zleceń przekazywanych od LEMF, bez udziału pracowników przedsiębiorcy telekomunikacyjnego.

2.2. W celu aktywacji każdego zlecenia monitorowania LEA określa:

1) LIID;
2) obiekt monitorowany;
3) monitorowaną usługę telekomunikacyjną;
4) zakres monitorowania;
5) okres monitorowania.

2.3. Interfejs HI1 zapewnia następujące kryteria wyboru obiektu monitorowanego w sieciach telekomunikacyjnych, stosownie do rodzaju sieci:

1) numer abonenta PSTN/ISDN/MSISDN/VoIP;
2) IMSI;
3) IMEI o długości 15 cyfr, zgodny z ETSI ETS 300 927;
4) LOGIN;
5) adres IP;

6) MAC;

7) ESN albo MEID.

2.4. Interfejs HI1 zapewnia następujące kryteria wyboru monitorowanych usług telekomunikacyjnych, stosownie do rodzaju sieci:

1) z komutacją kanałów, w tym połączenia głosowe, połączenia wideo, przesyłanie faksów, SMS, CSD;

2) z transmisją pakietową w ruchomych publicznych sieciach telefonicznych, zwanych dalej „sieciami ruchomymi”;

3) z dostępem do sieci internet;

4) VoIP.

2.5. Przez zakres monitorowania LEA wskazuje jeden z dwóch zakresów odnoszących się do danych:

1) IRI oraz opcjonalnie treści SMS;

2) IRI + CC.

2.6. Wysyłanie zleceń aktywacji następuje w chwili rzeczywistego uruchamiania monitoringu albo z wyprzedzeniem. Maksymalne wyprzedzenie ustala się na etapie uzgadniania zasad współpracy przez interfejs. W zleceniu aktywacji określa się czas zakończenia monitorowania.

2.7. Zlecenie modyfikacji monitorowania obejmuje:

1) czas wyłączenia monitorowania;

2) włączenie/wyłączenie trybu online w odniesieniu do usług sieci ruchomych.

2.8. ADMF przesyła do LEMF informację o czasie faktycznego wykonania polecenia aktywacji, dezaktywacji albo modyfikacji monitorowania. W przypadku błędu w trakcie wykonywania polecenia przesyła informację o fakcie pojawienia się błędu lub braku możliwości wykonania polecenia.

2.9. Przedsiębiorca telekomunikacyjny przesyła do każdego z LEA informacje o objętych awarią LIID, które znajdują się w dyspozycji tego przedsiębiorcy.

2.10. Po usunięciu awarii, o której mowa w pkt 2.9, przedsiębiorca telekomunikacyjny niezwłocznie przesyła do LEA informacje o czasie trwania przerwy w monitorowaniu.

2.11. ADMF w odpowiedzi na pytanie o status obserwacji nie przesyła żadnych danych identyfikujących obiekt monitorowany poza LIID.

2.12. Zlecenia wystawiane przez użytkownika LEMF, z wyjątkiem włączenia/wyłączenia trybu online oraz weryfikacji stanu obserwacji, są podpisywane elektronicznie.

2.13. Formatem stosowanego podpisu elektronicznego żądań HI1 jest CMS. Na potrzeby stosowania podpisu elektronicznego są wykorzystywane certyfikaty określone w ETSI TS 102 280, z uwzględnieniem wymagań technicznych dla certyfikatów, o których mowa w ustawie z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. z 2024 r. poz. 1725 oraz z 2026 r. poz. 252), oraz PKI.

2.14. Szczegółowa struktura elementów interfejsu HI1 jest przedstawiona w pkt V.

2.15. Za zgodą LEA dopuszcza się pracę interfejsu HI1 w trybie półautomatycznym, w którym pracownik przedsiębiorcy telekomunikacyjnego, spełniający wymagania określone w art. 43 ust. 9 ustawy, po odebraniu zlecenia od LEMF wykonuje prace niezbędne do przygotowania sieci przedsiębiorcy telekomunikacyjnego do realizacji zlecenia. Czas na przeprowadzenie tych prac nie przekracza 24 godzin.

3. Wymagania dla interfejsu HI2

3.1. Informacje związane z objętymi monitorowaniem przekazami telekomunikacyjnymi są przekazywane do LEMF niezwłocznie, jednak niepóźniej niż 10 minut od zakończenia przekazu. Raporty dotyczące zdarzeń występujących w danej sesji powinny być wysyłane w kolejności wystąpienia tych zdarzeń.

3.2. Przesyłanie do LEMF informacji związanych z objętymi monitorowaniem przekazami telekomunikacyjnymi odbywa się z wykorzystaniem FTP, zdefiniowanego w IETF RFC 0959, na zasadach określonych w ETSI ES 201 671.

3.3. Sesje FTP są nawiązywane tylko w kierunku od ADMF do LEMF w trybie pasywnym.

3.4. Do nazewnictwa plików wykorzystuje się metodę A zdefiniowaną w ETSI ES 201 671 (Annex C, pkt C.2.2). Zgodnie z tą metodą nazwa pliku ma postać: <LIID>_<seq>.<ext>.

3.5. Nazwa przesyłanego pliku jest zmieniana na docelową po udanym nagraniu. Plik tymczasowy ma dodatkowe rozszerzenie .tmp (<LIID>_<seq>.<ext>.tmp).

3.6. Zawartość plików (dane IRI) jest kodowana w formacie ASN.1/BER, zgodnie z:

1) ETSI ES 201 671 w odniesieniu do usług świadczonych w sieciach ruchomych oraz usług transmisji pakietowej świadczonych w sieciach ruchomych;
2) ETSI TS 102 232-1 i ETSI TS 102 232-6 w odniesieniu do usług świadczonych w stacjonarnej publicznej sieci telefonicznej, zwanej dalej „siecią stacjonarną”;
3) ETSI TS 102 232-1 i ETSI TS 102 232-3 w odniesieniu do usług dostępu do internetu;
4) ETSI TS 102 232-1 i ETSI TS 102 232-5 w odniesieniu do usług VoIP.

3.7. Specyfikacja interfejsu HI2 jest rozszerzona o parametr ExtendedPartyIdentity. Specyfikacja struktur danych w ASN.1 opisujących format tego parametru znajduje się w pkt VI.

3.8. Przesyłany plik może zawierać wiele pojedynczych rekordów IRI, pod warunkiem że dotyczą one tego samego LIID.

3.9. Nie stosuje się agregacji wielu rekordów IRI w jednej strukturze ASN.1.

3.10. Wartości parametrów IRI definiuje się w formatach zalecanych przez normy telekomunikacyjne, które ich dotyczą (np. ISDN user part, DSS1, MAP, IP).

3.11. Po skutecznym przekazaniu rekordów IRI ADMF usuwa związane z nimi dane ze swoich zasobów.

3.12. Interfejs HI2 nie wymaga stosowania podpisu elektronicznego.

4. Wymagania dla interfejsu HI3

4.1. Rozpoczęcie przekazywania do LEMF treści objętych monitorowaniem następuje niezwłocznie, jednak niepóźniej niż 10 minut od zakończenia przekazu.

4.2. Korelacja między rekordami IRI (w interfejsie HI2) a przekazywaną CC (w interfejsie HI3) odbywa się z wykorzystaniem LIID, a w przypadku usług sieci z komutacją kanałów – również parametru CIN (Communication Identity Number).

4.3. Do przekazywania treści objętych monitorowaniem dla usług sieci ruchomych:

1) w trybie offline:

a) stosuje się FTP, zdefiniowany w IETF RFC 0959, na zasadach określonych w ETSI ES 201 671,

b) zapis treści przekazów w przypadku połączeń głosowych może być realizowany:

– w trybie „stereo” dla każdego kierunku transmisji (od i do obiektu monitorowanego) jest tworzony odrębny plik,
– w trybie „mono” oba kierunki transmisji są zapisywane w ramach jednego pliku (zmiksowane w jeden strumień),

c) treść przesyłana za pośrednictwem HI3 jest zapisywana w plikach o nazwie zgodnej ze schematem: <LIID>_<CIN>.<ext>,

gdzie:

LIID – identyfikator obiektu monitorowanego,

CIN – Communication Identity Number,

ext – rodzaj zawartej informacji, przy czym:

– 2 oznacza CC (od obiektu monitorowanego),
– 4 oznacza CC (do obiektu monitorowanego),
– 6 oznacza CC (do i od obiektu monitorowanego),

d) nazwa przesyłanego pliku jest zmieniana na docelową po udanym nagraniu, a plik tymczasowy ma dodatkowe rozszerzenie .tmp (<LIID>_<CIN>.<ext>.tmp),

e) przedsiębiorca telekomunikacyjny nieodpłatnie dostarcza LEA kodeki umożliwiające odczyt plików audio i wideo oraz innych formatów danych i plików stosowanych przez przedsiębiorcę telekomunikacyjnego;

2) w trybie online:

a) ADMF przesyła do LEMF w czasie rzeczywistym przekazy telekomunikacyjne wysyłane i odbierane przez obiekt monitorowany,

b) do przesyłania przekazów stosuje się SIP, zgodny z IETF RFC 3261,

c) format pola Call-ID w nagłówku SIP przyjmuje postać LIID_cin,

d) przedsiębiorca telekomunikacyjny nieodpłatnie dostarcza LEA kodeki umożliwiające odbiór połączeń głosowych i wideo,

e) adres docelowy SIP określa się na podstawie parametru forwardingAddress, określanego przez LEA za pomocą interfejsu HI1.

4.4. Dopuszcza się przekazywanie treści objętych monitorowaniem, o których mowa w pkt 4.3, zgodnie z zasadami określonymi w ETSI TS 102 232-1 i ETSI TS 102 232-6.

4.5. W przypadku usług transmisji pakietowej w sieci ruchomej do przekazywania treści objętych monitorowaniem stosuje się protokół GLIC na zasadach określonych w ETSI ES 201 671.

4.6. Przekazywanie treści objętych monitorowaniem w sieci stacjonarnej jest realizowane zgodnie z zasadami określonymi w ETSI TS 102 232-1 i ETSI TS 102 232-6.

4.7. W przypadku usług dostępu do internetu przekazywanie treści objętych monitorowaniem jest realizowane zgodnie z zasadami określonymi w ETSI TS 102 232-1 i ETSI TS 102 232-3.

4.8. W przypadku usług VoIP przekazywanie treści objętych monitorowaniem jest realizowane zgodnie z zasadami określonymi w ETSI TS 102 232-1 i ETSI TS 102 232-5.

4.9. Po skutecznym przekazaniu treści objętych monitorowaniem do LEMF ADMF usuwa je ze swoich zasobów.

4.10. Interfejs HI3 nie wymaga stosowania podpisu elektronicznego.

V. Struktura interfejsu HI1

1. Warstwa transportowa:

1) jest stosowany TCP;

2) połączenia TCP są zestawiane w kierunkach:

a) od ADMF/MF/DF do LEMF (HI1LEMFOperations),

b) od LEMF do ADMF/MF/DF (HI1ADMFOperations);

3) w ramach jednego połączenia TCP jest wysyłana jedna wiadomość warstwy aplikacyjnej (żądanie, alarm), która jest potwierdzana przez drugą stronę (potwierdzenie otrzymania żądania, alarmu).

2. Warstwa aplikacyjna: wysyłane wiadomości są zdefiniowane w ASN.1 i kodowane w standardzie BER lub DER.

2.1. Opis

2.1.1. Przeznaczenie: przesyłanie zleceń aktywacji, dezaktywacji i modyfikacji dedykacji, zapytań o dedykacje, alarmów oraz raportów, w tym o statusie interfejsu.

2.1.2. Stosuje się dwa protokoły zdefiniowane w ASN.1:

1) HI1LEMFOperations – protokół przeznaczony do operacji inicjowanych przez LEMF;

2) HI1ADMFOperations – protokół przeznaczony do przesyłania alarmów i powiadomień wysyłanych przez ADMF.

2.1.3. Protokół HI1LEMFOperations i HI1ADMFOperations są całkowicie od siebie niezależne.

2.1.4. Każda operacja lub każde zapytanie to jedna sesja TCP.

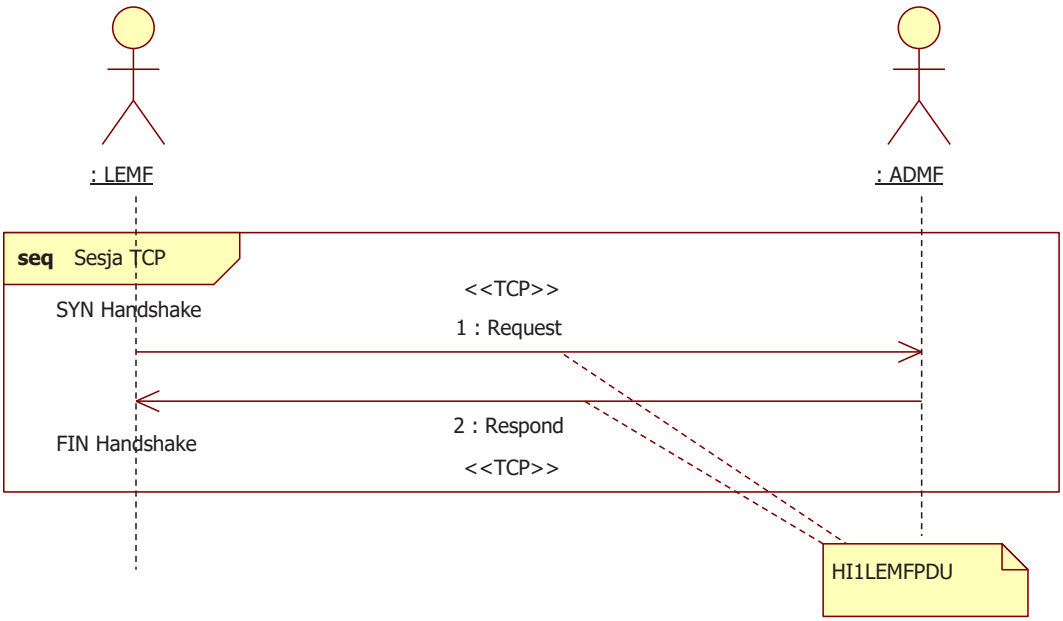
2.1.5. Każde zapytanie jest potwierdzane przez drugą stronę.

2.2. Protokół HI1LEMFOperations

2.2.1. Operacje wykonywane przez LEMF:

1) zapytana proste:
   a) Hello,
   b) ListRequest,
   c) RTRequest – żądanie włączenia lub wyłączenia trybu online (dotyczy tylko obserwacji rozpoczętych);
2) zapytana podpisane:
   a) Activate,
   b) Modificate, z wyjątkiem włączania/wyłączania trybu online,
   c) Deactivate.

2.2.2. Każda wiadomość definiująca zapytanie wysłane przez LEMF (Request) jest potwierdzana przez wiadomość zawierającą odpowiedź ADMF na wysłane żądanie LEMF (Respond), zgodnie ze schematem przedstawionym na rysunku 1.



Rysunek 1. Schemat operacji

2.2.3. LEMF czeka na odpowiedź 10 sekund, a o tym czasie uznaje wysłaną wiadomość za utraconą.

2.2.4. Nad harmonogramem aktywacji i dezaktywacji czuwa LEMF. Dopuszcza się wysłanie zlecenia aktywacji z wyprzedzeniem. Zlecenie aktywacji ma określony czas zakończenia obserwacji. Przesunięcie momentu zakończenia obserwacji ponad ten czas wymaga zlecenia modyfikacji.

2.2.5. ADMF przesyła do LEMF informacje o założeniu lub zdjęciu obserwacji w elementach sieci przedsiębiorcy telekomunikacyjnego.

2.2.6. LEMF ma możliwość zadania zapytania (ListRequest) służącego do weryfikacji stanu obserwacji.

2.2.7. Zlecenie dezaktywacji oznacza niezwłoczne zakończenie wskazanej obserwacji. W przypadku obserwacji, która się jeszcze nie rozpoczęła, oznacza to, że w ogóle nie zostanie zrealizowana. Fakt jej założenia ma jednak zostać odnotowany w logach systemu.

2.2.8. Modyfikacji podlegają jedynie zlecenia, które nie zakończyły się. Modyfikować można czasy zakończenia obserwacji oraz typ monitorowania (włączenie/wyłączenie online). Włączenie/wyłączenie obserwacji w trybie online nie powoduje zmian (zakłóceń) transmisji w trybie offline. Po rozpoczęciu obserwacji czas startu nie może być już modyfikowany.

2.2.9. Wiadomości są podzielone na dwie grupy:

1) Request – definiujące zapytania wysyłane przez LEMF;

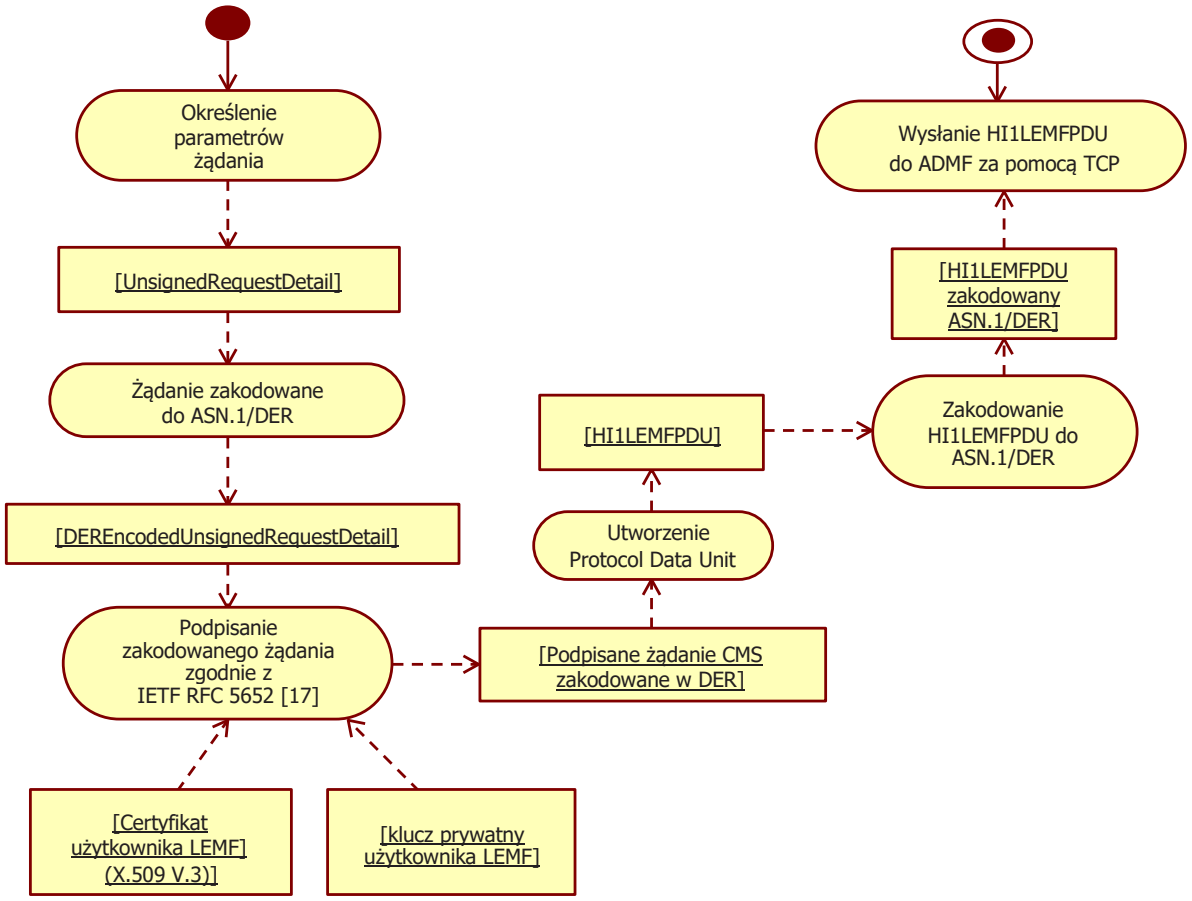
2) Respond – odpowiedzi ADMF na wysłane żądania LEMF.

2.2.10. Dopuszczalne są następujące interakcje między LEMF a ADMF:

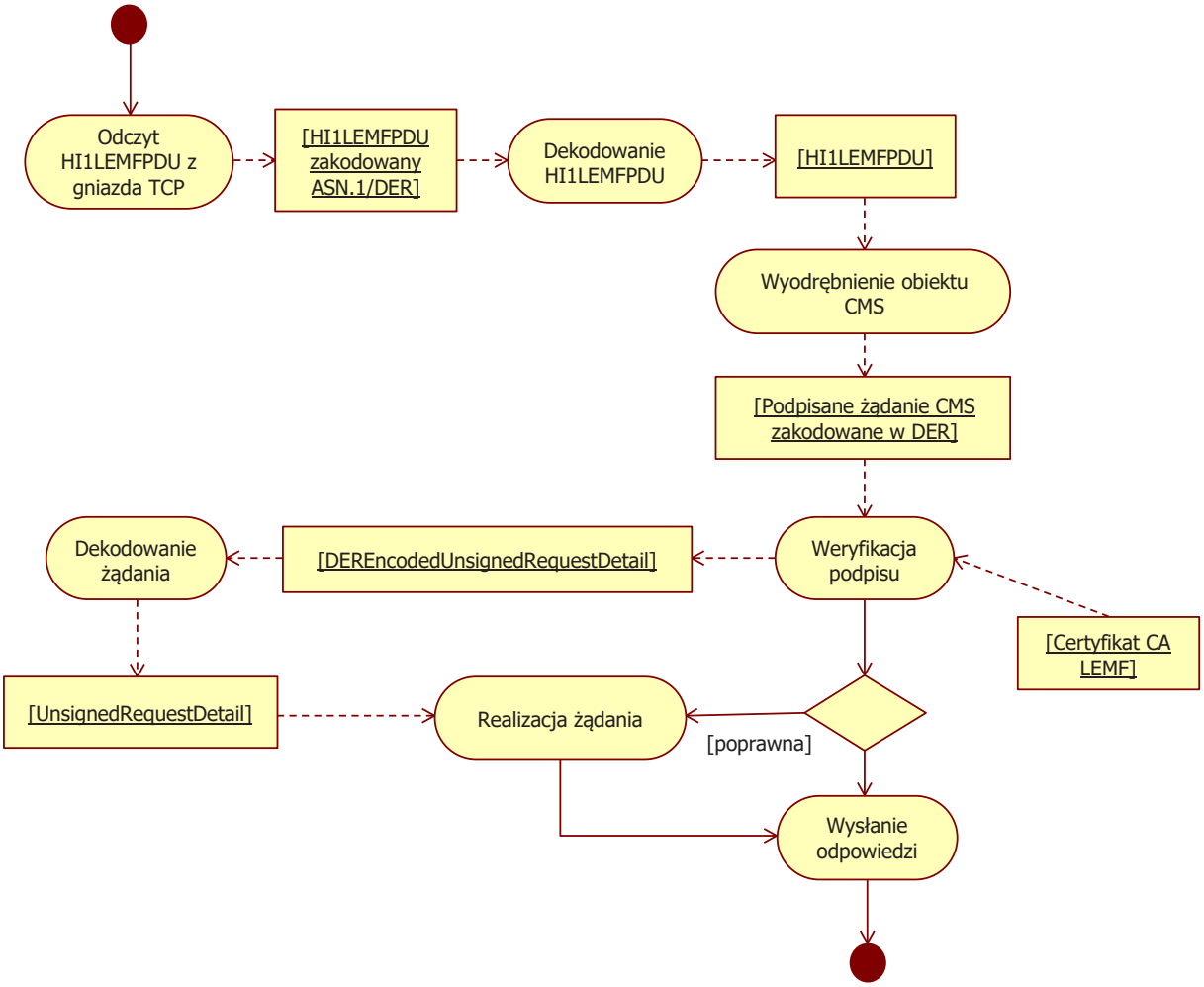
Tabela nr 3

Zapytanie LEMF	Odpowiedź ADMF	Alternatywna odpowiedź
SignedRequest	GeneralRespond	
HelloRequest	GeneralRespond	
ListRequest	ListRespond	GeneralRespond
RTRequest	GeneralRespond	

2.2.11. Zapytania podpisane (SignedRequest)**:** sposób tworzenia i weryfikacji wiadomości podpisanych przedstawiono w formie diagramów aktywności na rysunkach 2 i 3.



Rysunek 2. Tworzenie podpisanego zapytania



Rysunek 3. Weryfikacja podpisanego zapytania

2.2.12. Uwagi:

1) CMS – format binarny dokumentu z podpisem (z użyciem kodowania DER) stanowi podzbiór CMS; dokładna specyfikacja jest przedstawiona w IETF RFC 3852;

2) identyfikator obiektu OID (Object Identifier) definiujący standard ma w ASN.1 postać:

```
OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) modules(0) cms-2004(24) }
```

3) struktura UnsignedRequestDetail, przedstawiona na rysunku 6, opisuje szczegóły zapytania aktywacji, modyfikacji i dezaktywacji dedykacji; po zakodowaniu do postaci DER jest podpisywana zgodnie ze specyfikacją przedstawioną w IETF RFC 2315;

4) Service – obiekt reprezentujący usługi świadczone przez operatora;

5) monitorowaniu podlegają następujące usługi:

a) CS Circuit Switched (Mobile),

b) PS PacketSwitched,

c) InternetAccess,

d) InternetTelephony,

e) CS Circuit Switched (Fixed).

2.3. Protokół HI1ADMFOperations

2.3.1. Operacje wykonywane przez ADMF:

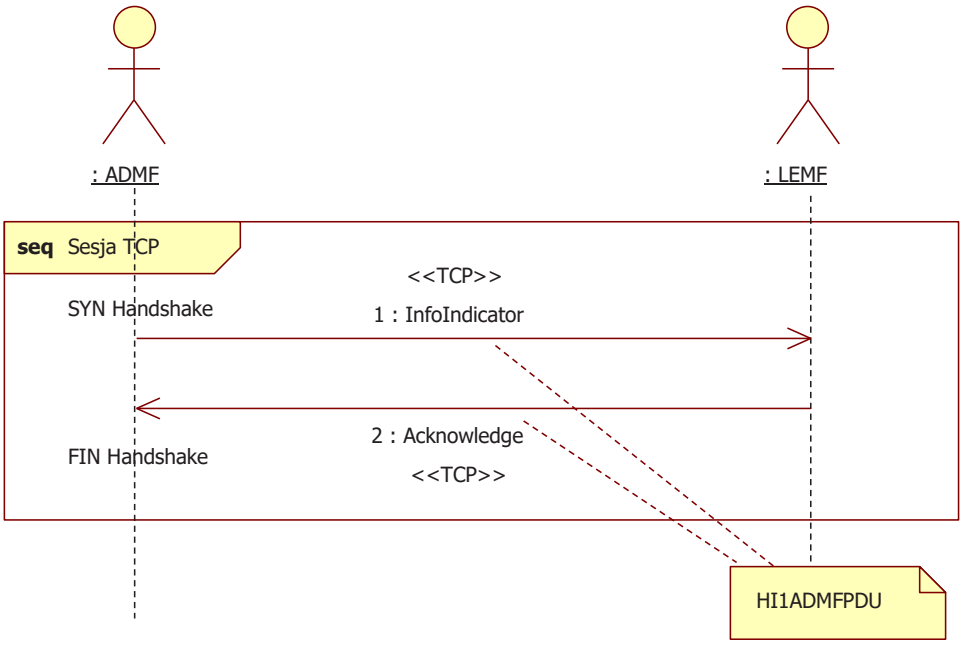
1) alarmy;

2) notyfikacje.

2.3.2. Wiadomości są podzielone na dwie grupy, zgodnie ze schematem przedstawionym na rysunku 4:

1) InfoIndicator – definiujące alarmy i notyfikacje wysyłane przez ADMF;

2) Acknowledge – potwierdzenia otrzymania wiadomości przez ADMF.



Rysunek 4. Schemat operacji

2.3.3. Dopuszczalne są następujące interakcje między ADMF a LEMF:

Tabela nr 4

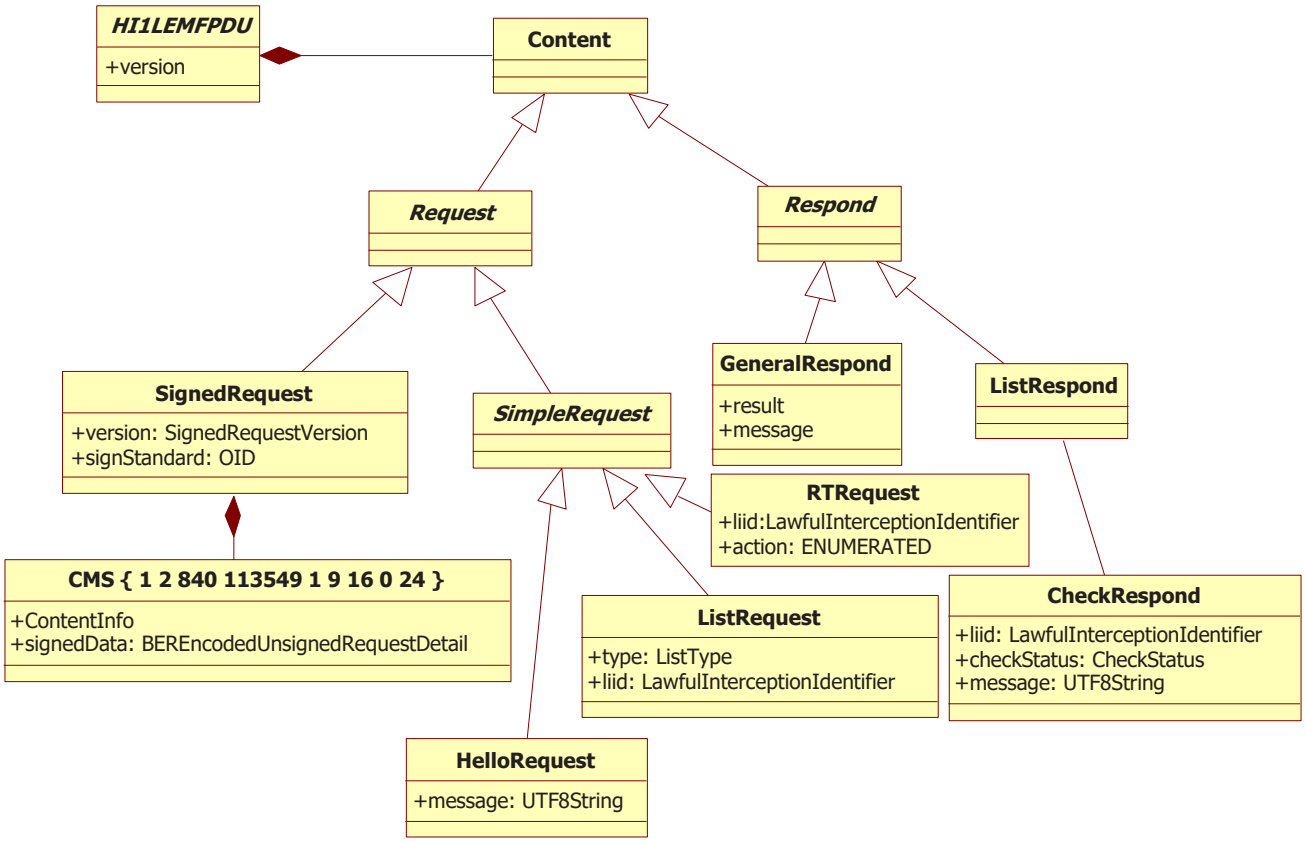
Wiadomość ADMF	Odpowiedź LEMF
HelloRequest	GeneralRespond
AlarmIndicator	GeneralRespond
NotificationIndicator	GeneralRespond

2.3.4. Uwagi:

1) wyróżnia się dwa typy wiadomości wysyłanych przez ADMF: alarmy i notyfikacje;
2) każda wysłana wiadomość (InfoIndicator) jest potwierdzana przez LEMF (Acknowledge);
3) potwierdzenie jest realizowane w ciągu 5 sekund;
4) alarmy mają dwa stany: włączony, wyłączony (pole status);
5) wiadomość wyłączająca alarm może zawierać tylko jego identyfikator (identity).

3. Protokół HI1LEMFPDU

3.1. Struktura protokołu HI1LEMFPDU



Rysunek 5. Struktura protokołu HI1LEMFPDU

3.2. Specyfikacja ASN.1 dla protokołu HI1LEMFPDU

```
HI1LEMFOperations DEFINITIONS AUTOMATIC TAGS ::=
BEGIN
IMPORTS
  LawfulInterceptionIdentifier,
  TimeStamp
FROM
  UnsignedRequestDetail;

HI1LEMFPDU ::= SEQUENCE
{
  version [0] Version,
  content [1] Content,
  operator [2] UTF8String OPTIONAL,
  ...
}

Version ::= ENUMERATED
{
  version1 (1),
  ...
}

Content ::= CHOICE
{
  request [1] Request,
  respond [2] Respond,
  ...
}

SignedRequest ::= SEQUENCE
{
  version [1] SignedRequestVersion,
  signStandard [2] OBJECT IDENTIFIER,
  -- CryptographicMessageSyntax2004 { iso(1) member-body(2) us(840) rsadsi(113549)
pkcs(1) pkcs-9(9) smime(16) modules(0) cms-2004(24)
  cmsDERSignedRequest [3] OCTET STRING,
  -- cmsDERSignedRequest [3] ANY DEFINED BY signStandard
  ...
}
```

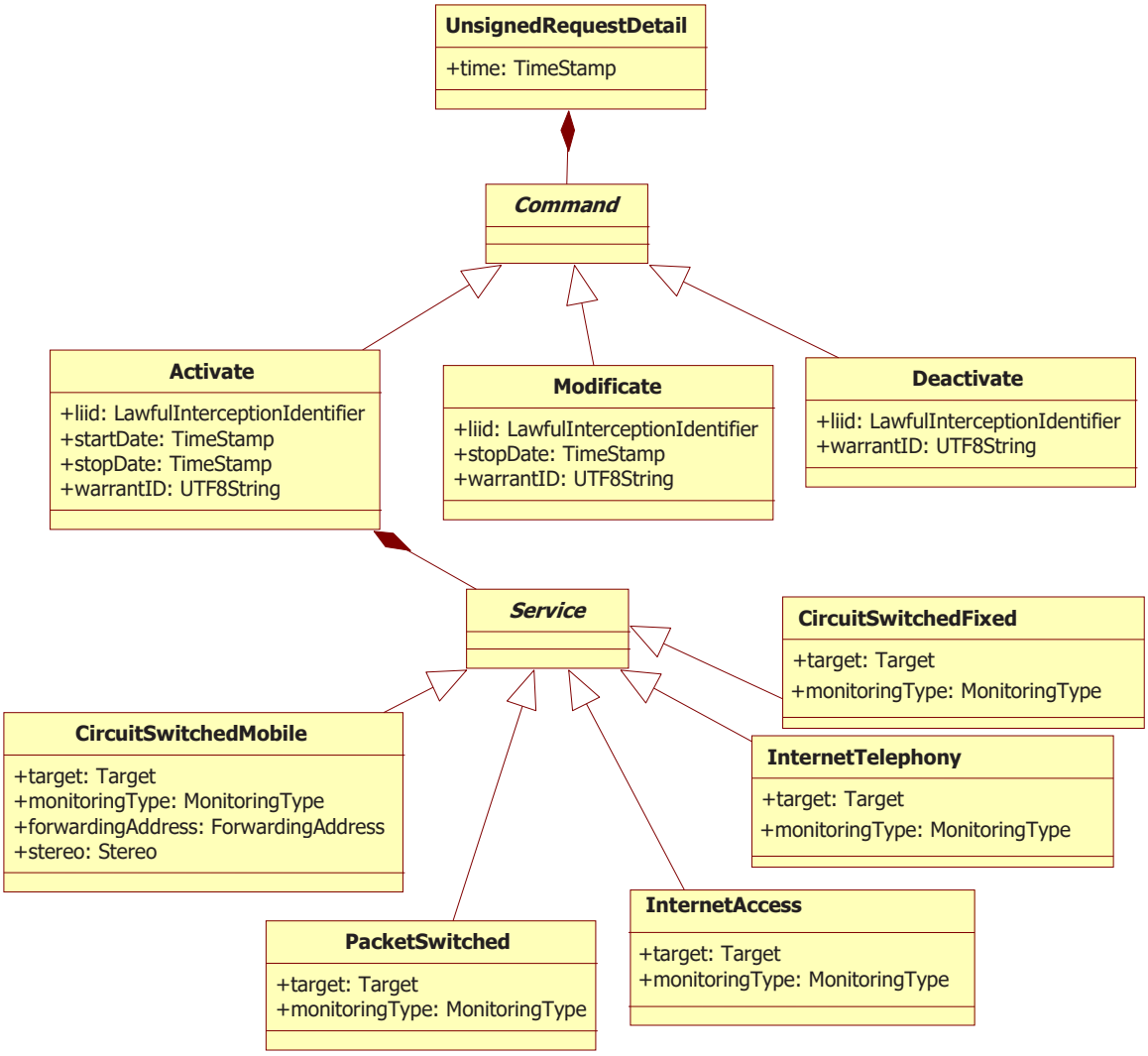
```
Request ::= CHOICE
{
  simpleRequest [1] SimpleRequest,
  signedRequest [2] SignedRequest,
  ...
}

SimpleRequest ::= CHOICE
{
  helloRequest [1] HelloRequest,
  listRequest [2] ListRequest,
  rtRequest [3] RTRequest, -- Żądanie włączenia lub  wyłączenia trybu online
(dotyczą tylko obserwacji rozpoczętych) dla obserwacji aktywnych
  ...
}
RTRequest ::= SEQUENCE
{
  liid [1] LawfulInterceptionIdentifier,
  action [2] ENUMERATED
  {
    start(0), -- Włączenie odsłuchu online
    stop(1) -- Wyłączenie odsłuchu online
  },
}

SignedRequestVersion ::= ENUMERATED
{
  v1 (0),
  ...
}

HelloRequest ::= SEQUENCE
{
  message [1] UTF8String,
  ...
}

Respond ::= CHOICE
{
  generalRespond [1] GeneralRespond,
  listRespond [2] ListRespond,
  ...
}
```

```
GeneralRespond ::= SEQUENCE
{
  result [1] Result,
  message [2] UTF8String OPTIONAL,
  -- return Hello request message
  ...
}

Result ::= ENUMERATED
{
  ok (1),
  missing-parameter (2),
  unknown-parameter (3),
  unknown-parameter-value (4),
  incorrect-BER (5),
  badSignature (6),
  certificateExpired (7),
  unknownError (10),
  unsupportedService (11),
  ...
}

CheckRespond ::= SEQUENCE
{
  liid [1] LawfulInterceptionIdentifier,
  checkStatus [2] CheckStatus,
  message [3] UTF8String OPTIONAL,
  ...
}

CheckStatus ::= ENUMERATED
{
  notFound (0),
  waiting (1),  -- założone przez lemf, nie ma w cn (czeka na zatwierdzenie lub )
  cnActivated (2), -- jest w cn
  unknown (3),
  deActivated (4), -- po deaktywowaniu w cn
  ...
}

ListRequest ::= SEQUENCE
{
```

```
  type [1] ListType,
  liid [2] LawfulInterceptionIdentifier OPTIONAL,
  ...
}

ListRespond ::= SET OF CheckRespond

ListType ::= ENUMERATED
{
  all (1),
  specific (2),
  ...
}

END
```

4. UnsignedRequestDetail

4.1. Struktura UnsignedRequestDetail



Rysunek 6. Struktura UnsignedRequestDetail

4.2. Specyfikacja ASN.1 dla UnsignedRequestDetail

```
UnsignedRequestDetail DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

UnsignedRequestDetail ::= SEQUENCE
{
  time [1] TimeStamp,
  command [2] Command,
  operator [2] UTF8String OPTIONAL,
  ...
}

Command ::= CHOICE
```

```
{
  activate [1] Activate,
  deactivate [2] Deactivate,
  modificate [3] Modificate,
  ...
}

Activate ::= SEQUENCE
{
  lawfulInterceptionIdentifier [1] LawfulInterceptionIdentifier,
  startTimestamp [2] TimeStamp,
  stopTimestap [3] TimeStamp,
  service [4] Service,
  warrantID [5] UTF8String,
  ...
}

Modificate ::= SEQUENCE
{
  lawfulInterceptionIdentifier [1] LawfulInterceptionIdentifier,
  stopTimestap [3] TimeStamp,
  warrantID [5] UTF8String,
  ...
}

Deactivate ::= SEQUENCE
{
  lawfulInterceptionIdentifier [1] LawfulInterceptionIdentifier,
  warrantID [5] UTF8String OPTIONAL,
  ...
}

Service ::= CHOICE
{
  circuitSwitchedMobile [1] CircuitSwitchedMobile,
  packetSwitched [2] PacketSwitched,
  wifi [3] WIFI, -- not used
  xdsl [4] XDSL, -- not used
  internetAccess [5] InternetAccess,
  internetTelephony [6] InternetTelephony,
  circuitSwitchedFixed [7] CircuitSwitchedFixed,
  generic [8] GenericService,
```

```
  ...
}

GenericService ::= SEQUENCE
{
  identityType [1] UTF8String (SIZE(1..20)),
  identityValue [2] UTF8String,
  service [3] UFT8String OPTIONAL,
  ...
}

CircuitSwitchedMobile ::= SEQUENCE
{
  target [1] Target,
  monitoringType [2] MonitoringType,
  onlineMonitoring [3] BOOLEAN,
  -- offline - wartość domyślna,
  -- online,
  forwardingAddress [4] ForwardingAddress,
  stereo [5] Stereo,
  ...
}

Stereo ::= ENUMERATED
{
  off (0),
  on (1)
}

PacketSwitched ::= SEQUENCE
{
  target [1] Target,
  monitoringType [2] MonitoringType,
  ...
}

WIFI ::= SEQUENCE
{
  target [1] Target,
  ...
}
```

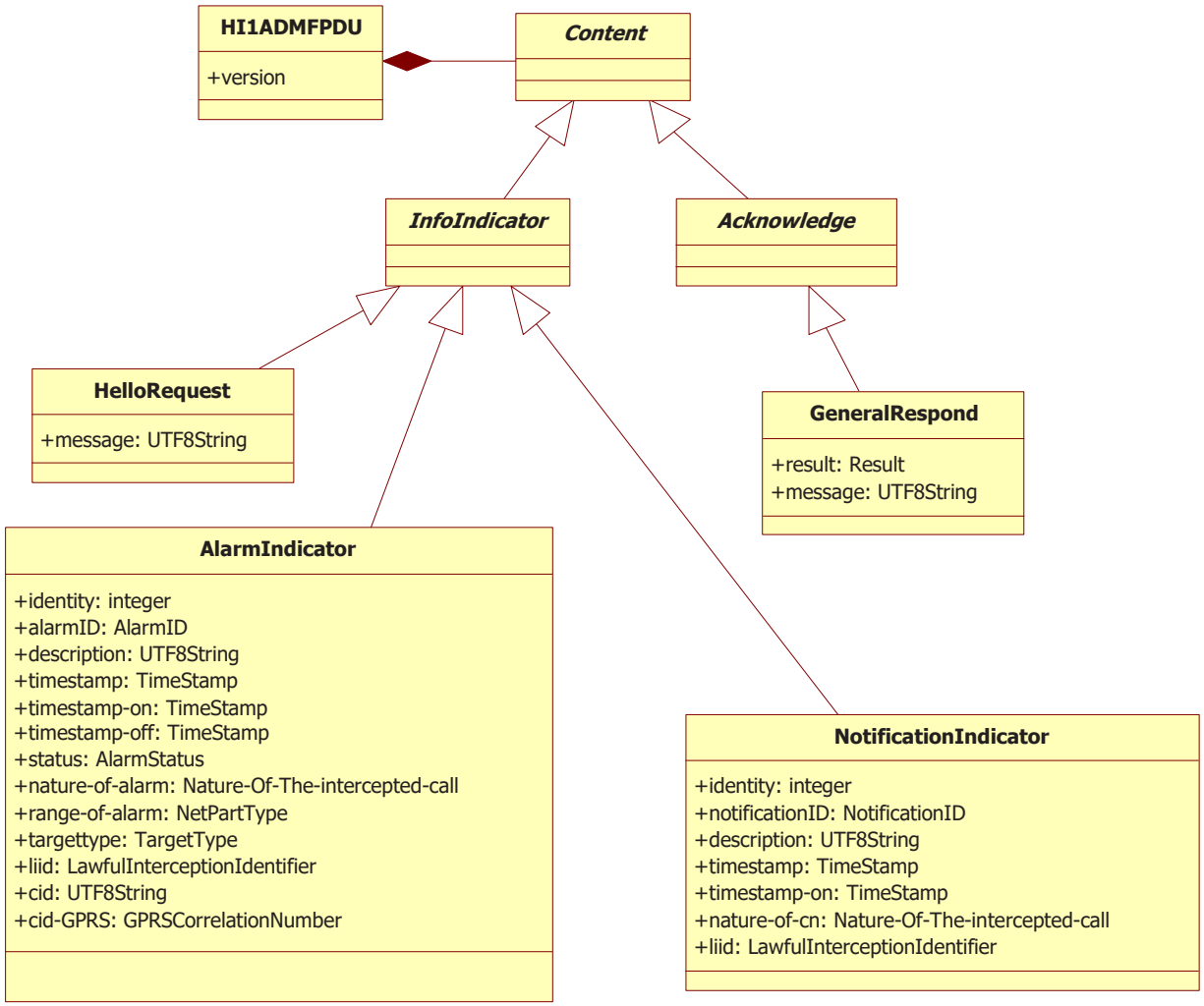
```
XDSL ::= SEQUENCE
{
  target [1] Target,
  ...
}

InternetAccess::= SEQUENCE
{
  target [1] Target,
  monitoringType [2] MonitoringType,
  ...
}

InternetTelephony ::= SEQUENCE
{
  target [1] Target,
  monitoringType [2] MonitoringType,
  ...
}

CircuitSwitchedFixed ::= SEQUENCE
{
  target [1] Target,
  monitoringType [2] MonitoringType,
  ...
}

Target ::= CHOICE
{
  mSISDN [1] MSISDN, -- wykorzystywany również jako numer abonenta ISDN/PSTN lub
telefonii internetowej(o ile jest to numer zgodny z E.164)
  iMSI [2] IMSI,
  iMEI [3] IMEI,
  login [4] Login,
  iPAddress [5] IPAddress,
  mAC [6] MAC,
  eSN [7] ESN,
  ...
}

MSISDN ::= OCTET STRING (SIZE (1..9))
IMSI ::= OCTET STRING (SIZE (3..8))
IMEI ::= OCTET STRING (SIZE (8))
```

```
Login ::= OCTET STRING (SIZE (1..120))
IPAddress ::= OCTET STRING (SIZE (4))
MAC ::= OCTET STRING (SIZE (6))
ESN ::= OCTET STRING (SIZE (8))

ForwardingAddress ::= SEQUENCE
{
  sipUrl [1] SIPURL,
  ...
}

SIPURL ::= UTF8String

MonitoringType ::= ENUMERATED
{
  iri (1),
  iriCC (2),
  ...
}

LawfulInterceptionIdentifier ::= OCTET STRING (SIZE (1..25))
-- It is recommended to use ASCII characters in " "0"…"9".
-- For subaddress option only "0"..."9" shall be used.
-- 17 znaków numerycznych ASCII
-- format: LEAID + TARGET(SEQ)
-- TARGET - (15 znaków) nadawany sekwencyjnie dla każdego LEAID
-- LEAID -(2 znaki) 00 – LEMF operatora, 01 - ABW, 02 - Policja, 03 - SKW, 04 - ZW,
05 - SG, 06 – MF, 07 - CBA

TimeStamp ::= CHOICE
{
  -- The minimum resolution required is one second.
  -- "Resolution" is the smallest incremental change that can be measured for time
and
  -- is expressed with a definite number of decimal digits or bits.
  localTime [0] LocalTimeStamp,
  utcTime [1] UTCTime
}

LocalTimeStamp ::= SEQUENCE
{
  generalizedTime [0] GeneralizedTime,
  -- The minimum resolution required is one second.
```

```
  -- "Resolution" is the smallest incremental change that can be measured for time
and
  -- is expressed with a definite number of decimal digits or bits.

  winterSummerIndication [1] ENUMERATED
  {
    notProvided(0),
    winterTime(1),
    summerTime(2)
  }
}
END
```

5. Protokół HI1ADMFPDU

5.1. Struktura protokołu HI1ADMFPDU



Rysunek 7. Struktura protokołu HI1ADMFPDU

5.2. Specyfikacja ASN.1 dla protokołu HI1ADMFPDU

```
HI1ADMFOperations DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

IMPORTS
  LawfulInterceptionIdentifier,
  TimeStamp
FROM
UnsignedRequestDetail;
HI1ADMFPDU ::= SEQUENCE
{
  version [0] Version,
  content [1] Content
  operator [2] UTF8String OPTIONAL,
}

Version ::= ENUMERATED
{
  version1 (1),
  ...
}

Content ::= CHOICE
{
  info [0] InfoIndicator,
  acknowledge [1] Acknowledge,
  ...
}

InfoIndicator ::= CHOICE
{
  helloRequest [1] HelloRequest,
  alarm [2] AlarmIndicator,
  notification [3] NotificationIndicator,
  ...
}

HelloRequest ::= SEQUENCE
{
  message [1] UTF8String,
  ...
```

```
}


AlarmIndicator ::= SEQUENCE

{

  identity [0] INTEGER, -- numer pozwalający na jednoznaczną identyfikację alarmu
razem z timestamp-on

  alarmID [1] AlarmID,

  description [2] UTF8String OPTIONAL,       -- dodatkowe informacje, opis, kod
błędu (np. z alarmu z MSC), tzw. powód

  timestamp[3] TimeStamp,           -- czas wysłania alarmu

  timestamp-on [4] TimeStamp OPTIONAL,      -- czas wystąpienia alarmowanego
zdarzenia

  timestamp-off [5] TimeStamp OPTIONAL,     -- czas wystąpienia zdarzenia
odwrotnego do zdarzenia alarmowanego

  status [6] AlarmStatus OPTIONAL,     -- powstanie/ustanie alarmu

  -- podobne nature-Of-The-intercepted-call z HI2 (jeżeli błąd globalny to
wszystkie service)

  nature-of-alarm  [7] Nature-Of-The-intercepted-call OPTIONAL,

  range-of-alarm [8] NetPartType OPTIONAL,   -- dotyczy całej sieci CN czy tylko
jej części (np.: tylko jeden GGSN, jedna centrala)

  targettype [9] TargetType OPTIONAL,     -- dotyczy konkretnego LIID lub konkretnej
sesji albo wszystkich obserwacji

  liid [10] LawfulInterceptionIdentifier OPTIONAL,

  cid [11] UTF8String OPTIONAL,         -- z HI2 (chodzi o wskazanie konkretnej
rozmowy lub sesji)

  cid-GPRS [12] GPRSCorrelationNumber OPTIONAL,-- z HI2 (chodzi o wskazanie
konkretnej rozmowy lub sesji)

  ...

}


Nature-Of-The-intercepted-call ::= ENUMERATED

{

  -- Nature of the intercepted "call":

  gSM-ISDN-PSTN-circuit-call(0),

  -- the possible UUS content is sent through the HI2 or HI3 "data" interface

  -- the possible call content call is established through the HI3 "circuit"
interface

  gSM-SMS-Message(1),

  -- the SMS content is sent through the HI2 or HI3 "data" interface

  uUS4-Messages(2),

  -- the UUS content is sent through the HI2 or HI3 "data" interface

  tETRA-circuit-call(3),

  -- the possible call content call is established through the HI3 "circuit"
interface

  -- the possible data are sent through the HI3 "data" interface

  teTRA-Packet-Data(4),
```

```
  -- the data are sent through the HI3 "data" interface
  gPRS-Packet-Data(5),
  -- the data are sent through the HI3 "data" interface
  uMTS-circuit-call(6),
  -- the possible call content call is established through the HI3 "circuit"
interface
  -- the possible data are sent through the HI3 "data" interface
  wIFI (11), -- not used
  xDSL (12), -- not used
  internetAccess (13),
  internetTelephony (14),
    ...
}


NotificationIndicator ::= SEQUENCE
{
  identity [0] INTEGER,      -- numer pozwalający na jednoznaczną identyfikację
alarmu razem z timestamp-on
  notificationID [1] NotificationID,
  description [2] UTF8String OPTIONAL,   -- dodatkowe informacje, opis, kod błędu
(np. z MSC), tzw. powód
  timestamp [3] TimeStamp,      -- czas wysłania powiadomienia
  timestampEvent [4] TimeStamp,    -- czas wystąpienia zdarzenia, którego dotyczy
powiadomienie
  liid [5] LawfulInterceptionIdentifier OPTIONAL,
  ...
}


AlarmID ::= ENUMERATED
{
  sm-buffer-overflow (0),     -- bufory wyjściowe w kierunku LEMF przepełnione =>
IRI i/lub CC tracone (operator)
  lemf-hi3-online-delivery-failure (1),  -- problem z monitoringiem online (LEMF)
  lemf-hi3-delivery-failure (2),   -- problem z zapisywaniem danych HI3 (LEMF)
  lemf-hi2-delivery-failure (3),   -- problem z zapisywaniem danych HI2 (LEMF)
  lemf-hi1-delivery-failure (4),   -- problem z monitoringiem online (LEMF)
  sm-hi1-failure (5),     -- brak lub przeciążenie komunikacji z CN na interfejsie
HI1 (SM operatora)
  sm-hi2-failure (6),     -- brak lub przeciążenie komunikacji z CN na interfejsie
HI2 (SM operatora)
  sm-hi3-failure (7),     -- brak lub przeciążenie komunikacji z CN na interfejsie
HI3 (SM operatora)
  sm-hi3-online-failure (8),  -- brak lub przeciążenie komunikacji z CN na
interfejsie HI3 (SM operatora)
  major-system-failure (9),   -- poważne uszkodzenie SM => konieczne sprawdzenie
spójności BD (SM operatora)
```

```
  -- zarządzanie obserwacjami prawidłowe, ale inne funkcje SM mogą nie działać (np.
część obserwacji stracona) (SM operatora)
  minor-system-failure (10),
  cn-activation-error (11),   -- obserwacja nie założona w CN a czas na nią (LIID
obowiązkowy) (SM operatora)
  cn-deactivation-error (12),   -- obserwacja nie usunięta z CN a czas na nią (LIID
obowiązkowy) (SM operatora)
  major-cn-li-failure (13),   -- po stronie CN LI całkowicie nie funkcjonowało, BD
obserwacji odbudowane w CN (SM operatora)
  minor-cn-li-failure (14),   -- po stronie CN pewne funkcje LI nie działały (SM
operatora)
  manual-system-failure (15),  -- informacja wprowadzana ręcznie: uszkodzenie w CN
lub SM (SM operatora)
  manual-system-maintenance (20),-- informacja wprowadzana ręcznie o pracach
planowych w systemie SM operatora (SM operatora)
  ...
}

AlarmStatus ::= ENUMERATED
{
  off (0),
  on (1),
  ...
}

NetPartType ::= ENUMERATED
{
  whole (1),
  part (2),
  ...
}

TargetType ::= ENUMERATED
{
  all (1),
  specific (2),
  ...
}

NotificationID ::= ENUMERATED
{
  target-activated (0),
  target-deactivated (1),
  target-modificated (2),
  ...
```

```
}

Acknowledge ::= CHOICE
{
  respond [0] GeneralRespond,
  ...
}

GeneralRespond ::= SEQUENCE
{
  result  [1] Result,
  message [2] UTF8String OPTIONAL,
  ...
}

Result ::= ENUMERATED
{
  ok (1),
  missing-parameter (2),
  unknown-parameter (3),
  unknown-parameter-value (4),
  incorrect-BER (5),
  badSignature (6),
  certificateExpired (7),
  unknownError (10),
  ...
}

GPRSCorrelationNumber ::= OCTET STRING (SIZE(8..20))

END
```

VI. Format parametru ExtendedPartyIdentity

```
PartyInformation ::= SEQUENCE
{
  ...
  partyExtendedIdentity [PRIVATE 1] PartyExtendedIdentity OPTIONAL,
  ...
}

PartyExtendedIdentity ::= SEQUENCE
```

```
{
  subscriptionType [1] ENUMERATED
  {
    postpaid (0),
    prepaid  (1),
    ...
  } OPTIONAL,

  activationDate [2] TimeStamp OPTIONAL,
  deactivationDate [3] TimeStamp OPTIONAL,
  subscriber [4] Subscriber OPTIONAL,
  postalAddress [5] PostalAddress OPTIONAL,
  mailAddress [6] MailAddress OPTIONAL,
  ...
}

Subscriber ::= CHOICE
{
  company [1] Company,
  person [2] Person,
  ...
}

Company ::= SEQUENCE
{
  name [0] UTF8String,
  regon[1] OCTET STRING (SIZE (5)) OPTIONAL,
  -- BCD coded 9 digits
  -- F digit not used
  ...
}

Person ::= SEQUENCE
{
  firstName [0] UTF8String,
  surname [1] UTF8String,
  pesel  [2] OCTET STRING (SIZE (6)) OPTIONAL,
  -- BCD coded 11 digits
  -- F digit not used
  passportNumber [3] OCTET STRING (SIZE (7..14)) OPTIONAL,
  -- ASCII coded
  ...
```

```
}

PostalAddress ::= SEQUENCE
{
  street [1] UTF8String OPTIONAL,
  buildingNumber [2] OCTET STRING (SIZE (1..10)) OPTIONAL,
  -- ASCII coded: 10 char
  apartmentNumber [3] OCTET STRING (SIZE (1..10)) OPTIONAL,
  -- ASCII coded: 10 char
  postcode [4] OCTET STRING (SIZE (1..8)) OPTIONAL,
  city [5] UTF8String OPTIONAL,
  country [6] UTF8String OPTIONAL
}
```