Warszawa, dnia 22 lutego 2012 r.

Pozycja 200

ROZPORZĄDZENIE
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[1)]

Na podstawie art. 182 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.[2)]) zarządza się, co następuje:

§ 1. Wymagania techniczne i eksploatacyjne dla interfejsów, o których mowa w art. 179 ust. 4a ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne, umożliwiających wykonywanie zadań i obowiązków na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego, o których mowa w art. 179 ust. 3 i w art. 180d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne, określa załącznik do rozporządzenia.

§ 2. Przepisów rozporządzenia nie stosuje się do umów, o których mowa w art. 179 ust. 4a ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne, zawartych przed dniem wejścia w życie rozporządzenia, w zakresie usług telekomunikacyjnych objętych tymi umowami, chyba że strony postanowią inaczej.

§ 3. Rozporządzenie wchodzi w życie po upływie 3 miesięcy od dnia ogłoszenia.

Prezes Rady Ministrów: *D. Tusk*

[1)] Niniejsze rozporządzenie zostało notyfikowane Komisji Europejskiej w dniu 6 września 2011 r., pod numerem 2011/0460/PL, zgodnie z § 4 rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. Nr 239, poz. 2039 oraz z 2004 r. Nr 65, poz. 597), które wdraża dyrektywę 98/34/WE Parlamentu Europejskiego i Rady z dnia 22 czerwca 1998 r. ustanawiającą procedurę udzielania informacji w dziedzinie norm i przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego (Dz. Urz. UE L 204 z 21.07.1998, z późn. zm.; Dz. Urz. UE Polskie wydanie specjalne, rozdz. 13, t. 20, str. 337, z późn. zm.).

[2)] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2004 r. Nr 273, poz. 2703, z 2005 r. Nr 163, poz. 1362 i Nr 267, poz. 2258, z 2006 r. Nr 12, poz. 66, Nr 104, poz. 708 i 711, Nr 170, poz. 1217, Nr 220, poz. 1600, Nr 235, poz. 1700 i Nr 249, poz. 1834, z 2007 r. Nr 23, poz. 137, Nr 50, poz. 331 i Nr 82, poz. 556, z 2008 r. Nr 17, poz. 101 i Nr 227, poz. 1505, z 2009 r. Nr 11, poz. 59, Nr 18, poz. 97 i Nr 85, poz. 716, z 2010 r. Nr 81, poz. 530, Nr 86, poz. 554, Nr 106, poz. 675, Nr 182, poz. 1228, Nr 219, poz. 1443, Nr 229, poz. 1499 i Nr 238, poz. 1578 oraz z 2011 r. Nr 102, poz. 586 i 587, Nr 134, poz. 779, Nr 153, poz. 903, Nr 171, poz. 1016, Nr 233, poz. 1381 i Nr 234, poz. 1390.

Załącznik do rozporządzenia Rady Ministrów
z dnia 20 stycznia 2012 r. (poz. 200)

WYMAGANIA TECHNICZNE I EKSPLOATACYJNE

dla interfejsów umożliwiających wykonywanie zadań i obowiązków na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego

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 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".

1.7. 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".

1.8. 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".

1.9. 802.3ab-1999 - IEEE Standard for 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".

1.10. IETF RFC 0791 *Internet Protocol,* zwany dalej „IETF RFC 0791".

1.11. IETF RFC 0793 *Transmission Control Protocol,* zwany dalej „IETF RFC 0793".

1.12. IETF RFC 0959 *File Transfer Protocol,* zwany dalej „IETF RFC 0959".

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

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

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

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

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

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

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

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

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

1.22. 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 - 1.8, są dostępne na stronach Europejskiego Instytutu Norm Telekomunikacyjnych ETSI (www.etsi.org).

3. Dokument, o którym mowa w pkt 1.9, jest dostępny na stronach Instytutu Inżynierów Elektryków i Elektroników IEEE (www.ieee.org).

4. Dokumenty, o których mowa w pkt 1.10 - 1.17, są dostępne na stronach zespołu inżynierów ustanawiających standardy techniczne i organizacyjne w Internecie IETF (www.ietf.org).

5. Dokumenty, o których mowa w pkt 1.18 - 1.22, są dostępne na stronach 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 pomiędzy 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 notacji ASN.1 do postaci transmitowanej w sieciach telekomunikacyjnych (Basic Encoding Rules), zgodny z ITU-T X.690.

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

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

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

8. CS – komutacja kanałów (Circuit Switched).

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

10. ESN – indywidualny numer identyfikujący telekomunikacyjne urządzenie końcowe używane w ruchomej publicznej sieci telefonicznej wykorzystującej technologię CDMA (Code Division Multiple Access) (Electronic Serial Number).

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

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

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

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

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

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

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

18. LEMF – system monitorowania uprawnionego podmiotu umożliwiający dostęp do wybranych treści przekazów telekomunikacyjnych (Law Enforcement Monitoring Facility).

19. LI HI – interfejs pomiędzy systemem monitorowania uprawnionego podmiotu a systemem przedsiębiorcy telekomunikacyjnego, wykorzystywany na potrzeby uprawnionego monitorowania (Lawful Interception Handover Interface).
20. LIID – identyfikator obiektu monitorowanego (Lawful Interception Identifier).
21. LOGIN – nazwa użytkownika logującego się do sieci, używana w procesie jego uwierzytelnienia.
22. MAC – sprzętowy adres karty sieciowej (Media Access Control).
23. MEID – unikalny numer identyfikujący telekomunikacyjne urządzenie końcowe używane w ruchomej publicznej sieci telefonicznej wykorzystującej technologię CDMA, zastępujący ESN (Mobile Equipment Identifier).
24. MSISDN – numer przydzielony użytkownikowi końcowemu ruchomej publicznej sieci telefonicznej z integracją usług (Mobile Subscriber Integrated Services Digital Network).
25. PKI – Infrastruktura Klucza Publicznego będąca systemem kryptograficznym, w którego skład wchodzą urzędy certyfikacyjne, użytkownicy certyfikatów (subskrybenci) oraz oprogramowanie i sprzęt (Public Key Infrastructure).
26. PSTN – publiczna komutowana sieć telefoniczna (Public Switched Telephone Network).
27. 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.
28. SMS – krótka wiadomość tekstowa (Short Message Service).
29. TCP – protokół komunikacji w sieci komputerowej (Transmission Control Protocol), zdefiniowany w IETF RFC 0793.
30. VoIP – telefonia internetowa (Voice over IP).
31. WAN – rozległa sieć komputerowa (Wide Area Network).

III. Określenia użyte w załączniku oznaczają:

1. Interfejs LI HI – elektroniczny, zdalny, oparty na protokole komunikacyjnym IP, interfejs między systemem przedsiębiorcy telekomunikacyjnego a systemem uprawnionego podmiotu, umożliwiający realizację dostępu do wybranych treści przekazów telekomunikacyjnych, w skład którego wchodzą:
   a) interfejs HI1 – styk umożliwiający dwukierunkową wymianę wiadomości między LEMF a ADMF. Wykorzystywany jest przez LEMF do przesyłania żądań, natomiast ADMF przesyła głównie notyfikacje zdarzeń/stanu realizacji żądań. Ponadto realizuje inne funkcje, opisane w pkt VI,
   b) interfejs HI2 – styk umożliwiający jednokierunkowe, w kierunku od ADMF do LEMF, przesyłanie informacji związanych z objętymi monitorowaniem

przekazami telekomunikacyjnymi oraz treści krótkich wiadomości tekstowych SMS,

c) interfejs HI3 – styk umożliwiający jednokierunkowe, w kierunku od ADMF do LEMF, przesyłanie treści monitorowanych.

2. Interfejs HI A-B – elektroniczny, zdalny, oparty na protokole komunikacyjnym IP, interfejs służący do dostarczania przez przedsiębiorcę telekomunikacyjnego uprawnionemu podmiotowi danych, o których mowa w art. 180d ustawy – Prawo telekomunikacyjne, w skład którego wchodzą:

   a) interfejs HI A – styk służący do realizowania funkcji administracyjnych polegających na przesyłaniu i obsłudze wiadomości przekazywanych w obu kierunkach między LEMF a ADMF,

   b) interfejs HI B – styk służący do przekazywania przez ADMF wyników zapytań składanych za pośrednictwem HI A.

3. Obiekt monitorowany – obiekt wskazany w postanowieniu sądu wydanym na podstawie wniosku albo zarządzenia organu uprawnionego podmiotu wydanego na podstawie odrębnych przepisów.

4. Bufor – zespół urządzeń przedsiębiorcy telekomunikacyjnego odpowiedzialnych za magazynowanie danych do czasu ich przekazania do systemu teleinformatycznego uprawnionego podmiotu.

5. Monitorowanie – dostęp do przekazów telekomunikacyjnych i związanych z nimi danych, o których mowa w art. 179 ust. 3 pkt 1 lit. a ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne.

IV. Interfejs LI HI

1. Wymagania ogólne

1.1. W warstwie fizycznej stosowany jest interfejs standardu Ethernet 100/1000BASE-T zgodny z IEEE 802.3ab. Do obsługi każdego z uprawnionych podmiotów przewidziany jest oddzielny port w standardzie Ethernet, z zastrzeżeniem pkt 1.8.

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 pomiędzy ADMF a LEMF jest siecią wydzieloną (w ramach sieci WAN), za którą odpowiada LEA. Wybór protokołu, o którym mowa w pkt 1.2, dostosowanie przesyłanych informacji oraz szyfrowanie sygnału na łączach sieci WAN leży w gestii 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 numer LIID.

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

1.7. System LEMF w wiadomościach interfejsu LI HI używa poniżej zdefiniowanego formatu LIID. Numer LIID składa się z dwóch członów: LEAID + SEQ (kolejny niepowtarzalny numer). 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	MF	Ministerstwo Finansów
07	CBA	Centralne Biuro Antykorupcyjne

1.8. Dopuszcza się wykorzystanie jednego portu do obsługi więcej niż jednego uprawnionego podmiotu. Wykorzystanie takiego rozwiązania ustala się na etapie uzgadniania zasad współpracy poprzez interfejs pomiędzy przedsiębiorcą telekomunikacyjnym i zainteresowanymi LEA.

2. Wymagania dla interfejsu HI1

2.1. Interfejs HI1 zapewnia:

a) przekazywanie do ADMF zleceń w zakresie włączania, modyfikacji i wyłączania monitorowania obiektów oraz zapytań o status obserwacji,

b) przekazywanie od ADMF do LEMF informacji o statusie realizacji zleceń, zapytań oraz występowaniu awarii,

c) możliwość realizacji podstawowych testów diagnostycznych tego interfejsu,

d) w pełni automatyczną realizację zleceń przekazywanych od LEMF, bez udziału pracowników przedsiębiorcy telekomunikacyjnego, z zastrzeżeniem pkt 2.15.

2.2. W celu aktywacji każdego zlecenia monitoringu, LEA określa:

a) numer LIID,

b) obiekt monitorowania,

c) monitorowaną usługę,

d) zakres monitorowania,

e) okres monitorowania.

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

a) numer abonenta PSTN/ISDN/MSISDN/VoIP,

b) IMSI,

c) numer IMEI o długości 15 cyfr, zgodny z ETSI ETS 300 927,

d) LOGIN,

e) adres IP,

f) adres MAC,

g) ESN/MEID.

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

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

b) transmisji pakietowej w ruchomych publicznych sieciach telefonicznych, zwanych dalej „sieciami ruchomymi”,

c) dostępu do sieci internet,

d) VoIP.

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

a) IRI – przesyłanie informacji związanych z objętymi monitorowaniem przekazami telekomunikacyjnymi oraz opcjonalnie treści SMS,

b) IRI+CC – przesyłanie informacji związanych z objętymi monitorowaniem przekazami telekomunikacyjnymi oraz treści monitorowanych przekazów telekomunikacyjnych.

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

2.7. Zlecenie modyfikacji monitorowania obejmuje:

a) czas jej wyłączenia,

b) włączenia/wyłączenia trybu online w odniesieniu do usług sieci ruchomych.

2.8. System monitoringu przedsiębiorcy telekomunikacyjnego przesyła do systemu LEMF informację o czasie faktycznego wykonania polecenia aktywacji,

deaktywacji 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 uprawnionych podmiotów informacje o objętych awarią numerach LIID, które znajdują się w jego dyspozycji.

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

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

2.12. Zlecenia wystawiane przez użytkownika LEMF, za 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 wykorzystywane są certyfikaty określone w ETSI TS 102 280, z uwzględnieniem wymagań technicznych zawartych w aktach wykonawczych wydanych na podstawie art. 10 ust. 4, art. 17 ust. 2 i art. 18 ust. 3 ustawy z dnia 18 września 2001 r. o podpisie elektronicznym (Dz. U. Nr 130, poz. 1450, z 2002 r. Nr 153, poz. 1271, z 2003 r. Nr 124, poz. 1152 i Nr 217, poz. 2125, z 2004 r. Nr 96, poz. 959, z 2005 r. Nr 64, poz. 565, z 2006 r. Nr 145, poz. 1050, z 2009 r. Nr 18, poz. 97, z 2010 r. Nr 40, poz. 230 i Nr 182, poz. 1228 oraz z 2011 r. Nr 106, poz. 622), oraz PKI.

2.14. Szczegółowa specyfikacja elementów interfejsu HI1 przedstawiona jest w pkt VI.

2.15. Za zgodą uprawnionego podmiotu dopuszcza się pracę interfejsu HI1 w trybie półautomatycznym, w którym pracownik przedsiębiorcy telekomunikacyjnego spełniający wymagania określone w art. 179 ust. 4b 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 przekazywane są do LEMF niezwłocznie, jednak nie później niż 10 minut od zakończenia przekazu. Raporty dotyczące zdarzeń występujących w danej sesji komunikacyjnej powinny być wysyłane w kolejności wystąpienia tych zdarzeń.

3.2. Przesyłanie do LEMF informacji związanych z objętymi monitorowaniem przekazami telekomunikacyjnymi odbywa się z wykorzystaniem protokołu FTP zdefiniowanym w IETF RFC 959 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 posiada dodatkowe rozszerzenie .tmp (<LIID>_<seq>.<ext>.tmp).

3.6. Zawartości plików (dane IRI) kodowane są w formacie ASN.1/BER zgodnie z:

a) ETSI ES 201 671 w odniesieniu do usług świadczonych w sieciach ruchomych oraz usług transmisji pakietowej świadczonych w sieciach ruchomych,

b) 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”,

c) ETSI TS 102 232-1 i ETSI TS 102 232-3 w odniesieniu do usług dostępu do Internetu,

d) ETSI TS 102 232-1 i ETSI TS 102 232-5 w odniesieniu do usług telefonii internetowej.

3.7. Specyfikacja interfejsu HI2 jest rozszerzona o parametr ExtendedPartyIdentity. Specyfikacja struktur danych w notacji ASN.1 opisujących ten parametr znajduje się w pkt VII.

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, system monitoringu przedsiębiorcy telekomunikacyjnego 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 nie później niż 10 minut od zakończenia przekazu.

4.2. Korelacja pomiędzy rekordami IRI (HI2) a przekazywaną treścią komunikacji CC (HI3) odbywa się z wykorzystaniem numeru LIID, a w przypadku usług sieci z komutacją kanałów również parametru CIN.

4.3. Do przekazywania treści komunikacji objętych monitorowaniem, dla usług sieci ruchomych stosuje się:

a) dla trybu offline:

– protokół FTP zdefiniowany w IETF RFC 959 na zasadach określonych w ETSI ES 201 671,

– w przypadku połączeń głosowych zapis treści przekazów może być realizowany na dwa sposoby. W pierwszym sposobie dla każdego z kierunków (w kierunku od i do obiektu monitorowanego) tworzony jest odrębny plik (tryb „stereo”). W drugim sposobie oba kierunki transmisji zapisywane są w ramach jednego pliku – oba kierunki połączenia są ze sobą zmiksowane w jeden strumień (tryb „mono”),

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

gdzie:

LIID – identyfikator celu LIID

CIN – Communication Identity Number

ext – rodzaj zawartej informacji, gdzie:

– 2 oznacza CC (od monitorowanego obiektu),

– 4 oznacza CC (do monitorowanego obiektu),

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

- nazwa przesyłanego pliku jest zmieniana na docelową po udanym nagraniu; plik tymczasowy posiada dodatkowe rozszerzenie .tmp (<LIID>_<CIN>.<ext>.tmp),
- przedsiębiorca telekomunikacyjny nieodpłatnie dostarcza uprawnionemu podmiotowi kodeki umożliwiające odczyt plików audio i wideo oraz innych formatów danych i plików stosowanych przez przedsiębiorcę telekomunikacyjnego,

b) dla trybu online:

- przekazy telekomunikacyjne wysyłane i odbierane przez monitorowany obiekt ADMF przesyła do LEMF w czasie rzeczywistym,
- do przesyłania przekazów stosuje się protokół SIP zgodny z IETF RFC 3261,
- format pola Call-ID w nagłówku SIP przyjmuje postać LIID_cin,
- przedsiębiorca telekomunikacyjny nieodpłatnie dostarcza uprawnionemu podmiotowi kodeki umożliwiające odbiór połączeń głosowych i wideo,
- adres docelowy SIP określany jest na podstawie parametru *forwardingAddress*, który LEA określa za pomocą interfejsu HI1.

4.4. Dopuszcza się przekazywanie treści komunikacji objętej 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 komunikacji objętych monitorowaniem stosuje się protokół GLIC z zastosowaniem zasad określonych w ETSI ES 201 671.

4.6. Przekazywanie treści komunikacji objętej 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 komunikacji objętej monitorowaniem jest realizowane zgodnie z zasadami określonymi w ETSI TS 102 232-1 i ETSI TS 102 232-3.

4.8. W przypadku usług telefonii internetowej, przekazywanie treści komunikacji objętej 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 komunikatów do LEMF system monitoringu przedsiębiorcy telekomunikacyjnego usuwa je ze swoich zasobów.

4.10. Interfejs HI3 nie wymaga stosowania podpisu elektronicznego.

V. Interfejs HI A-B

1. Interfejs systemu monitoringu przedsiębiorcy telekomunikacyjnego dostępny jest w jednym punkcie (lokalizacji) dla wszystkich uprawnionych podmiotów. Do obsługi każdego z uprawnionych podmiotów przewidziany jest oddzielny port w standardzie Ethernet.
2. W warstwie fizycznej stosowany jest interfejs standardu Ethernet 100/1000BASE-T, zgodny z IEEE 802.3ab.
3. Protokołem warstwy sieciowej interfejsu HI A-B jest protokół IPv4, zgodny z IETF RFC 0791, lub protokół IPv6, zgodny z IETF RFC 2460 i IETF RFC 4291. Stosuje się publiczne adresy IP.
4. Stosuje się mechanizm podpisu elektronicznego.
5. Realizacja interfejsu HI A-B jest zgodna z ETSI TS 102 657.
6. Dla realizacji komunikacji w interfejsie HI A-B stosuje się wariant określony w ETSI TS 102 657 (pkt 7.3), gdzie:
   a) w warstwie transportowej stosowany jest protokół TCP,
   b) stosowane jest kodowanie elementów informacyjnych w formacie ASN.1/BER.
7. Wartość parametru cSPID odpowiada identyfikatorowi przypisanemu danemu przedsiębiorcy w Rejestrze przedsiębiorców telekomunikacyjnych.
8. Pole „*countryCode*” w parametrze „*RequestID*” przyjmuje wartość „*PL*”.
9. Pole „*authorisedOrganisationID*” w parametrze „*RequestID*” przyjmuje wartość zgodnie z przypisaniem LEAID, według tabeli nr 2 w pkt IV.1.7.
10. Nie stosuje się niżej wymienionych rozwiązań opcjonalnych:
    a) priorytetów dla obsługi żądań skierowanych przez LEA „*RequestPriority”,* zgodnie z ETSI TS 102 657 (pkt A.2.2.1),
    b) mechanizmu „*multi-part delivery”,* zgodnie z ETSI TS 102 657 (pkt 5.1.7),
    c) trybu *„Authorized-Organization-initiated”,* zgodnie z ETSI TS 102 657 (pkt 5.3).

11. Niewykorzystywane są elementy informacyjne wymienione w tabeli nr 3.

Tabela nr 3

Punkt w normie ETSI TS 102 657 0	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

VI. Struktura interfejsu HI1

1. Warstwa transportowa

1.1. Stosowany jest protokół TCP.

1.2. Zestawiane są połączenia TCP w kierunkach:

a) ADMF/MF/DF ► LEMF (HI1LEMFOperations),

b) LEMF ► ADMF/MF/DF (HI1ADMFOperations).

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

2. Warstwa aplikacyjna

Wiadomości wysyłane w warstwie aplikacyjnej zostały zdefiniowane w notacji ASN.1 i są kodowane w standardzie BER lub DER.

2.1. Opis

2.1.1. Przeznaczenie: aktywacje, dezaktywacje i modyfikacje dedykacji, zapytania o dedykacje, alarmy, raporty, status interfejsu.

2.1.2. Stosowane są dwa protokoły zdefiniowane w ASN.1:

a) HI1LEMFOperations – operacje inicjowane przez LEMF,

b) HI1ADMFOperations – alarmy i powiadomienia wysyłane przez ADMF.

2.1.3. Operacje, o których mowa w pkt 2.1.2, są całkowicie od siebie niezależne.

2.1.4. Każda operacja/zapytanie to jedna sesja TCP.

2.1.5. Każde zapytanie jest potwierdzane przez drugą stronę.

2.2. Protokół HI1LEMFOperations

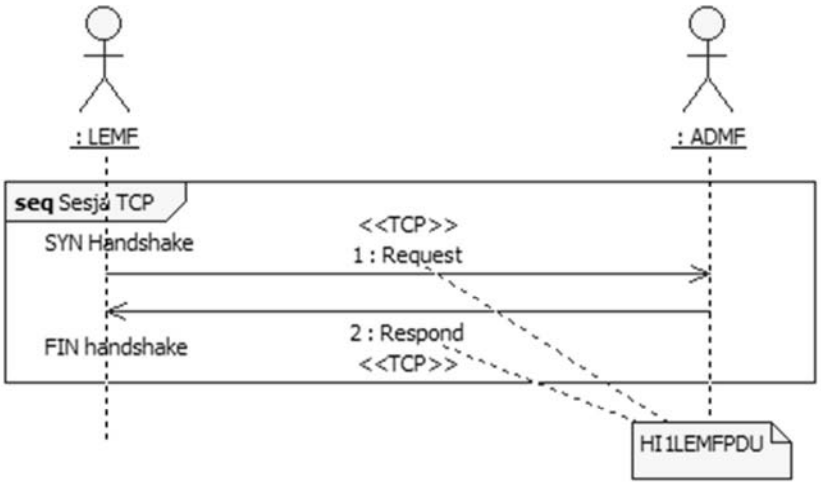
2.2.1. Operacje wykonywane przez LEMF:

a) zapytanie proste:
- Hello,
- ListRequest,
- RTRequest – żądanie włączenia lub wyłączenia trybu online (dotyczą tylko obserwacji rozpoczętych),

b) zapytania podpisane:
- Activate,
- Modificate, z wyłączeniem w odniesieniu do włączania/wyłączania trybu online,
- 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 rys. 1.



Rys. 1. Schemat operacji

2.2.3. LEMF czeka na odpowiedź 10 sekund. Po 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 posiada określony czas zakończenia obserwacji. Przesunięcie momentu zakończenia obserwacji ponad ten czas wymaga zlecenia modyfikacji.

2.2.5. System monitoringu przedsiębiorcy telekomunikacyjnego 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 ze wszystkimi tego konsekwencjami odnotowany w logach systemu.

2.2.8. Modyfikacji podlegają jedynie zlecenia, które nie zakończyły się. Modyfikować można czasy zakończenia obserwacji oraz typ monitoringu (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:

a) Request – definiujące zapytania wysyłane przez LEMF,

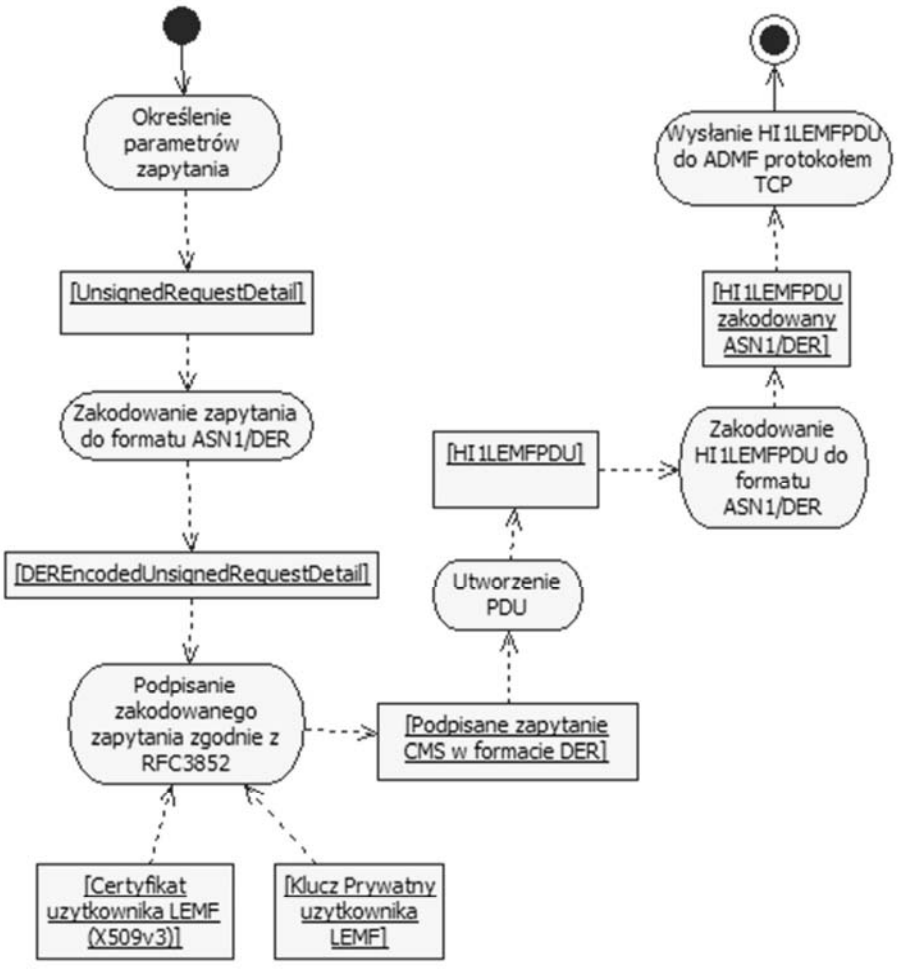
b) Respond – odpowiedzi ADMF'a na wysłane żądania LEMF.

2.2.10. Dopuszczalne są następujące interakcje pomiędzy LEMF a ADMF:

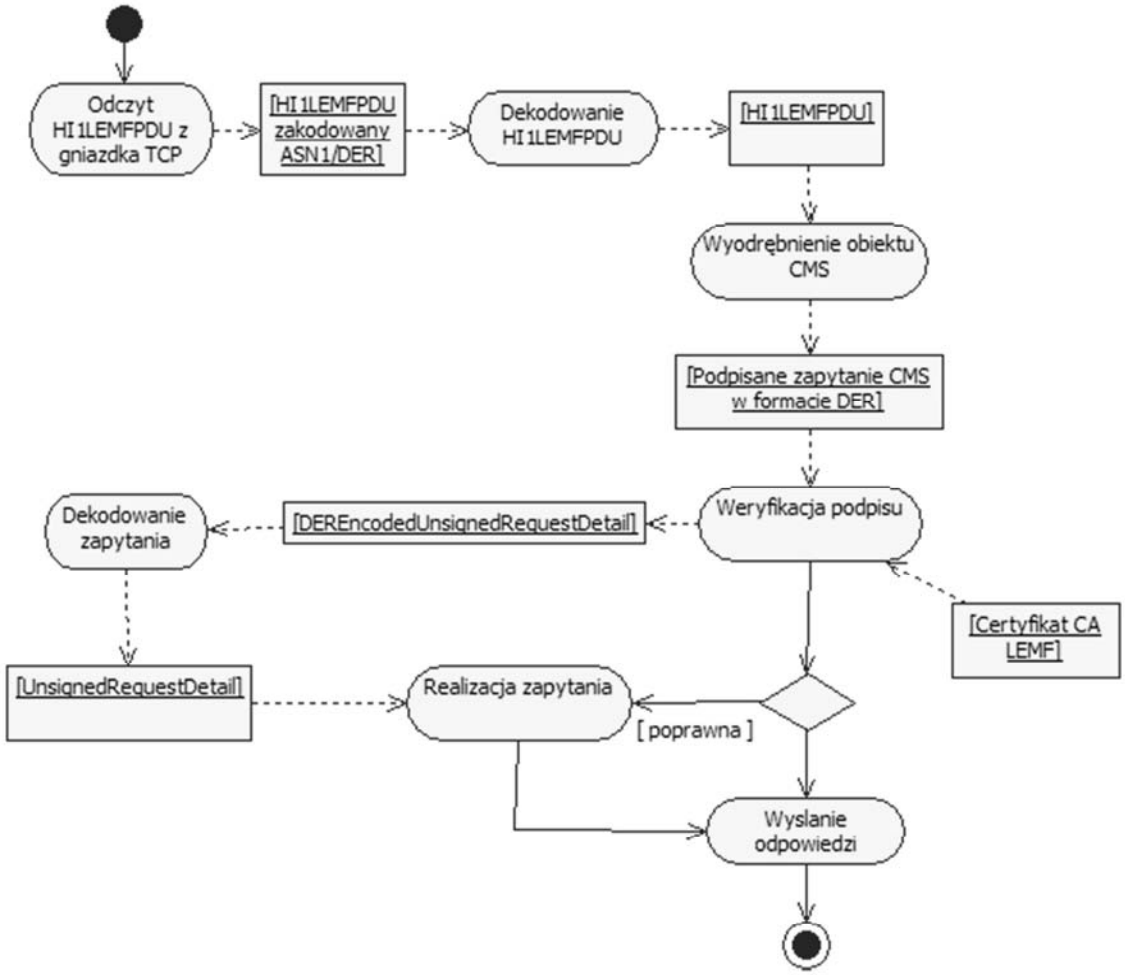
Zapytanie LEMF	Odpowiedź ADMF	Alternatywna odpowiedź
SignedRequest	GeneralRespond	
HelloRequest	GeneralRespond	
ListRequest	ListRespond	GeneralRespond
RTRequest	GeneralRespond	

2.2.11. Zapytania podpisane (SignedRequest)

Sposób tworzenia i weryfikacji wiadomości podpisanych za pomocą diagramów aktywności przedstawiony jest na rys. 2 i rys. 3.



Rys. 2. Tworzenie podpisanego zapytania



Rys. 3. Weryfikacja podpisanego zapytania

2.2.12. Uwagi:

a) CMS (Cryptographic Message Syntax 2004): format binarny dokumentu z podpisem (z użyciem kodowania DER) stanowi podzbiór CMS. Dokładna specyfikacja przedstawiona jest w dokumencie IETF RFC 3852.

b) identyfikator obiektu OID definiujący standard w notacji ASN.1:

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

c) UnsignedRequestDetail:
Struktura opisująca szczegóły zapytania aktywacji, modyfikacji i deaktywacji dedykacji. Po zakodowaniu do postaci DER jest podpisywana zgodnie ze specyfikacją przedstawioną w dokumencie IETF RFC 2315. Struktura UnsignedRequestDetail przedstawiona jest na rys. 6.

d) Service:

Obiekt reprezentujący usługi świadczone przez operatora.

e) monitorowane są następujące usługi:

- CS Circuit Switched (Mobile),
- PS PacketSwitched,
- InternetAccess,
- InternetTelephony,
- CS Circuit Switched (Fixed).

2.3. Protokół HI1ADMFOperations

2.3.1 Operacje wykonywane przez ADMF:

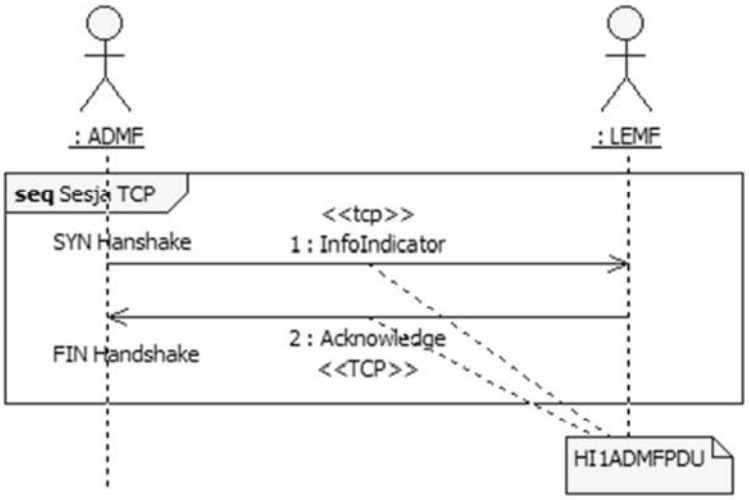
a) Alarmy,

b) Notyfikacje.

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

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

b) Acknowledge – potwierdzenia otrzymania wiadomości przez ADMF.



Rys. 4. Schemat operacji

2.3.3 Dopuszczalne są następujące interakcje pomiędzy ADMF a LEMF:

Wiadomość ADMF	Odpowiedź LEMF
HelloRequest	GeneralRespond
AlarmIndicator	GeneralRespond
NotificationIndicator	GeneralRespond

2.3.4 Uwagi:

a) wyróżnia się dwa typy wiadomości wysyłanych przez ADMF: alarmy i notyfikacje,

b) każda wysłana wiadomość (InfoIndicator) jest potwierdzana przez LEMF (Acknowledge),

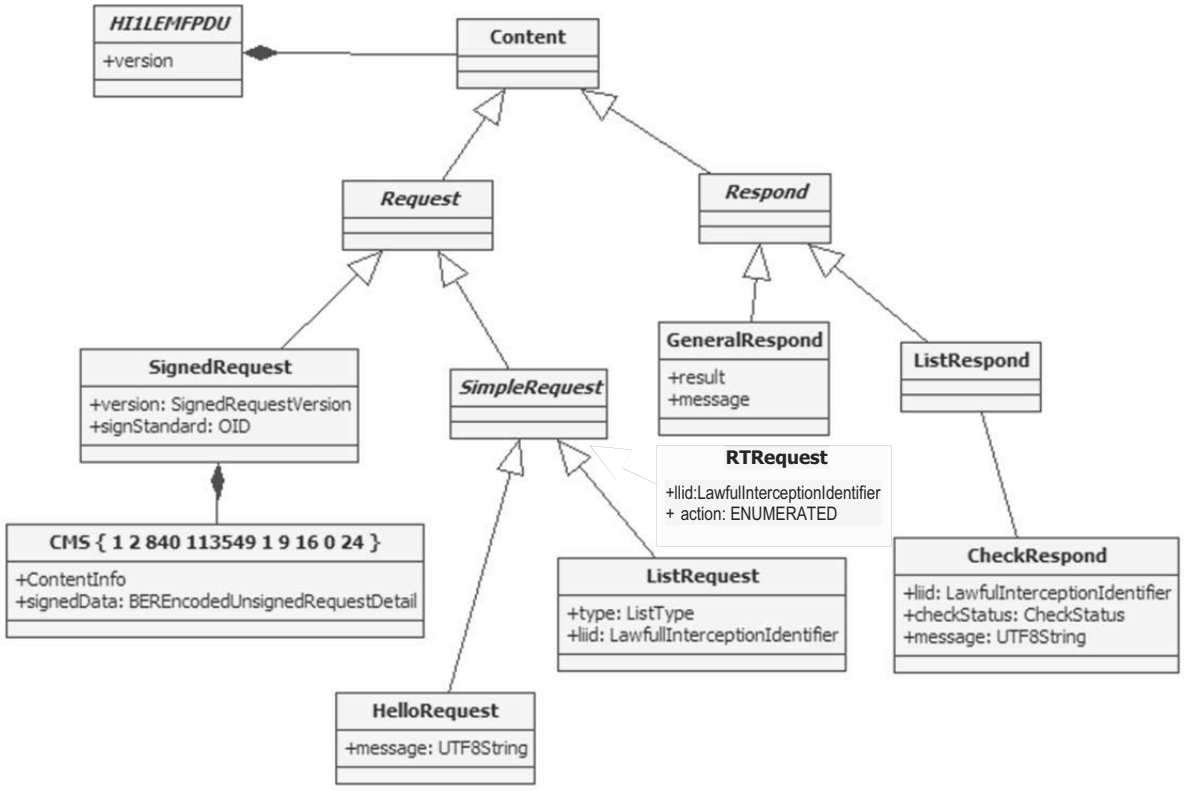
c) potwierdzenie jest realizowane w czasie 5 sekund,

d) alarmy posiadają dwa stany: włączony, wyłączony (pole status),

e) wiadomość wyłączająca alarm może zawierać tylko jego identyfikator (identity).

3. HI1LEMFPDU

3.1 Struktura HI1LEMFPDU



Rys. 5. Struktura HI1LEMFPDU

3.2 Specyfikacja ASN.1 dla 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
  ...
}
```

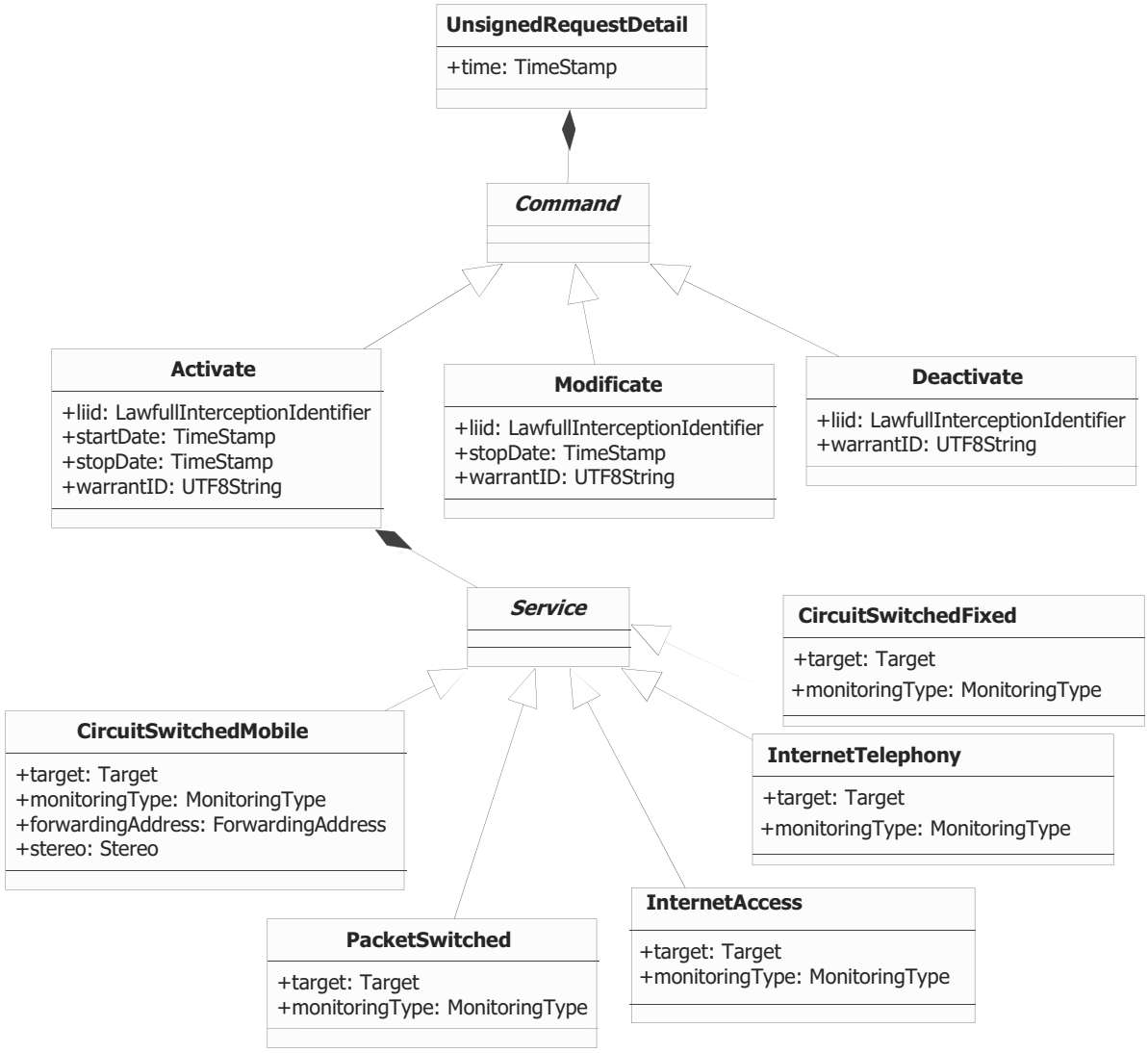
```
Request ::= CHOICE
{
  simpleRequest [1] SimpleRequest,
  signedRequest [2] SignedRequest,
  ...
}

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



Rys. 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
```

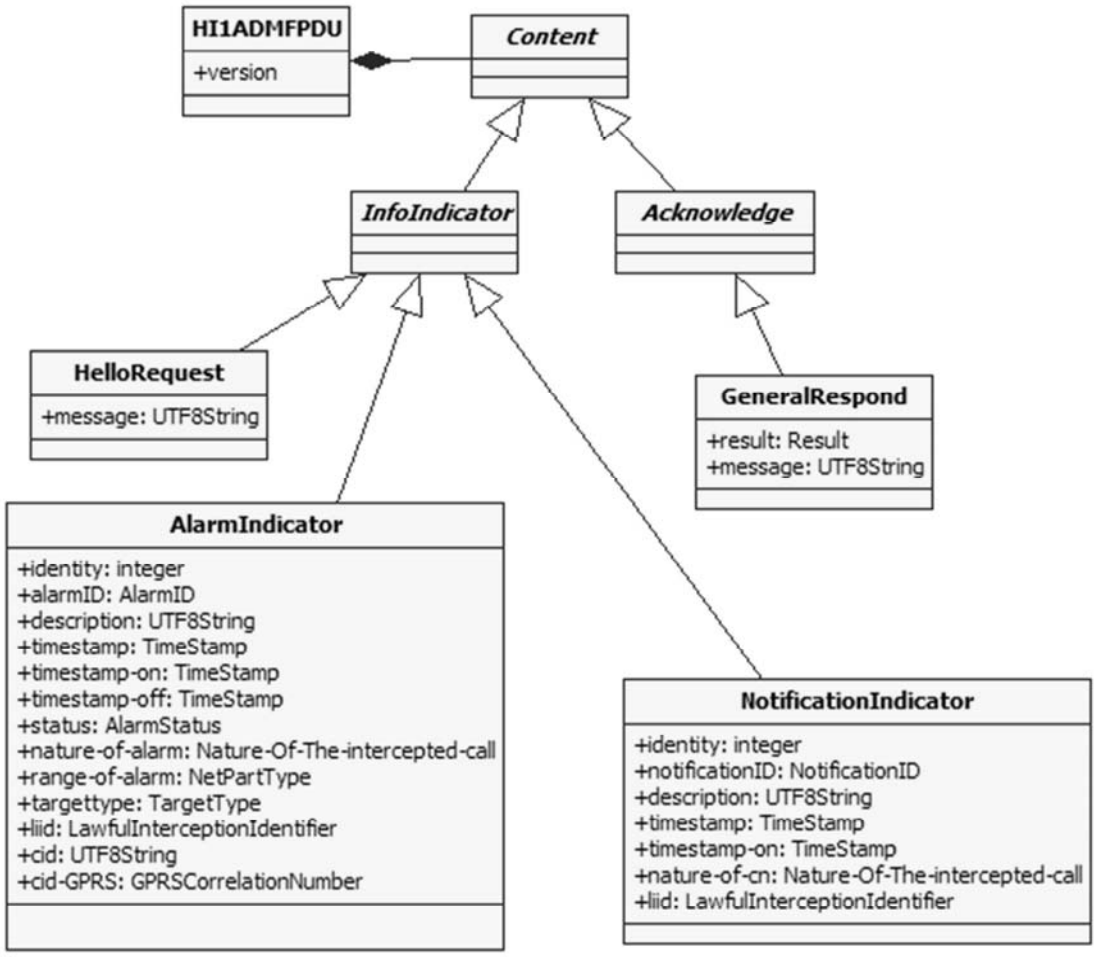
```
{
  target [1] Target,
  monitoringType [2] MonitoringType,
  ...
}

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. HI1ADMFPDU

5.1. Struktura HI1ADMFPDU



Rys. 7. Struktura HI1ADMFPDU

5.2. Specyfikacja ASN.1 dla 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
```

VII. 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
}
```