PROJEKT

17 czerwca 2011 r.

ROZPORZĄDZENIE RADY MINISTRÓW

z dnia ..... 2011 r.

w sprawie wymagań technicznych i eksploatacyjnych dla interfejsów umożliwiających wykonywanie zadań i obowiązków na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego

Na podstawie art. 182 ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.[1)]) zarządza się, co następuje:

§ 1. 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 nr 1 do rozporządzenia.

2. Wymagania w zakresie specyfikacji elementów interfejsu HI1 oraz formatu parametru ExtendedPartyIdentity określa załącznik nr 2 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

[1)] 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.

UZASADNIENIE

Projekt rozporządzenia jest wykonaniem upoważnienia zawartego w art. 182 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.), zwanej dalej „ustawą".

Powyższe upoważnienie ustawowe zobowiązuje Radę Ministrów do określenia wymagań technicznych i eksploatacyjnych dla interfejsów, o których mowa w art. 179 ust. 4a ustawy, 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. Zagadnienia objęte zakresem regulacji projektowanego rozporządzenia mają zostać unormowane z zastosowaniem zasady minimalizacji nakładów przedsiębiorcy telekomunikacyjnego i podmiotów uprawnionych.

Zgodnie z art. 179 ust. 4a ustawy zastosowanie rozwiązania technicznego opartego o interfejs, jest tylko jedną z możliwości wykonywania przez przedsiębiorców telekomunikacyjnych zadań i obowiązków na rzecz obronności i bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego. Nie jest natomiast obligatoryjnym wymogiem ustawodawcy.

Zastosowanie interfejsu powinno wynikać z zasady minimalizacji nakładów przedsiębiorcy telekomunikacyjnego, podmiotów uprawnionych i mieć miejsce tylko w tym przypadku, kiedy przyniesie to obu zainteresowanym stronom wymierne korzyści. Ewentualny wybór przez przedsiębiorcę telekomunikacyjnego tej metody realizacji jego ustawowych obowiązków jest więc uzależniony nie tylko od jego chęci, ale także od wyrażenia zgody przez uprawnione podmioty.

W projekcie w § 2 proponuje się rozwiązanie mające na celu realizację zasady minimalizacji nakładów przedsiębiorcy telekomunikacyjnego i uprawnionego podmiotu, co stanowi realizację wytycznych zawartych w upoważnieniu do wydania rozporządzenia. Polega ono na uwzględnieniu umów, które zawierane są pomiędzy przedsiębiorcą telekomunikacyjnym a uprawnionym podmiotem na podstawie art. 179 ust. 4a ustawy - Prawo telekomunikacyjne. Przedsiębiorcy telekomunikacyjni, którzy zawarli takie umowy przed dniem wejścia w życie rozporządzenia, nie muszą dostosowywać swoich interfejsów do wymagań zawartych w rozporządzeniu. Wpłynie to również korzystanie na budżety uprawnionych podmiotów, które będą korzystać z dotychczasowych rozwiązań.

W chwili obecnej nie ma żadnego aktu prawnego regulującego standardy dla realizacji interfejsów. Unormowanie prawne przedmiotowej kwestii jest konieczne dla zapewnienia odpowiednim służbom, właściwych warunków dla realizacji ich zadań związanych z pracą operacyjną. Stosowane aktualnie rozwiązania opierają się na metodach przyjętych w sieciach operatorów telefonii ruchomej (Polkomtel, PTC, PTK Centertel), określonych w dokumencie pt: *„Specyfikacja Interfejsu LI HI na styku między systemem operatora telefonii ruchomej umożliwiającym realizację dostępu do wybranych treści przekazów telekomunikacyjnych (ADMF/DF), a systemem uprawnionego podmiotu umożliwiającym dostęp do wybranych treści przekazów telekomunikacyjnych (LEMF)"*. Rozwiązania interfejsów LI HI są stosowane tylko u operatorów telefonii ruchomej. Nie są obecnie używane w sieci żadnego z innych operatorów (telefonia stacjonarna, dostęp do internetu). Interfejs dla retencji HI A-B również nie jest stosowany w sieci żadnego z krajowych operatorów.

Zastosowanie interfejsów zmierza do stopniowego wprowadzenia elektronicznego dostępu do danych telekomunikacyjnych będących w posiadaniu przedsiębiorcy telekomunikacyjnego. Z uwagi na fakt, że dane te będą niejednokrotnie obejmować tysiące pojedynczych rekordów, konieczne jest aby dane te przekazywane były w postaci elektronicznej. Postać elektroniczna przekazywanych danych niesie ze sobą wiele korzyści. Są to między innymi: łatwość

archiwizacji danych, łatwe przeszukiwanie i analiza danych (z wykorzystaniem systemów informatycznych), łatwość przesyłania danych. Dlatego istnieje konieczność wskazania jednolitego dla wszystkich przedsiębiorców telekomunikacyjnych formatu danych, który mógłby być wykorzystywany do tego celu. Dodatkowo powinny istnieć ogólnodostępne narzędzia umożliwiające konwersje przesyłanych przez operatora danych do wymaganego formatu oraz pozwalające na tworzenie podmiotom uprawnionym aplikacji analizujących dane otrzymane w tym formacie. Formatem spełniającym powyższe wymagania jest ASN.1. Jest on wspierany przez wiele systemów baz danych oraz istnieje wiele komercyjnych i darmowych narzędzi do jego generowania, weryfikowania i analizy. Dokumenty ASN.1 pozwalają także na szybkie zweryfikowanie ich poprawności. Rozwiązanie to wymusza na przedsiębiorcach telekomunikacyjnych digitalizację wszystkich posiadanych danych (w tym danych, o których mowa w art. 161 ustawy), co biorąc pod uwagę charakter wykonywanej działalności, nie powinno za sobą nieść nadmiernych kosztów ani powodować trudności technicznych.

Przy konstruowaniu projektu rozporządzenia przyjęto generalną zasadę odwołań do istniejących międzynarodowych zaleceń oraz dokumentów normalizacyjnych, głównie Europejskiego Instytutu Norm Telekomunikacyjnych ETSI. Uwzględniono również - celem minimalizacji kosztów - uwarunkowania istniejące w Polsce, w tym cechy charakterystyczne krajowych rozwiązań interfejsów. W przypadku, gdy rozwiązania krajowe wymagają specyficznego podejścia, dokonano szczegółowego wskazania wymagań technicznych. W sytuacji, gdy normy międzynarodowe nie odnoszą się do konkretnego rozwiązania oraz w Polsce jeszcze go nie wykorzystywano (np. w przypadku przechwytywania strumieni wideo), zaproponowano stosowne zapisy.

Wymagania techniczne i eksploatacyjne dla interfejsów, o których mowa w art. 179 ust. 4a ustawy zostały określone w załącznikach do projektowanego rozporządzenia. Proponowane rozwiązania mają na celu umożliwienie podmiotom uprawnionym, którymi są: Policja, Straż Graniczna, Agencja Bezpieczeństwa Wewnętrznego, Służba Kontrwywiadu Wojskowego, Żandarmeria Wojskowa, Centralne Biuro Antykorupcyjne i wywiad skarbowy, dostępu do: przekazów telekomunikacyjnych, nadawanych lub odbieranych przez użytkownika końcowego lub telekomunikacyjne urządzenie końcowe oraz posiadanych przez przedsiębiorcę danych związanych z przekazami telekomunikacyjnymi oraz dostępu do zatrzymywanych danych, które są generowane lub przetwarzane w sieci telekomunikacyjnej.

Ponadto, zgodnie z art. 180d ustawy - Prawo telekomunikacyjne, przedsiębiorcy telekomunikacyjni udostępniają uprawnionym podmiotom, a także sądowi i prokuratorowi[2], przetwarzane przez siebie dane, o których mowa w art. 159 ust. 1 pkt 1 i pkt 3-5, w art. 161 oraz w art. 179 ust. 9 ustawy - Prawo telekomunikacyjne, związanych ze świadczoną usługą telekomunikacyjną.

Szczególnego wyjaśnienia wymaga odwołanie się w definicji obiektu monitorowanego do zarządzeń odpowiednich organów uprawnionych podmiotów wydanych na podstawie odrębnych przepisów. Przepisy takie zawierają ustawy kompetencyjne dotyczące poszczególnych uprawnionych podmiotów.

Zgodnie z tymi przepisami, w przypadkach niecierpiących zwłoki, jeżeli mogłoby to spowodować utratę informacji lub zatarcie albo zniszczenie dowodów przestępstwa, odpowiedni organ uprawnionego podmiotu może zarządzić, po uzyskaniu pisemnej zgody

[2] W związku z art. 6 projektu ustawy zmianie ustawy o grach hazardowych oraz niektórych innych ustaw (druk sejmowy nr 3860), uprawniona do pozyskiwania danych, o których mowa w art. 180a i 180d ustawy - Prawo telekomunikacyjne będzie również Służba Celna.

prokuratora, kontrolę operacyjną, zwracając się jednocześnie do właściwego sądu, z wnioskiem o wydanie postanowienia w tej sprawie.

Projekt rozporządzenia przewiduje okres 3 - miesięcznego *vacatio legis*. Pomimo, że stosowanie interfejsów nie jest obligatoryjne, taki okres *vacatio legis* pozwoli na uporządkowanie spraw związanych z trwającymi obecnie negocjacjami dotyczącymi umów pomiędzy przedsiębiorcami telekomunikacyjnymi a uprawnionymi podmiotami. Prowadzone do tej pory negocjacje nie przewidywały wymagań, o których mowa w rozporządzeniu.

Przedmiotowy projekt podlega notyfikacji zgodnie z trybem przewidzianym w przepisach dotyczących sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych.

Projekt został opublikowany na stronach Biuletynu Informacji Publicznej Ministerstwa Infrastruktury zgodnie z przepisami ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie tworzenia prawa (Dz. U. Nr 169, poz. 1414).

Przedmiot projektowanego aktu prawnego nie jest objęty prawem Unii Europejskiej.

OCENA SKUTKÓW REGULACJI

I. Podmioty, na które oddziałuje rozporządzenie.

Do podmiotów, na które oddziałuje projektowane rozporządzenie należą:

1) przedsiębiorcy telekomunikacyjni wpisani do rejestru prowadzonego przez Prezesa Urzędu Komunikacji Elektronicznej,

2) podmioty uprawnione w rozumieniu ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.): Policja, Straż Graniczna, Agencja Bezpieczeństwa Wewnętrznego, Centralne Biuro Antykorupcyjne, Służba Kontrwywiadu Wojskowego, Żandarmeria Wojskowa, wywiad skarbowy, oraz sądy i prokuratura[3].

II. Konsultacje społeczne.

W ramach konsultacji społecznych projekt został przedstawiony do zaopiniowania branżowym izbom zrzeszającym przedsiębiorców telekomunikacyjnych. Zasadnicze uwagi zgłoszone przez przedsiębiorców telekomunikacyjnych zrzeszonych w Polskiej Izbie Informatyki i Telekomunikacji, Polskiej Konfederacja Pracodawców Prywatnych Lewiatan oraz Pracodawcach Rzeczpospolitej Polskiej, które mogłyby mieć wpływ na wzrost kosztów budowy lub rozbudowy interfejsów, dotyczyły:

1) braku możliwości zwolnienia przedsiębiorców telekomunikacyjnych, którzy już posiadają zawarte umowy z podmiotami uprawnionymi na udostępnianie treści przekazów telekomunikacyjnych za pośrednictwem interfejsów, z obowiązku posiadania rozwiązania zgodnego z proponowaną w nowelizacji specyfikacją interfejsu.

   Dodano § 2, w którym proponuje się rozwiązanie mające na celu realizację zasady minimalizacji nakładów przedsiębiorcy telekomunikacyjnego i uprawnionego podmiotu. Polega ono na uwzględnieniu umów, które zawierane są pomiędzy przedsiębiorcą telekomunikacyjnym a uprawnionym podmiotem na podstawie art. 179 ust. 4a ustawy - Prawo telekomunikacyjne. Przedsiębiorcy telekomunikacyjni, którzy zawarli takie umowy przed dniem wejścia w życie rozporządzenia, nie muszą dostosowywać swoich interfejsów do wymagań zawartych w rozporządzeniu.

2) zbyt krótkiego *vacatio legis*; proponowany przez przedsiębiorców okres to 36 miesięcy.

   Biorąc pod uwagę treść nowego § 2, wprowadzonego na wniosek przedsiębiorców telekomunikacyjnych oraz fakt, że stosowanie interfejsów nie jest obligatoryjne, zmieniono okres *vacatio legis* na 3 miesięczny, co pozwoli na uporządkowanie spraw związanych z trwającymi obecnie negocjacjami dotyczącymi umów pomiędzy przedsiębiorcami telekomunikacyjnymi a uprawnionymi podmiotami .

3) braku technicznej możliwości automatycznego informowania przez system monitoringu przedsiębiorcy telekomunikacyjnego o objętych awarią numerach LIID.

---

[3] W związku z art. 6 projektu ustawy zmianie ustawy o grach hazardowych oraz niektórych innych ustaw (druk sejmowy nr 3860), uprawniona do pozyskiwania danych, o których mowa w art. 180a i 180d ustawy - Prawo telekomunikacyjne będzie również Służba Celna.

Przychylono się do opinii przedsiębiorców telekomunikacyjnych i zaproponowano, aby informacje o awariach były przekazywane nieautomatycznie, tzn przez przedsiębiorcę telekomunikacyjnego, a nie przez system.

4) w trakcie spotkania konsultacyjnego przedstawiciel Pracodawców RP zgłosił „formalny" wniosek o wstrzymanie dalszych prac nad projektem rozporządzenia do czasu podpisania rozporządzenia wydanego na podstawie art. 179 ust. 12 ustawy - Prawo telekomunikacyjne.

   Ze względu na harmonogram prac legislacyjnych rządu, nie jest możliwe wstrzymanie prac nad rozporządzeniem art. 182. Projekt rozporządzenia art. 179 ust. 12 znajduje się na etapie uzgodnień wewnątrzresortowych i wkrótce zostanie przesłany do konsultacji społecznych.

Pozostałe uwagi dotyczyły kwestii technicznych. Uwagi te omówiono na spotkaniu konsultacyjnym z udziałem przedstawicieli uprawnionych podmiotów.

III. Wpływ na sektor finansów publicznych, w tym na budżet państwa i budżety jednostek samorządu terytorialnego.

Zastosowanie interfejsów dla prowadzenia kontroli operacyjnej przez uprawnione podmioty wiąże się z koniecznością ponoszenia przez nie kosztów budowy i eksploatacji części systemu uprawnionego monitoringu, znajdującego się po ich stronie i spowoduje dodatkowe skutki finansowe dla budżetu państwa.

Koszty te można podzielić na dwie zasadnicze grupy:

I. Koszty budowy i instalacji systemów, w skład których wchodzą:

1) koszt zakupu i instalacji samego systemu monitoringu, tj. urządzeń służących do rejestracji i przechowywania uzyskanych z systemu przedsiębiorcy telekomunikacyjnego treści przekazów telekomunikacyjnych i powiązanych z nimi danych telekomunikacyjnych,

2) koszt zakupu i instalacji urządzeń służących do ochrony przekazywanych za pomocą sieci telekomunikacyjnych uzyskanych z systemu przedsiębiorcy telekomunikacyjnego treści przekazów telekomunikacyjnych i powiązanych z nimi danych telekomunikacyjnych na trasie przedsiębiorca telekomunikacyjny - uprawniony podmiot oraz pomiędzy rozproszonymi elementami systemu uprawnionego podmiotu (szyfratory),

3) koszt budowy lub dzierżawy sieci telekomunikacyjnych służących do transmisji uzyskanych z systemu przedsiębiorcy telekomunikacyjnego treści przekazów telekomunikacyjnych i powiązanych z nimi danych telekomunikacyjnych na trasie przedsiębiorca telekomunikacyjny uprawniony podmiot oraz pomiędzy rozproszonymi elementami systemu uprawnionego podmiotu, koszty budowy lub modernizacji infrastruktury budowlanej niezbędnej dla zapewnienia właściwych warunków eksploatacji systemu.

II. Koszty eksploatacji i modernizacji poszczególnych elementów interfejsu:

1) koszty serwisu firmy - producenta systemu. Jest to koszt stały stanowiący określony procent kosztu zakupu systemu ponoszony corocznie (około 10% sumy kontraktu). Na wysokość tego kosztu wpływa wymóg natychmiastowej reakcji serwisu na

wszelkie objawy nieprawidłowego działania systemu (wymagana jest całodobowa gotowość serwisu do podjęcia działań) oraz wynikające z ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz. 1228) wymagania w stosunku do producenta systemu i personelu serwisującego. Obejmują one koszty likwidacji ewentualnych awarii i usterek systemu oraz aktualizację zastosowanego oprogramowania,

2) koszty modernizacji systemu - ze względu na szybki postęp technologiczny w dziedzinie telekomunikacji, pojawianie się wciąż nowych publicznie dostępnych usług telekomunikacyjnych, systemy uprawnionego monitoringu (zarówno po stronie przedsiębiorcy telekomunikacyjnego, jak i uprawnionego podmiotu) wymagają stałej rozbudowy i modernizacji. Zgodnie z art. 179 ust. 3a ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne przedsiębiorca telekomunikacyjny jest obowiązany zapewnić warunki dostępu i utrwalania w zakresie wszystkich świadczonych usług telekomunikacyjnych od dnia rozpoczęcia działalności telekomunikacyjnej, a w przypadku rozpoczęcia świadczenia nowej usługi telekomunikacyjnej od dnia jej uruchomienia. Zapis ten obliguje przedsiębiorcę telekomunikacyjnego do stałej modernizacji i unowocześniania raz zbudowanego systemu, a tym samym uwzględniania w kosztach uruchomienia nowej usługi telekomunikacyjnej, także kosztów związanych z jego obowiązkami na rzecz obronności i bezpieczeństwa państwa oraz porządku publicznego. Działanie takie ma zapewnić uprawnionym podmiotom możliwość stosowania kontroli operacyjnej nawet w stosunku do użytkowników najnowszych i najbardziej zaawansowanych technicznie usług telekomunikacyjnych. Warunkiem skutecznej realizacji tych celów jest jednak stała modernizacja i rozbudowa systemów monitoringu uprawnionych podmiotów tak, aby były one w stanie przechwycić i przetworzyć uzyskane od przedsiębiorcy telekomunikacyjnego treści przekazów telekomunikacyjnych, przesyłanych przy pomocy nowych usług telekomunikacyjnych. Koszty takich prac są jednak trudne do oszacowania, gdyż na ich wysokość wpływa bezpośrednio szybkość i zakres zmian następujących na rynku usług telekomunikacyjnych,

3) koszty eksploatacji i modernizacji urządzeń szyfrujących przekaz informacji pomiędzy przedsiębiorcą telekomunikacyjnym i uprawnionym podmiotem oraz pomiędzy elementami systemu uprawnionego podmiotu. Ze względu na stały rozwój technik dekryptażu niezbędna jest systematyczna zmiana kluczy szyfrujących stosowanych w tych urządzeniach oraz modernizacja lub wymiana samych urządzeń szyfrujących tak, aby spełniały one wymagania Departamentu Bezpieczeństwa Teleinformatycznego Agencji Bezpieczeństwa Wewnętrznego, a tym samym posiadały aktualny certyfikat do określonej klauzuli niejawności (zależnej od stosującego je uprawnionego podmiotu).

Wielkość wymienionych grup kosztów w odniesieniu do konkretnego uprawnionego podmiotu zależy w dużym stopniu od zakresu jego ustawowych uprawnień, jego struktury organizacyjnej oraz ilości spraw, w których niezbędne jest wykorzystanie kontroli operacyjnej (lub ilości zapytań o dane telekomunikacyjne w przypadku interfejsu HI A-B).

W celu minimalizacji kosztów zarówno po stronie przedsiębiorcy telekomunikacyjnego, jak również po stronie uprawnionych podmiotów, proponuje się przepis § 2, który nie zobowiązuje do dostosowania do wymagań rozporządzenia już istniejących interfejsów, jeśli przed dniem wejścia w życie rozporządzenia została podpisana umowa, o której mowa w art. 179 ust. 4a ustawy - Prawo telekomunikacyjne. Biorąc pod uwagę istnienie

już stosownych rozwiązań, nie przewiduje się znacznego wydatkowania ze środków budżetowych. Ewentualne niewielkie koszty związane z funkcjonowaniem istniejących rozwiązań pokryte zostaną ze środków planowanych w budżetach poszczególnych dysponentów, bez konieczności dodatkowego zwiększania wydatków.

IV. Wpływ regulacji na rynek pracy.

Wejście w życie rozporządzenia nie będzie miało wpływu na rynek pracy.

V. Wpływ regulacji na konkurencyjność gospodarki i przedsiębiorczość, w tym na funkcjonowanie przedsiębiorstw.

Wejście w życie rozporządzenia nie będzie miało wpływu na konkurencyjność wewnętrzną i zewnętrzną gospodarki.

Wpływ na przychody i wydatki przedsiębiorców telekomunikacyjnych

Przyjęcie uregulowań prawnych zaproponowanych w przedmiotowym rozporządzeniu wpłynie na realne obniżenie kosztów funkcjonowania przedsiębiorców telekomunikacyjnych, w porównaniu z aktualnym stanem prawnym. W chwili obecnej przedsiębiorca telekomunikacyjny jest obowiązany do ponoszenia kosztów, a następnie do eksploatacji kompleksowego rozwiązania technicznego umożliwiającego uprawnionym podmiotom wykonywanie ich ustawowych zadań. Decyzja o zastosowaniu rozwiązania opartego o interfejs spowoduje, że część kosztów, w tym także koszty późniejszej eksploatacji, przeniesiona zostanie na podmioty uprawnione, na podstawie umów zawieranych pomiędzy uprawnionym podmiotem, a przedsiębiorcami telekomunikacyjnymi.

Zastosowanie przez przedsiębiorcę telekomunikacyjnego rozwiązania interfejsowego pozwala mu też na skuteczne skorzystanie z dobrodziejstw art. 179 ust. 4c ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne, tj. wykonywania swych obowiązków na rzecz obronności i bezpieczeństwa państwa oraz bezpieczeństwa, porządku publicznego na zasadach outsourcingu, wspólnie z innym przedsiębiorcą telekomunikacyjnym. Wspólna budowa interfejsu przez kilku przedsiębiorców telekomunikacyjnych będzie niewątpliwie wpływała na obniżenie kosztów inwestycji i późniejszej eksploatacji (w tym także koszty osobowe), a w związku z powyższym sprawi, że nawet stosunkowo niewielcy przedsiębiorcy telekomunikacyjni mogą być zainteresowani zastosowaniem takiego rozwiązania. Fakt ten może także spowodować powstanie grupy wyspecjalizowanych w tej dziedzinie przedsiębiorców telekomunikacyjnych, ich głównym źródłem dochodu będą pobierane od innych przedsiębiorców telekomunikacyjnych opłaty za wykonywanie powierzonych zadań na zasadach określonych w art. 179 ust. 7. W związku z powyższym regulacje te będą działać stymulująco na rozwój przedsiębiorczości telekomunikacyjnej.

Proponowane regulacje nie mają wpływu na konkurencyjność gospodarki w zakresie rynku telekomunikacyjnego. Przedsiębiorcy telekomunikacyjni oraz podmioty uprawnione w świetle przepisów ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne mogą na podstawie odrębnych umów określić, iż warunki dostępu i utrwalania zapewnia się za pomocą interfejsów zlokalizowanych w miejscach obejmowanych przez sieć przedsiębiorcy telekomunikacyjnego. Umowa może określać współudział stron w kosztach zastosowania interfejsów. Biorąc pod uwagę autonomiczność woli stron przy kształtowaniu zobowiązań umownych, nie ma

praktycznych możliwości wskazania kosztów realizacji zapisów rozporządzenia. Ewentualną podstawą do dokonania takich szacunków powinny być dane uzyskane od producentów/dostawców tego typu urządzeń/systemów z uwzględnieniem zmian jakie należy dokonać w związku ze specyficznymi wymogami ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne.

Wysokość realnie ponoszonych kosztów przez poszczególnych przedsiębiorców telekomunikacyjnych jest trudna do oszacowania. W dużym stopniu zależy ona nie tylko od wielkości i obszaru działania danego podmiotu, ale też od poziomu zaawansowania technologicznego eksploatowanej przez niego infrastruktury i świadczonych usług telekomunikacyjnych. Istotnym czynnikiem wpływającym na wysokość tych wydatków jest także sposób, w jaki przedsiębiorca telekomunikacyjny dotychczas realizował swe obowiązki wynikające z art. 179 ust. 3 i 180d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne. W przypadku przedsiębiorców, którzy systematycznie rozwijali systemy teleinformatyczne zapewniające realizację ustawowych obowiązków i współdziałali w tym zakresie z uprawnionymi podmiotami zastosowanie interfejsu będzie wymagało stosunkowo niewielkich nakładów i krótkiego czasu. W sytuacji, gdy przedsiębiorca telekomunikacyjny nie przykładał znaczenia przedmiotowej problematyce, a swoje dotychczasowe działania w tej dziedzinie starał się ograniczyć do minimum nie uwzględniając tych potrzeb przy zakupie nowego sprzętu centralowego oraz pomijając uwagi i sugestie uprawnionych podmiotów (w stopniu nie spełniającym podstawowych wymagań ustawowych podmiotów), koszt pełnego wdrożenia przedmiotowych interfejsów może się wiązać z poważnymi wydatkami i wymagać całkowitej modernizacji posiadanej infrastruktury telekomunikacyjnej. Mając jednak na uwadze fakt, że deklaracja zastosowania interfejsu jest przejawem wolnej woli przedsiębiorcy telekomunikacyjnego należy uznać, że rozwiązanie takie przyjmie on tylko wówczas, gdy związane z tym wydatki i nakład prac będzie znacząco mniejsze niż realizacja ustawowych obowiązków w inny sposób, zgodny z wymaganiami zawartymi w rozporządzeniu, o którym mowa w art. 179 ust. 12 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne.

VI. Wpływ regulacji na sytuację i rozwój regionalny.

Wejście w życie rozporządzenia nie będzie miało wpływu na sytuację i rozwój regionalny.

Załącznik nr 1 do rozporządzenia
Rady Ministrów z dnia ..... 2011 r.

WYMAGANIA TECHNICZNE I EKSPLOATACYJNE

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

I. Normy i dokumenty powołane

1. Wykaz norm i dokumentów powołanych:

[1] ETSI ES 201 671v3.1.1 *Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic*

[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*

[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*

[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*

[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*

[6] ETSI TS 102 657 V1.7.1 *Lawful Interception (LI); Retained data handling;Handover interface for the request and delivery of retained data*

[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)

[8] ETSI TS 102 280 *X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons" V1.1.1 (2004-03)*

[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*

[10] IETF RFC 0791 *Internet Protocol*

[11] IETF RFC 0793 *Transmission Control Protocol*

[12] IETF RFC 0959 *File Transfer Protocol*

[13] IETF RFC 2460 *Internet Protocol Version 6 (IPv6) Specification*

[14] IETF RFC 3852 *Cryptographic Message Syntax (CMS)*

[15] IETF RFC 3261 *SIP: Session Initiation Protocol*

[16] IETF RFC 4296 *Internet Protocol Version 6 (IPv6) Addressing Architecture*

[17] ITU-T X.680 *Abstract Syntax Notation One (ASN.1): Specification of basic notation*

[18] ITU-T X.681 *Abstract Syntax Notation One (ASN.1): Information object specification*

[19] ITU-T X.682 *Abstract Syntax Notation One (ASN.1): Constrain specification*

[20] ITU-T X.683 *Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specifications*

[21] ITU-T X.690 *ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*

2. Dokumenty, o których mowa w jednostkach redakcyjnych [1]–[8], są dostępne na stronach Europejskiego Instytutu Norm Telekomunikacyjnych ETSI (www.etsi.org).
3. Dokument, o których mowa w jednostce redakcyjnej [9], jest dostępny na stronach Instytutu Inżynierów Elektryków i Elektroników IEEE (www.ieee.org).
4. Dokumenty, o których mowa w jednostkach redakcyjnych [10]-[16], są dostępne na stronach zespołu inżynierów ustanawiających standardy techniczne i organizacyjne w Internecie IETF (www.ietf.org).
5. Dokumenty, o których mowa w jednostkach redakcyjnych [17]-[21], są dostępne na stronach Międzynarodowego Związku Telekomunikacyjnego ITU (www.itu.int).

II. Stosowane skróty

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

ASN.1 - zestandaryzowana notacja stosowana do opisu struktur danych przenoszonych przez wiadomości wymieniane pomiędzy komunikującymi się elementami systemu, zdefiniowana w zaleceniach ITU-T X.680 [17], ITU-T X.681[18], ITU-T X.682 [19], ITU-T X.683 [20] (Abstract Syntax Notation One)

BER - sposób kodowania informacji zapisanej przy użyciu notacji ASN.1 do postaci transmitowanej w sieciach telekomunikacyjnych, zgodny z zaleceniem ITU-T X.690 [21] (Basic Encoding Rules)

CC - treść przekazu telekomunikacyjnego (Content of Communication)

CSD - transmisja danych z wykorzystaniem komutacji łączy (Circuit Switched Data)

CS - komutacja kanałów (Circuit Switched)

DER - sposób kodowania informacji, zgodny z zaleceniem ITU-T X.690 [21] (Distinguished Encoding Rules)

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

FTP - protokół transferu plików, zdefiniowany w dokumencie IETF RFC 0959 [12] (File Transfer Protocol)

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

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

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

IRI - informacje związane z przekazem telekomunikacyjnym (Intercept Related Information)

ISDN - sieć cyfrowa z integracją usług (Integrated Services Digital Network)

LEA - podmiot uprawniony do monitorowania (Law Enforcement Agency)

LEMF - system uprawnionego podmiotu umożliwiający dostęp do wybranych treści przekazów telekomunikacyjnych (Law Enforcement Monitoring Facility)

LI HI - interfejs pomiędzy systemem uprawnionego podmiotu a systemem przedsiębiorcy telekomunikacyjnego, wykorzystywany na potrzeby uprawnionego monitorowania (Lawful Interception Handover Interface)

LOGIN - nazwa użytkownika logującego się do sieci, używana w procesie jego uwierzytelnienia

MEID - unikalny numer identyfikujący telekomunikacyjne urządzenie końcowe używane w ruchomej publicznej sieci telefonicznej wykorzystującej technologię CDMA, zastępujący ESN (Mobile Equipment Identifier)

MSISDN - numer przydzielony użytkownikowi końcowemu ruchomej publicznej sieci telefonicznej (Mobile Subscriber Integrated Services Digital Network)

PSTN - publiczna komutowana sieć telefoniczna (Public Switched Telephone Network)

SIP - protokół sygnalizacyjny warstwy aplikacyjnej wykorzystywany do inicjowania, zarządzania oraz zakańczania sesji (połączenia telefonii internetowej, konferencji multimedialnej), zdefiniowany w dokumencie IETF RFC 3261 [15] (Session Initiation Protocol)

TCP - protokół komunikacji w sieci komputerowej, zdefiniowany w dokumencie IETF RFC 0793 [11] (Transmission Control Protocol)

VoIP - telefonia internetowa (Voice over IP)

III. Określenia użyte w załącznikach 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 załączniku nr 2,
   b) interfejs HI2 – styk umożliwiający jednokierunkowe, w kierunku od AMDF 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 dokumentem IEEE 802.3ab [9]. 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 dokumentem IETF RFC 0791[10], lub IPv6, zgodny z dokumentami IETF RFC 2460 [13] i IETF RFC 4296 [16]. Stosuje się publiczne adresy IP.

1.3. Sieć pomiędzy ADMF a LEMF jest siecią wydzieloną (sieć 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 '0' - '9': 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 normą ETSI ETS 300 927 [7],

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, krótkich wiadomości tekstowych 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:

a) przesyłanie informacji związanych z objętymi monitorowaniem przekazami telekomunikacyjnymi oraz opcjonalnie treści krótkich wiadomości tekstowych SMS (IRI),

b) przesyłanie informacji związanych z objętymi monitorowaniem przekazami telekomunikacyjnymi oraz treści monitorowanych przekazów telekomunikacyjnych (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 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 (Cryptographics Message Syntax) zdefiniowany w dokumencie IETF RFC 3852 [14]. Na potrzeby stosowania podpisu elektronicznego wykorzystywane są certyfikaty określone w dokumencie ETSI TS 102 280 [8], z uwzględnieniem wymagań technicznych zawartych w rozporządzeniu wykonawczym do ustawy o podpisie elektronicznym, oraz Infrastruktura Klucza Publicznego.

2.14 Szczegółowa specyfikacja elementów interfejsu HI1 przedstawiona jest w załączniku nr 2.

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 dokumencie IETF RFC 959 [12] na zasadach określonym w normie ETSI ES 201 671[1].

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 normie ETSI ES 201 671 [1], 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[1] w odniesieniu do usług świadczonych w sieciach ruchomych oraz usług transmisji pakietowej świadczonych w sieciach ruchomych,

b) ETSI TS 102 232-1[2] i ETSI TS 102 232-6[5] w odniesieniu do usług świadczonych w stacjonarnej publicznej sieci telefonicznej, zwanej dalej „siecią stacjonarną",

c) ETSI TS 102 232-1[2] i ETSI TS 102 232-3[3] w odniesieniu do usług dostępu do Internetu,

d) ETSI TS 102 232-1[2] i ETSI TS 102 232-5[4] 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 załączniku nr 2.

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 na interfejs HI3

4.1 Rozpoczęcie przekazywania do LEMF treści objętych monitorowaniem następuje niezwłocznie, jednak nie później niż 10 min. 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 dokumencie IETF RFC 959 [12] na zasadach określonych w normie ETSI ES 201 671[1].
- 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 (trybu „stereo"). W drugim sposobie oba kierunki transmisji zapisywane są w ramach jednego pliku (trybu „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,

  2 – treść CC (od monitorowanego obiektu),

  4 – treść CC (do monitorowanego obiektu),

  6 – treść 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 dokumentem IETF RFC 3261[15];
- 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 normach ETSI TS 102 232-1[2] i ETSI TS 102 232-6[5].

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 normie ETSI ES 201 671[1].

4.6 Przekazywanie treści komunikacji objętej monitorowaniem w sieci stacjonarnej jest realizowane zgodnie zasadami określonymi w normach ETSI TS 102 232-1[2] i ETSI TS 102 232-6[5].

4.7 W przypadku usług dostępu do Internetu, przekazywanie treści komunikacji objętej monitorowaniem jest realizowane zgodnie zasadami określonymi w normach ETSI TS 102 232-1[2] i ETSI TS 102 232-3[3].

4.8 W przypadku usług telefonii internetowej, przekazywanie treści komunikacji objętej monitorowaniem jest realizowane zgodnie zasadami określonymi w normach ETSI TS 102 232-1[2] i ETSI TS 102 232-5[4].

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

1.1 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.

1.2 W warstwie fizycznej stosowany jest interfejs standardu Ethernet 100/1000BASE-T, zgodny z dokumentem IEEE 802.3ab [9].

1.3 Protokołem warstwy sieciowej interfejsu HI A-B jest protokół IPv4, zgodny z dokumentem IETF RFC 0791[10], lub protokół IPv6, zgodny z dokumentami IETF RFC 2460 [13] i IETF RFC 4296 [16]. Stosuje się publiczne adresy IP.

1.4 Stosuje się mechanizm podpisu elektronicznego.

1.5 Realizacja interfejsu HI A-B jest zgodna ze normą ETSI TS 102 657 [6].

1.6 Dla realizacji komunikacji w interfejsie HI A-B stosuje się wariant określony w punkcie 7.3 normy ETSI TS 102 657 [6] tj.

a) w warstwie transportowej stosowany jest protokół TCP,

b) stosowane jest kodowanie elementów informacyjnych w formacie ASN.1/BER.

1.7 Wartość parametru cSPID odpowiada identyfikatorowi przypisanemu danemu przedsiębiorcy w Rejestrze przedsiębiorców telekomunikacyjnych.

1.8 Pole „*countryCode*" w parametrze „*RequestID*" przyjmuje wartość „*PL*".

1.9 Pole „*authorisedOrganisationID*" w parametrze „*RequestID*" przyjmuje wartość zgodnie z przypisaniem LEAID.

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

1.10 Nie stosuje się niżej wymienionych rozwiązań opcjonalnych:

a) priorytetów dla obsługi żądań skierowanych przez LEA („*RequestPriority*", punkt A.2.2.1w normie ETSI TS 102 657 [1]),

b) mechanizm „*multi-part delivery*", zgodnie z punktem 5.1.7 w normie ETSI TS 102 657 [1],

c) trybu „*Authorized-Organization-initiated*", zgodnie z punktem 5.3 w normie ETSI TS 102 657 [1].

1.11 Niewykorzystywane są elementy informacyjne wymienione w tabeli nr 3.

Tabela nr 3

Punkt w normie ETSI TS 102 657 [1]	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

Załącznik nr 2 do rozporządzenia
Rady Ministrów z dnia ..... 2011 r.

Wymagania w zakresie specyfikacji elementów interfejsu HI1 oraz formatu parametru ExtendedPartyIdentity

4.11 Struktura interfejsu HI1

1.1 Warstwa transportowa

1.1.1 Stosowany jest protokół TCP.

1.1.2 Zestawiane są połączenia TCP w kierunkach:

- ADMF/MF/DF ▶ LEMF (HI1LEMFOperations),
- LEMF ▶ ADMF/MF/DF (HI1ADMFOperations).

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

1.2 Warstwa aplikacyjna

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

1.2.1 Opis

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

1.2.1.2 Stosowane są dwa protokoły zdefiniowane w ASN.1:

- HI1LEMFOperations – operacje inicjowane przez LEMF,
- HI1ADMFOperations – alarmy i powiadomienia wysyłane przez ADMF.

1.2.1.3 Operacje, o których mowa w pkt 1.2.1.2, są całkowicie od siebie niezależne.

1.2.1.4 Każda operacja/zapytanie to jedna sesja TCP.

1.2.1.5 Każde zapytanie jest potwierdzane przez drugą stronę.

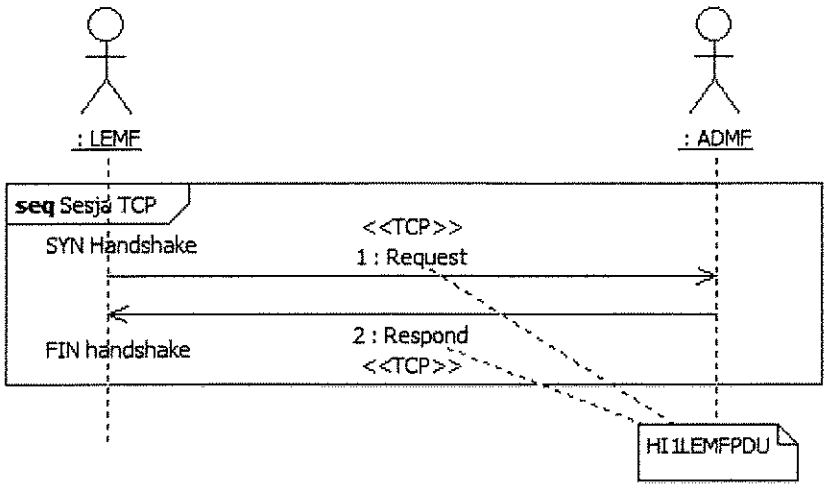
1.2.2 Protokół HI1LEMFOperations

1.2.2.1 Operacje wykonywane przez LEMF:

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

– Zapytania podpisane:

- Activate
- Modificate, z wyłączeniem w odniesieniu do włączania/ wyłączania trybu online
- Deactivate



Rysunek 1: Schemat operacji

1.2.2.2 Każda wiadomość definiująca zapytanie wysłane przez LEMF (Request) jest potwierdzana przez wiadomość zawierającą odpowiedź ADMF na wysłane żądanie LEMF (Respond).

1.2.2.3 LEMF czeka na odpowiedź 10 sek. Po tym czasie uznaje wysłaną wiadomość za utraconą.

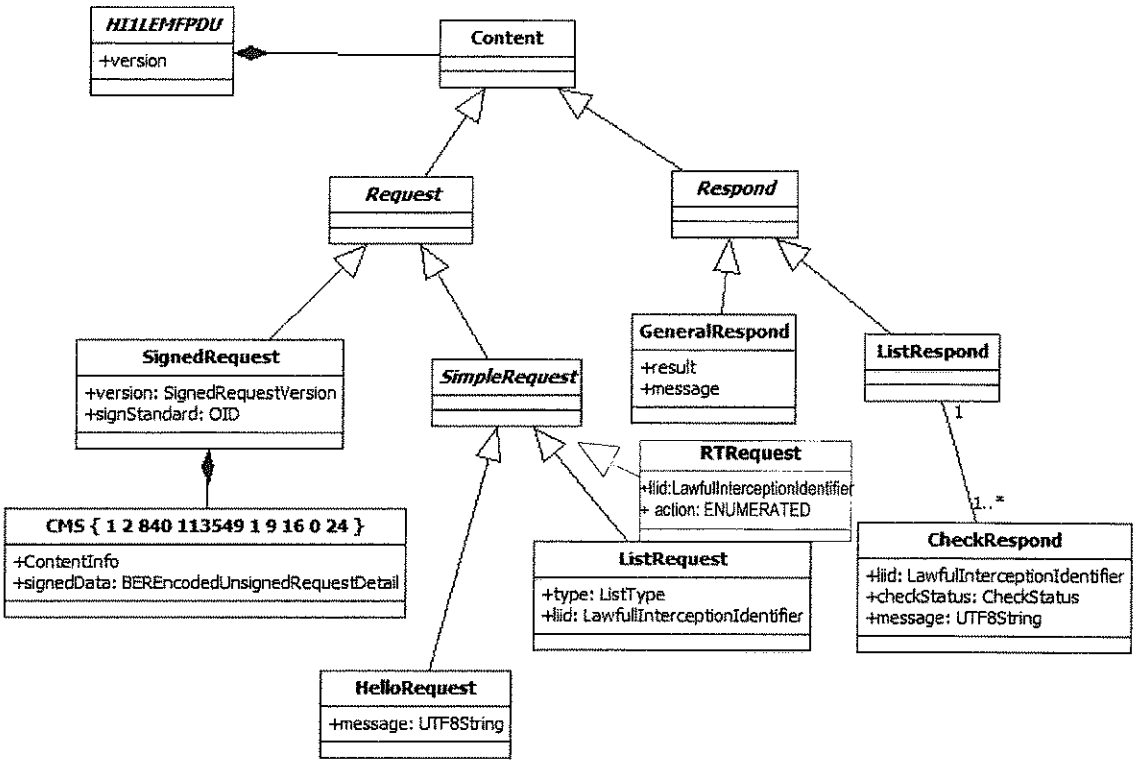
1.2.2.4 Nad harmonogramem aktywacji i dezaktywacji czuwa LEMF. Dopuszcza się wysłanie zlecenia aktywacji z wyprzedzeniem. Zlecenie aktywacji posiada określony czas zakończenia obserwacji. Przesunięcie momentu zakończenia obserwacji ponad ten czas wymaga zlecenia modyfikacji.

1.2.2.5 System monitoringu przedsiębiorcy telekomunikacyjnego przesyła do LEMF informacje o założeniu, zdjęciu obserwacji w elementach sieci przedsiębiorcy telekomunikacyjnego.

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

1.2.2.7 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.

1.2.2.8 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.



Rysunek 2: Struktura HI1LEMFPDU

1.2.2.9 Wiadomości są podzielone na dwie grupy:

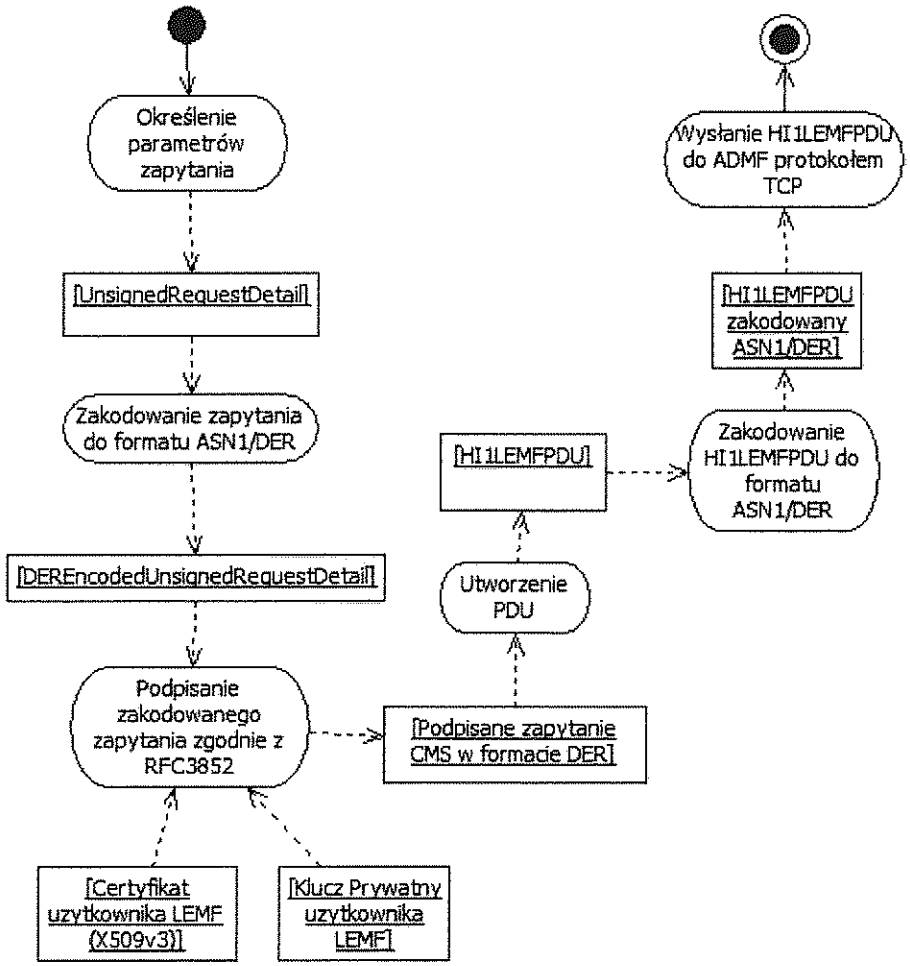
- Request – definujące zapytania wysyłane przez LEMF
- Respond – odpowiedzi ADMF'a na wysłane żądania LEMF'a

1.2.2.10 Dopuszczalne są następujące interakcje pomiędzy LEMF a ADMF

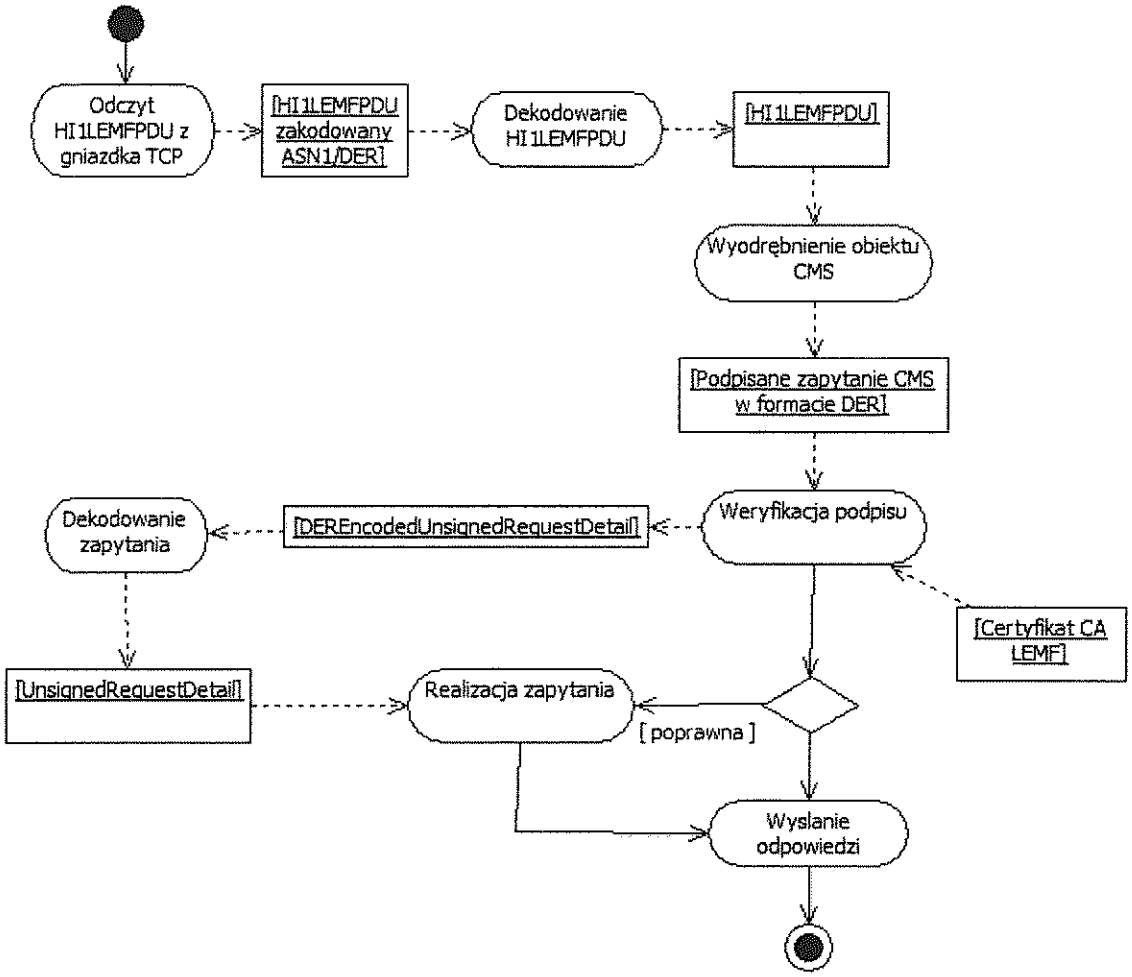
Zapytanie LEMF	Odpowiedź ADMF	Alternatywna odpowiedź
SignedRequest	GeneralRespond	
HelloRequest	GeneralRespond	
ListRequest	ListRespond	GeneralRespond
RTRequest	GeneralRespond	

1.2.2.11 Zapytania podpisane (SignedRequest)

Sposób tworzenia i weryfikacji wiadomości podpisanych za pomocą diagramów aktywności przedstawiony jest na rys. 3 i rys. 4.



Rysunek 3: Tworzenie podpisanego zapytania



Rysunek 4: Weryfikacja podpisanego zapytania

1.2.2.12 Uwagi:

- CMS (Cryptographic Message Syntax 2004): format binarny dokumentu z podpisem (z użyciem kodowania DER) stanowi podzbiór CMS. Dokładna specyfikacja przedstawiona jest w dokumencie IETF RFC3852 [13].
- OID definiujący standard w notacji ASN.1:

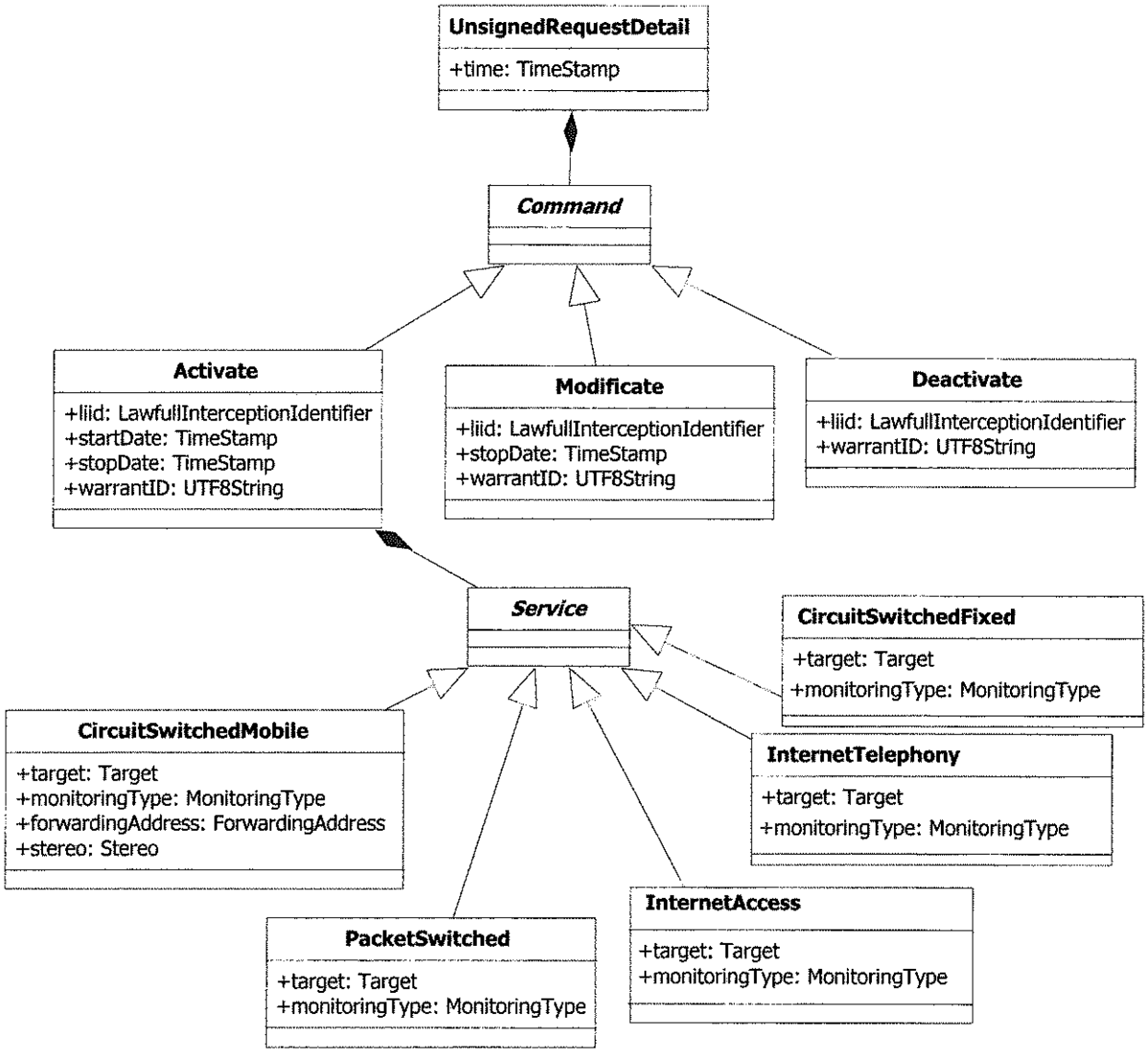
  OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) modules(0) cms-2004(24) }

- UnsignedRequestDetail:
  Struktura opisująca szczegóły zapytania aktywacji, modyfikacji i deaktywacji dedykacji. Po zakodowaniu do postaci DER jest podpisywana zgodnie ze specyfikacją przedstawioną w dokumencie RFC2315. Struktura UnsignedRequestDetail przedstawiona jest na rys. 5.
- Service:

Obiekt reprezentujący usługi świadczone przez operatora.

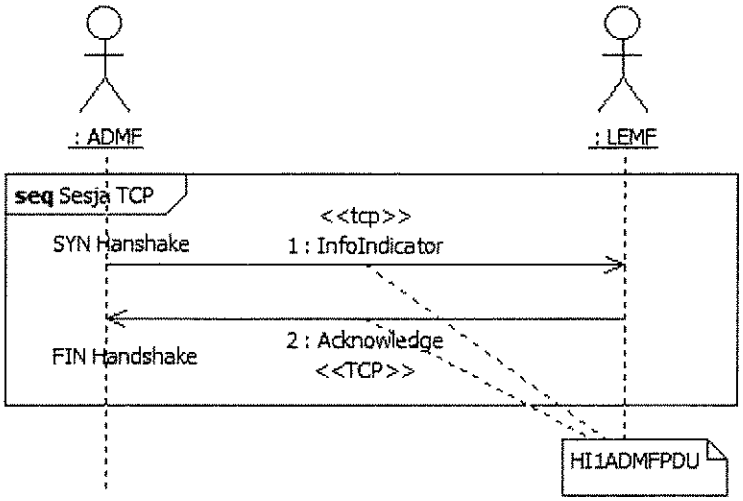
- Monitorowane są następujące usługi:

  CS Circuit Switched (Mobile)
  PS PacketSwitched
  InternetAccess
  InternetTelephony
  CS Circuit Switched (Fixed)



Rysunek 5: Struktura UnsignedRequestDetail

1.2.3 *Protokół HI1ADMFOperations*



Rysunek 6: Schemat Operacji

1.2.3.1 Operacje wykonywane przez ADMF:

- Alarmy
- Notyfikacje

1.2.3.2 Wiadomości są podzielone na dwie grupy:

- InfoIndicator - definiujące alarmy i notyfikacje wysyłane przez ADMF
- Acknowledge - potwierdzenia otrzymania wiadomości przez ADMF

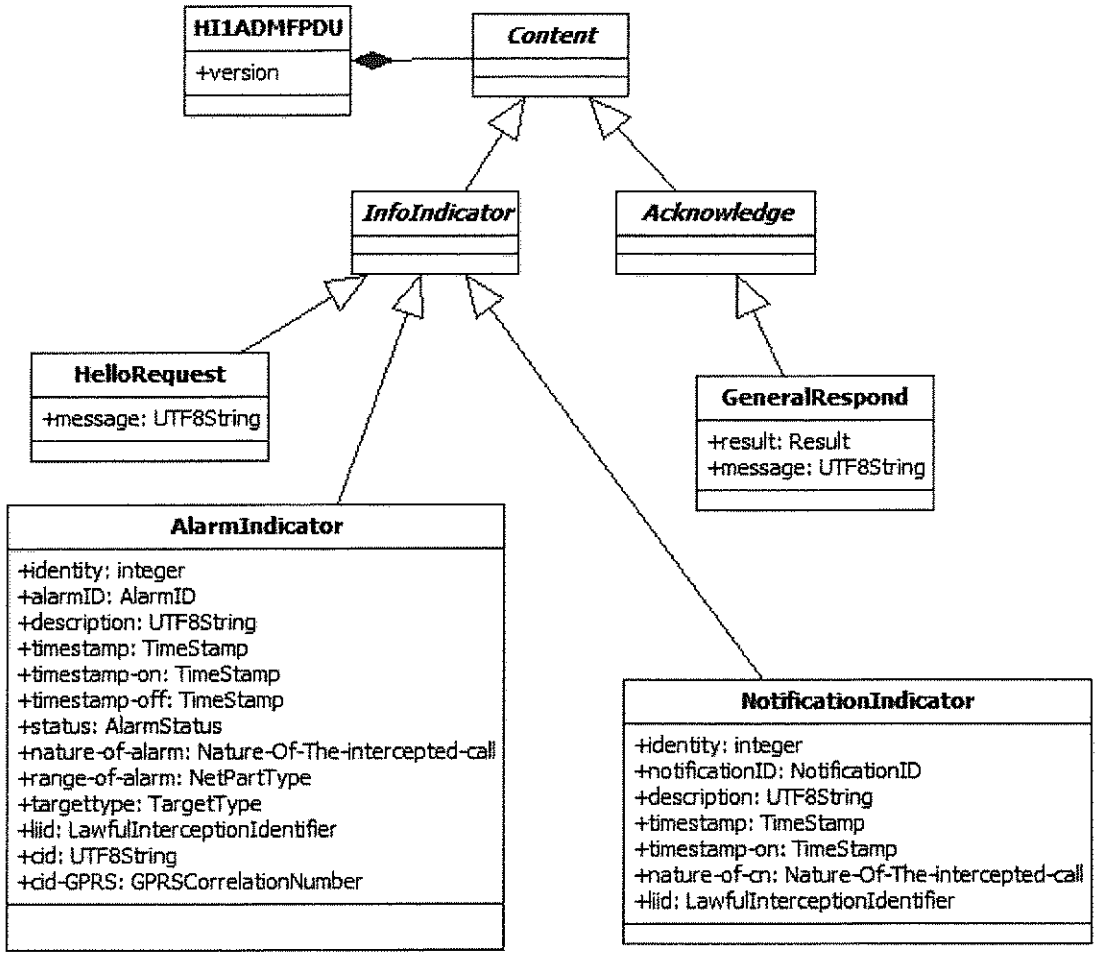
1.2.3.3 Dopuszczalne są następujące interakcje pomiędzy ADMF a LEMF

Wiadomość ADMF	Odpowiedź LEMF
HelloRequest	GeneralRespond
AlarmIndicator	GeneralRespond
NotificationIndicator	GeneralRespond

1.2.3.4 Uwagi:

- Wyróżnia się dwa typy wiadomości wysyłanych przez ADMF: alarmy i notyfikacje.
- Każda wysłana wiadomość (InfoIndicator) jest potwierdzana przez LEMF (Acknowledge).
- Potwierdzenie jest realizowane w czasie 5 sek.

- Alarmy posiadają dwa stany: włączony, wyłączony (pole status).
- Wiadomość wyłączająca alarm może zawierać tylko jego identyfikator (identity).



Rysunek 7: Struktura HI1ADMFPDU

1.3 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
```

1.4 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 znakow numerycznych ASCII
-- format: LEAID + TARGET(SEQ)
-- TARGET - (15 znakow) nadawany sekwencyjnie dla kazdego 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
```

1.5 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 identyfikacje 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
identyfikacje 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
przepełnine => 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 usunieta 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
```

2. 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
}
```