

Architektura i zasada działania systemu IP Multimedia Subsystem

Robert Janowski*

Warszawska Wyższa Szkoła Informatyki

Abstrakt

W niniejszym opracowaniu przedstawiono koncepcję systemu IP Multimedia Subsystem, skrótowy opis jego architektury, zasady działania, podstawowe scenariusze sygnalizacyjne oraz sposób realizacji usług. Opisywane koncepcje zilustrowano przykładem konfiguracji i uruchomienia usługi bezwarunkowego przekierowania połączenia telefonicznego wdrożonej na platformie OpenIMSCore z wykorzystaniem oprogramowania Kamailio jako serwera aplikacyjnego.

Słowa kluczowe – IP Multimedia Subsystem, OpenIMSCore, SIP, Kamailio

1. Wprowadzenie

W ciągu ostatnich 30 lat sieć telekomunikacyjna przeszła rewolucyjne zmiany. Początkowo sieć telekomunikacyjna służyła jedynie do przekazu głosu czyli świadczenia usług telefonicznych tzw. POTS (*Plain Old Telephone Service*) realizowanych w technologii analogowej. Wraz z pojawieniem się faksu oraz komputerów rozpoczęto w sieci telekomunikacyjnej również przesyłanie danych, ale wymagało

* E-mail: rjanowski@poczta.wysi.edu.pl

to konwersji sygnału cyfrowego, pierwotnie generowanego przez te urządzenia, na sygnał analogowy poprzez zastosowanie modemów. W efekcie transmisja danych realizowana była tak samo jak telefonia czyli poprzez nadawanie sygnałów analogowych.

Postępujące upowszechnianie się komputerów i wynikająca z tego potrzeba przekazywania przez sieć telekomunikacyjną danych i ruchomych obrazów w postaci pierwotnej (czyli cyfrowej) spowodowała pod koniec lat 80. zeszłego wieku zstandardyzowanie sieci ISDN (*Integrated Services Digital Network*) [1].

Według tej koncepcji, ta sama sieć telekomunikacyjna oferowała zintegrowane usługi, tj. przekaz głosu, video i danych w technologii komutacji kanałów z wykorzystaniem strumieni $n \times 64$ kbps, ale z ograniczeniem do 2 Mbps. Z punktu widzenia użytkownika w punkcie zakończenia sieci telekomunikacyjnej (*Network Termination; NT*) istniał dostęp nie do jednej jak poprzednio ale do trzech usług [2].

Wzrost zapotrzebowania na przepustowość sieci, stymulowany głównie usługami video oraz szerokopasmową transmisją danych, doprowadził do pojawienia się koncepcji szerokopasmowej sieci z integracją usług B-ISDN (*Broadband-ISDN*) [3]. Z uwagi na wymaganie szerokopasmowości, które wówczas, tj. na przełomie lat 80. i 90. definiowano umowną granicą 2 Mbps, nie było możliwe użycie rozwiązań stosowanych w sieci ISDN. Ostatecznie jako sposób realizacji idei sieci B-ISDN wybrano technikę ATM (*Asynchronous Transfer Mode*), która wykorzystywała technologię komutacji pakietów [4].

Dzięki temu możliwe było przekazywanie w sieci B-ISDN strumieni o dowolnej przepływności bez ograniczenia wynikającego z wielokrotności strumieni 64 kbps. Próbkę głosu, video oraz dane przekazywane były w porcjach o stałej długości 53 bajtów w tym 5 bajtów nagłówka zwanych komórkami (*cells*) [4].

Niestety, technika ATM będąc nowym sposobem realizacji warstwy łącza danych według modelu OSI, wymagała nowego sprzętu zarówno po stronie sieci, czyli operatora telekomunikacyjnego, jak i użytkowników (karty sieciowe w komputerach). Koszty migracji od rozpowszechnionego już wówczas standardu IEEE 802.3 (*Ethernet*) okazały się główną przeszkodą upowszechnienia się techniki ATM wśród użytkowników końcowych, którzy już posiadali lub mogli nabyć względnie tanie karty sieciowe standardu Ethernet. W efekcie zastosowanie techniki ATM ograniczyło się

do wewnętrznej sieci operatorów telekomunikacyjnych, a z punktu widzenia użytkowników nadal nie istniała szerokopasmowa sieć z integracją usług, do której byłby dostęp “w jednym gniazdku”.

W końcu rozwiązanie przyszło ze środowiska operatorów sieci mobilnych. To właśnie 3GPP (*3rd Generation Partnership Project*) [5], organizacja wywodząca się z tego grona, w swoich dokumentach standaryzujących opisała architekturę systemu IMS (*IP Multimedia Subsystem*) [6], który realizował postulat sieci zintegrowanej usługowo. Co więcej, IMS oferuje również konwergencję różnych technik dostępowych, czyli umożliwia dostęp do tych samych usług za pośrednictwem różnych sieci dostępowych. Dzięki temu możliwa jest na przykład zmiana sieci radiowej 4G na sieć Wi-Fi po wejściu do budynku bez konieczności przerywania rozmowy telefonicznej [7].

Pozostała część tego opracowania zorganizowana jest w następujący sposób. W rozdziale 2 została przedstawiona architektura systemu IMS opierająca się na podziale na 3 płaszczyzny oraz zostały opisane poszczególne elementy funkcjonalne. W rozdziale 3 opisane zostały podstawowe procedury sygnalizacyjne. Rozdział 4 przybliży sposób realizacji usług w sieci IMS oraz rolę serwerów aplikacyjnych. W rozdziale 5 został opisany przykład realizacji usługi bezwarunkowego przekierowania połączenia w środowisku OpenIMSCore [8] – uproszczonej implementacji systemu IMS dostępnej na licencji Open Source. Rozdział 6 stanowi podsumowanie opracowania.

2. Architektura systemu IMS

Twórcy standardów związanych z siecią IMS jasno określili wymagania stawiane nowej architekturze. Zostały one sprecyzowane po wnikliwej analizie istniejącej sytuacji oraz trendów rozwojowych w obszarze sieci telekomunikacyjnych i teleinformatycznych.

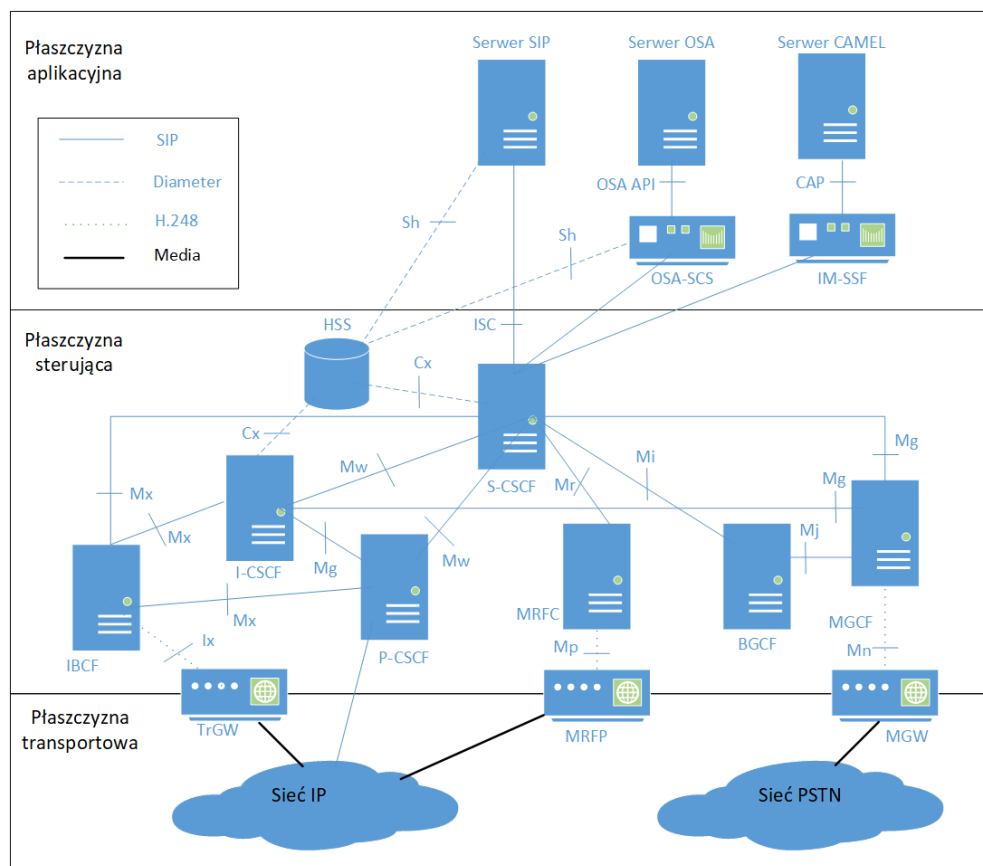
Jako najważniejsze wymagania, spośród tych opisanych w dokumencie [9], należy wymienić:

- przyjęcie sieci IP za podstawową technikę transportową oraz przeniesienie razem z nią modelu usług Internetowych. Najważniejsze elementy tego modelu to wzbogacanie podstawowej usługi przenoszenia głosu poprzez łączenie jej

z innymi usługami, np. usługą obecności oraz możliwość korzystania z wielu usług jednocześnie;

- konwergencję technik dostępowych poprzez istnienie jednej wspólnej infrastruktury sieci (szkieletowej) niezależnej od typu sieci dostępowej. Oznacza to, że po stronie operatora te same aplikacje mogą być wykorzystywane, żeby oferować zunifikowane usługi niezależnie od sieci dostępowej, poprzez którą podłączony jest użytkownik, np. UMTS, LTE, WiFi, xDSL. Ponadto użytkownik powinien móc korzystać z tej samej usługi zmieniając sieć dostępową;
- zapewnienie odpowiedniej jakości, stosownie do usługi, z której korzysta użytkownik w ujęciu całościowym, tzn. „od końca do końca” (*end-to-end*). Sposób transportu bez zapewnienia parametrów jakościowych tzw. usługa typu „*best effort*”, oferowany obecnie przez sieć Internet, jest niewystarczający do zagwarantowania użytkownikom oczekiwanej jakości w zakresie usług wymagających reżimu czasu rzeczywistego, np. telefonia, videokonferencje, telewizja;
- konieczność istnienia efektywnej polityki sterowania dostępem do zasobów sieciowych. Mechanizmy zarządzania zasobami oraz sterowania przyjmowaniem nowych połączeń (*Call Admission Control*) muszą zostać dodane jako nakładka na sieć IP;
- konieczność zapewnienia współpracy z istniejącymi sieciami np. PSTN (*Public Switced Telephone Network*), ISDN (*Integrated Service Digital Network*), PLMN (*Public Land Mobile Network*). Ze względu na fakt, że wdrażanie systemu IMS będzie realizowane etapami, musi być zapewniona możliwość komunikacji pomiędzy użytkownikami korzystającymi z systemu IMS oraz niekorzystającymi z niego;
- elastyczne modele taryfikowania usług, pozwalające na implementację wielu różnych schematów taryfikowania. Jest to konieczne dla zapewnienia konkurencyjności rynkowej, możliwości implementacji wymagań regulacyjnych oraz różnych aspektów technicznych związanych ze współpracą różnych sieci. Przykładami wymagającymi odmiennych modeli taryfikowania są usługi abonamentowe, usługi przedpłacone tzw. „na kartę” oraz usługi z opłatą obciążającą odbierającego połączenie.

W celu osiągnięcia wyżej podanych wymagań, architektura systemu IMS składa się z szeregu elementów funkcjonalnych zorganizowanych w 3 płaszczyzny [10]: transportową (*Bearer plane*), sterowania (*control plane*) oraz płaszczyznę aplikacyjną (*application plane*).



Rysunek 1. Architektura systemu IMS z uwidocznieniem podziału na 3 płaszczyzny [18]

Elementy funkcjonalne należące do płaszczyzny transportowej i sterowania reprezentują funkcje realizowane w mobilnej centrali telefonicznej (*Mobile Switching Center*), czyli realizują odpowiednio obsługę strumieni mediów i sygnalizacji. Płaszczyzna aplikacyjna została dodana w celu powielenia paradygmatu sieci inteligent-

nych (*Intelligent Networks*) [11],[12] tj. przeniesienia sterowania z płaszczyzny sterującej [13] do płaszczyzny aplikacyjnej (w sieciach inteligentnych nazywaną usługową) celem wykonania określonej logiki [14].

Takie rozwiązanie, podobnie jak w sieciach inteligentnych, umożliwia swobodne wprowadzanie nowych usług, gdyż są one całkowicie niezależne od płaszczyzny sterowania, z której przychodzą jedynie powiadomienia o wywołaniu konkretnej logiki przenoszone przez zestandaryzowany protokół komunikacyjny[11].

Zatem nowe usługi mogą powstawać i być wdrażane bez wpływu na pozostałą część systemu IMS dzięki ustalonemu stykowi pomiędzy płaszczyzną aplikacyjną, a płaszczyzną sterowania (styk ISC; *IMS Service Control*) [10], który w systemie IMS wykorzystuje protokół SIP (*Session Initiation Protocol*) [15]. W sieciach inteligentnych komunikacja pomiędzy warstwą sterowania a usługową odbywała się w analogiczny sposób z wykorzystaniem protokołów INAP (*Intelligent Network Application Part*) [16] lub CAP (*CAMEL Application Part*) [17].

2.1. Charakterystyka płaszczyzny transportowej

Płaszczyzna transportowa jest odpowiedzialna za realizację usług przenoszenia (*bearer services*) tzn. za transport ruchu użytkowników. Składa się ona z fizycznych zasobów koniecznych do ustanowienia połączenia oraz przenoszenia treści (ruchu głosowego, danych lub video) od źródła do przeznaczenia.

Do tej płaszczyzny należą następujące elementy funkcjonalne architektury [18]:

- Media Gateway (MGW) – jednostka odpowiedzialna za przenoszenie ruchu pomiędzy sieciami różnych typów, w szczególności sieciami IP (transport z wykorzystaniem protokołów RTP i IP) oraz sieciami komutacji kanałów np. kanały 64 kbps kodowane w standardzie PCM (*Pulse Code Modulation*),
- Media Resource Function Processor (MRFP) – jednostka odpowiedzialna za realizację połączeń konferencyjnych, transkodowanie strumieni audio i video (w obrębie sieci IMS) oraz odgrywanie zapowiedzi słownych typu „Wybrany numer jest niedostępny” na żądanie elementu sterującego – MRFC (*Media Resource Function Control*),
- Transition Gateway (TrGW) – jednostka odpowiedzialna za realizację funkcji translacji protokołów sieciowych (IPv4 i IPv6), protokołów transportowych

(UDP i TCP), translację adresów sieciowych (*Network Address Translation; NAT*) i portów. TrGW jest sterowany przez jednostkę IBCF (*Interconnection Border Control Function*) [19].

2.2. Charakterystyka płaszczyzny sterowania

Płaszczyzna sterowania jest odpowiedzialna za dopuszczenie użytkownika do korzystania z sieci, kierowanie połączeń i wywoływanie konkretnych usług. Należą do niej następujące elementy funkcjonalne architektury [18]:

- Home Subscriber Server (HSS) – baza danych zawierająca wszystkie informacje związane z abonentami usług niezbędne do obsługi połączeń. HSS jest bazą przechowującą profile oraz informacje niezbędne do uwierzytelnienia wszystkich użytkowników a także bieżące informacje ich dotyczące takie jak obecny stan rejestracji oraz lokalizacja. HSS można postrzegać jako nową wersję bazy HLR (*Home Location Register*), znaną z sieci GSM (*Global System for Mobile communication*). HSS realizuje te same funkcje, które realizował HLR, np. uwierzytelnienie użytkownika, oraz dodatkowo funkcje specyficzne dla działania system IMS, np. udział w obsłudze usług oferowanych przez serwery aplikacyjne poprzez dostarczanie serwerom aplikacyjnym (SIP lub OSA-SCS) informacji na temat profili użytkowników lub udział w zestawianiu połączeń i sesji użytkowników poprzez udostępnianie węzłowi I-CSCF informacji na temat węzła S-CSCF aktualnie obsługującego danego abonenta. Pozostałe elementy systemu IMS komunikują się z węzłem HSS poprzez 3 standardowe styki: Cx, Si, Sh. Styk Cx obsługuje komunikację z węzłami CSCF (I-CSCF lub S-CSCF). Styk Sh obsługuje komunikację z serwerami aplikacji, umożliwiając przesyłanie zapytań do węzła HSS dotyczących informacji o profilu danego użytkownika. Styk Si obsługuje zapytania ze środowiska CSE (*CAMEL Service Environment*). Na wszystkich 3 stykach do komunikacji pomiędzy elementami wykorzystywany jest protokół DIAMETER [20].
- Subscriber Locator Function (SLF) – jednostka odpowiedzialna za identyfikację adresu bazy HSS właściwej dla danego abonenta, w przypadku gdy istnieje więcej niż jedna baza HSS.

- Call Session Control Function (CSCF) – jednostka odpowiedzialna za realizację funkcji przetwarzania i sterowania połączeniami, analogiczne do tych które realizowane są przez centrale telefoniczne w sieciach z techniką komutacji kanałów. Jednostka CSCF realizuje również funkcję zarządzania sesjami, sterowanie usługami i udogodnieniami oraz alokacją zasobów. W zależności od przypisanej roli możemy wyróżnić trzy rodzaje jednostek CSCF:
 - Serving CSCF (S-CSCF) – jednostka CSCF odpowiedzialna za funkcje obsługi połączeń (analogicznie do sieci z komutacją kanałów) i sesji. Wszystkie wiadomości SIP przesyłane od i do danego terminala użytkownika kierowane są przez przypisany mu węzeł S-CSCF. Węzeł S-CSCF utrzymuje informacje dotyczące wszystkich sesji, ponadto obsługuje interakcje z platformami aplikacyjnymi realizującymi usługi, obsługuje zgłoszenia dotyczące zasobów sieci transportowej oraz wywołuje funkcje taryfikacji;
 - Interrogating CSCF (I-CSCF) odbiera wiadomości SIP od węzła P-CSCF i przekazuje dalej do węzła S-CSCF, który obsługuje dany terminal. Węzeł I-CSCF jest odpowiedzialny za wyznaczenie właściwego węzła S-CSCF, do którego powinny zostać przekazane wiadomości sygnalizacyjne SIP. Po otrzymaniu od terminala abonenta wiadomości SIP REGISTER, I-CSCF kieruje pytanie do węzła HSS danego abonenta poprzez styk Cx w celu ustalenia czy abonent ma przypisany węzeł obsługujący S-CSCF, wskazanie przypisanego węzła S-CSCF, określenie jakie są wymagania dotyczące usług abonenta oraz preferencje operatora dla tego konkretnego abonenta. Oprócz wyznaczenia przypisanego węzła S-CSCF, podstawową rolą I-CSCF-a jest ukrywanie wewnętrznej struktury sieci operatora przed węzłami innych operatorów systemu IMS;
 - Proxy CSCF (P-CSCF) – jednostka CSCF stanowiąca pierwszy punkt kontaktu dla terminali z danej domeny IMS tzw. punkt wejścia do systemu IMS. Oznacza to, że terminal użytkownika adresuje wszystkie wiadomości sygnalizacyjne do jednostki P-CSCF.
- Breakout Gateway Control Function (BGCF) – jednostka odpowiedzialna za wyznaczenie następnego węzła obsługującego kierowane wiadomości SIP.

Sposób wyznaczania następnego węzła sieci lub punktu wyjścia z sieci, polega na analizowaniu wiadomości SIP otrzymywanych od węzła S-CSCF i sprawdzeniu możliwości przełożenia adresu docelowego SIP URI w DNS-ie. Jeżeli adres docelowy istnieje w DNS-ie wówczas wiadomo, że połączenie jest obsługiwane w sieci IMS. W przeciwnym przypadku połączenie jest przekazywane do sieci komutacji kanałów (*Circuit Switched; CS*). W takiej sytuacji jednostka BGCF określa czy wyjście do sieci CS (sieć PSTN lub PLMN) nastąpi w tej samej domenie IMS czy innej. Jeżeli w tej samej, wówczas wybiera odpowiedni węzeł MGCF (*Media Control Gateway Function*), który zajmuje się przekazaniem tego połączenia do sieci PSTN. Jeżeli wyjście ma nastąpić w innej domenie, wówczas BGCF przekazuje wiadomości sygnalizacyjne SIP dalej do węzła BGCF z tej innej domeny [19].

- Media Gateway Control Function (MGCF) – jednostka sterująca elementem MGW. Sterowanie odbywa się za pomocą protokołu H.248 [21] poprzez styk Mn. Protokół H.248 jest protokołem wykorzystującym do transportu protokół IP, zgodnie z założeniami architektury IMS. Nazwa H.248 jest nazwą standardu wprowadzonego przez ITU-T. Prace nad tym samym standardem prowadziła też organizacja IETF, nadając protokołowi nazwę *Megaco*. Faktycznie określenia H.248 i *Megaco* odnoszą się do tego samego protokołu na styku MGW z MGCF. MGCF jest odpowiedzialny za konwersję pomiędzy protokołami sterowania połączeniami ISUP i SIP tzn. odbiera wiadomości sygnalizacyjne z jednej strony, tłumaczy je na protokół drugiej strony (ISUP na SIP, a SIP na ISUP) i przekazuje dalej. W związku z tym zadaniem, MGCF ustanawia powiązania pomiędzy identyfikatorami strumieni transportowych po stronie sieci z komutacją kanałów a identyfikatorami strumieni transportowych po stronie sieci z komutacją pakietów (sieci IP). MGCF musi przekazać informację o tych powiązaniach elementowi obsługującemu translację strumieni transportowych tzn. węzłowi MGW. Ponadto MGW musi być poinformowany o sposobie kodowania strumieni danych. Tę informację MGW otrzymuje od MGCF, ponieważ jest ona dostępna w ramach sygnalizacji IMS związanej z zestawianiem połączenia, w której uczestniczy również MGCF. MGCF komunikuje się z jednostkami CSCF i BGCF oraz wyznacza kolejny węzeł obsługujący wiadomości SIP dla połączeń przychodzących z sieci CS.

- Multimedia Resource Function Controller (MRFC) – jednostka sterująca elementem MRFP wykorzystywanym do zestawiania połączeń typu zapowiedzi słowne, mostki konferencyjne, transkodowanie strumieni mediów. Odbiera i interpretuje również informacje z jednostek S-CSCF i serwerów aplikacyjnych (AS).
- Interconnection Border Control Function (IBCF) – jednostka odpowiedzialna za realizację funkcji warstwy aplikacji w odniesieniu do protokołów SIP i SDP (*Session Description Protocol*) w celu zapewnienia połączenia pomiędzy dwoma różnymi domenami sieci IMS. W szczególności IBCF wykonuje dopasowanie sygnalizacji SIP (modyfikacja, usuwanie, dodawanie nagłówek SIP i SDP), ukrywanie topologii sieci z poziomu sygnalizacji SIP, np. usuwanie elementów nagłówek pozwalających na sprawdzenie przebytej drogi w domenie, steruje funkcjami płaszczyzny transportowej – TrGW, generuje rekordy billingowe (*Call Data Records; CDR*).
- Signaling Gateway (SGW) – jednostka łącząca różne typy sieci sygnalizacyjnych na przykład sieci SS7 [22] z sieciami opartymi na IP, np. IMS. W sensie funkcjonalnym jest odpowiednikiem jednostki MGW dla ścieżki przekazującej sygnalizację. Dokonuje zatem konwersji transportu sygnalizacji pomiędzy stosem SS7/MTP [23] a SCTP/IP [24]). Jednostka ta nie dokonuje interpretacji protokołów sygnalizacyjnych, których ruch przenosi tj. protokołów MAP (*Mobile Application Part*) [25], CAP (*CAMEL Application Part*) [17], BICC (*Bearer Independent Call Control*) [26], ISUP (*Integrated Services User Part*) [27].

2.3. Charakterystyka płaszczyzny aplikacyjnej

Płaszczyzna aplikacyjna (*application plane*) jest odpowiedzialna za realizację usług. Zawiera całą logikę usługową oraz wszystkie dane niezbędne do oferowania usług użytkownikom końcowym. W jej obszarze znajdują się następujące elementy funkcjonalne [18]:

- serwer aplikacyjny (*Application Server; AS*) – jednostka funkcjonalna realizująca określoną logikę usługową. AS komunikuje się z siecią IMS poprzez styk ISC (*IMS Service Control*) z wykorzystaniem protokołu SIP.

- IP Multimedia Service Switching Function (*IM-SSF*) – jednostka, która stanowi punkt pośredniczący pomiędzy systemem IMS a środowiskiem usług realizowanych w modelu CAMEL (*Customised Applications for Mobile network Enhanced Logic*) [28]. Uwzględnienie tej jednostki w architekturze IMS wynika z chęci zachowania kompatybilności wstecznej z usługami realizowanymi w sieciach inteligentnych w architekturze CAMEL. Jednostka IM-SSF z jednej strony posiada styk ISC w kierunku sieci IMS (jednostki S-CSCF) a z drugiej styk z protokołem CAP w kierunku aplikacji modelu CAMEL. Dzięki temu można wprowadzić usługi wytworzone w modelu CAMEL do realizacji w architekturze IMS bez konieczności zmiany styku z nimi czyli np. punktów wyzwalania (*trigger points*), maszyny stanów jednostki SSF, protokołu komunikacyjnego CAP.
- Open Service Access Service Capability Server (*OSA-SCS*) – jednostka, która stanowi punkt pośredniczący pomiędzy systemem IMS a środowiskiem usług realizowanych w modelu OSA (*Open Service Access*). Podobnie jak IM-SSF, ta jednostka została również wprowadzona do architektury IMS w celu zachowania kompatybilności z wcześniejszymi realizacjami serwerów w środowisku telekomunikacyjnym, w którym usługi były programowane przy wykorzystaniu OSA Parlay API [29]. W ten sposób OSA Parlay dawała niezależnym dostawcom oprogramowania możliwość dostępu do dodatkowych, specyficznych dla telekomunikacji funkcji sieciowych i informacji o konkretnych użytkownikach oraz możliwość ich użycia w celu dostarczania nowych usług.
- Service Capability Interaction Manager (*SCIM*) – jednostka pełniąca rolę zarządcy interakcji pomiędzy różnymi usługami lub komponentami usługi. Stosowana w sytuacji, gdy usługa lub jej komponenty zaimplementowane są na kilku serwerach aplikacyjnych, ale muszą być „widoczne” w sieci dla jednostek S-CSCF pod jednym adresem – właśnie adresem jednostki SCIM.

W koncepcji systemu IMS zakładano, że nowe usługi będą implementowane na serwerach aplikacyjnych SIP, natomiast jednostki IM-SSF oraz OSA-SCS będą służyły zachowaniu wstecznej kompatybilności, czyli umożliwieniu oferowania usług rozwiniętych wcześniej dla np. sieci inteligentnych. Niezależnie od wybranej metody dostępu, węzeł S-CSCF zawsze komunikuje się z serwerem aplikacyjnym poprzez styk ISC z wykorzystaniem protokołu SIP.

Zgodnie z założeniami, system IMS powinien zapewniać możliwość korzystania z wielu usług, oferowanych z różnych źródeł, tj. z różnych serwerów i od różnych dostawców, zgodnie z subskrypcjami posiadanymi przez abonenta. W szczególności w przypadku, gdy użytkownik posiada subskrypcję dla więcej niż jednej usługi, konieczny jest mechanizm wybierania serwerów aplikacyjnych odpowiedzialnych za poszczególne usługi, a także serwerów w ramach konkretnej usługi.

Informacja o sposobie i kolejności kierowania połączeń do odpowiednich serwerów aplikacyjnych przechowywana jest w bazie HSS. Węzeł HSS przechowuje profil każdego abonenta systemu IMS, a w nim listę reguł sterujących wyborem odpowiednich serwerów aplikacyjnych dla realizacji poszczególnych usług i kolejność, w jakiej powinny być one wywoływane. Lista ta nosi nazwę początkowych kryteriów filtrowania iFC (*Initial Filter Criteria*) i jest przekazywana do węzła S-CSCF podczas procedury rejestracji użytkownika w systemie IMS. Węzeł S-CSCF bezpośrednio odpowiedzialny za wywoływanie usług, przekierowuje przychodzące żądanie zestawienia sesji do odpowiedniego serwera aplikacyjnego zgodnie z regułami wskazanymi na liście iFC.

Główne informacje przekazywane z węzła HSS do węzła S-CSCF obejmują:

- adres serwera aplikacyjnego;
- priorytet serwera aplikacyjnego określający kolejność odwołań do poszczególnych serwerów aplikacyjnych;
- zasady domyślnej obsługi;
- subskrybowane rodzaje usług transportowych;
- punkty wywoływania (*trigger points*);
- dodatkowe informacje o usłudze.

3. Podstawowe procedury sygnalizacyjne w sieci IMS

W specyfikacji systemu IMS opisanych zostało kilkanaście procedur sygnalizacyjnych, które występują podczas normalnej pracy systemu. Procedury te związane są z wywoływaniem usług, stworzeniem możliwości korzystania z sieci (procedura rejestracji), zestawianiem sesji (różne warianty uwzględniające kierunek zestawiania połączenia: wychodzące, przychodzące, rodzaj sieci: PLMN, IMS, PSTN, typ sieci: macierzysta lub obca), kończeniem sesji, zarządzaniem sesjami multimedialnymi, itd.

3.1. Rejestracja w systemie IMS

Celem procedury rejestracji jest stworzenie powiązania pomiędzy nazwą symboliczną (katalogową) użytkownika tzw. identyfikatorem publicznym IMPU (*IP Multimedia Public Identity*) reprezentowanym przez adres SIP URI [15] a adresem IP terminala. To powiązanie przechowywane jest w węźle S-CSCF, który odpowiada za kierowanie wiadomości sygnalizacyjnych do właściwego adresata czyli na właściwy adres IP.

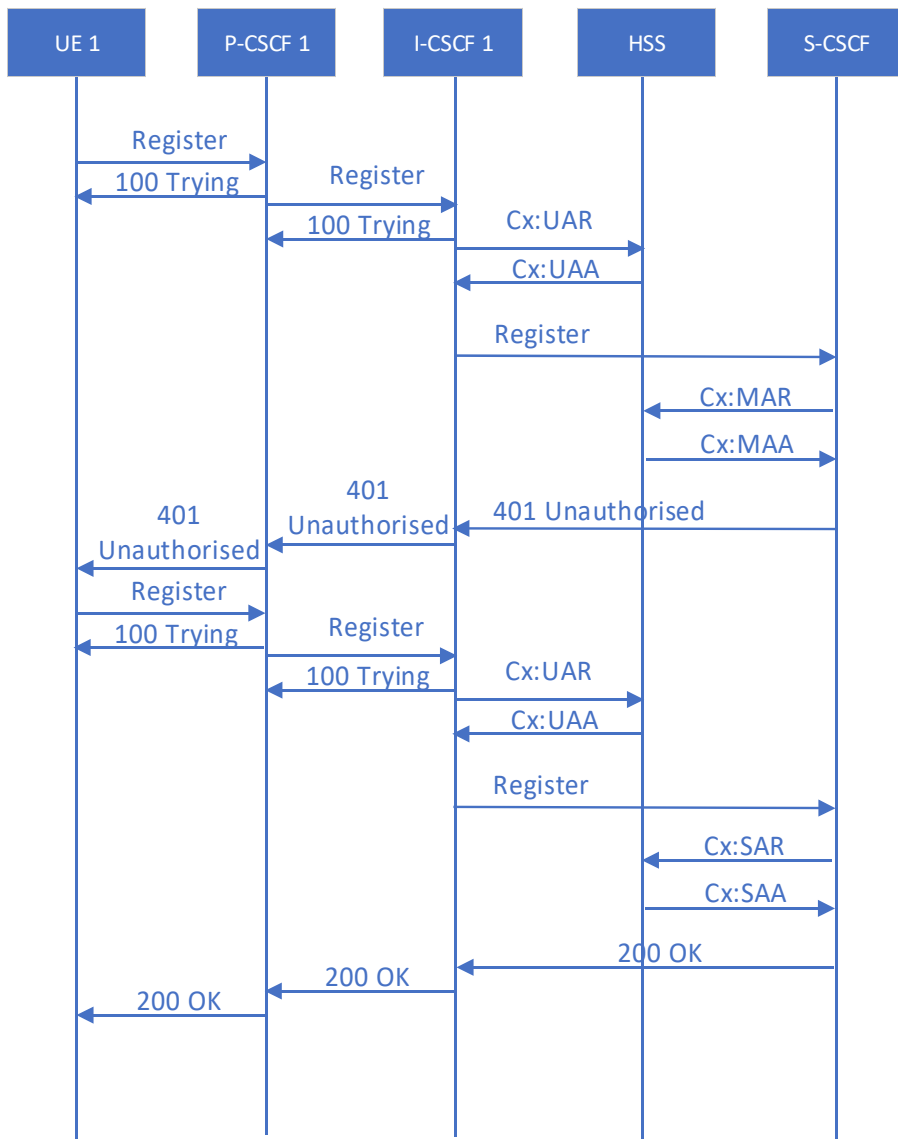
Przebieg rejestracji w systemie IMS jest następujący (rysunek 2):

1. Terminal wysyła wiadomość SIP REGISTER do węzła P-CSCF, stanowiącego jego punkt wejścia do systemu IMS. Wiadomość ta zawiera identyfikator osoby rejestrującej się oraz nazwę domeny macierzystej.
2. Węzeł P-CSCF przetwarza tą wiadomość i wykorzystuje otrzymaną nazwę domeny do przełożenia jej na adres IP węzła I-CSCF. Wysyła wiadomość SIP REGISTER do tego węzła I-CSCF.
3. Węzeł I-CSCF kontaktuje się z węzłem HSS w celu otrzymania informacji koniecznych do właściwego wyboru węzła S-CSCF dla tego użytkownika (na podstawie jego identyfikatora). Węzeł HSS zwraca te informacje do węzła I-CSCF.
4. Węzeł I-CSCF dokonuje wyboru węzła S-CSCF dla użytkownika i kieruje do tego węzła wiadomość SIP REGISTER.
5. Węzeł S-CSCF zauważa, że użytkownik nie został jeszcze zautoryzowany dlatego zwraca się do węzła HSS o dane do uwierzytelnienia.
6. Węzeł S-CSCF wysyła odpowiedź 401 (Not Authorized) z żądaniem uwierzytelnienia zawierającym liczbę losową (*challenge*).
7. Węzeł I-CSCF przekazuje odpowiedź 401 dalej do kolejnego węzła na ścieżce tj. do węzła P-CSCF.
8. Węzeł P-CSCF przekazuje odpowiedź 401 do terminala użytkownika.
9. Po odebraniu odpowiedzi 401 z losową liczbą, terminal oblicza odpowiedź i wysyła ją ponownie w wiadomości SIP REGISTER do węzła P-CSCF.
10. Węzeł P-CSCF (podobnie jak poprzednio) przetwarza tą wiadomość i wykorzystuje otrzymaną nazwę domeny do przełożenia jej na adres IP

- węzła I-CSCF. Wysyła wiadomość SIP REGISTER do tego węzła I-CSCF.
11. Węzeł I-CSCF (podobnie jak poprzednio) kontaktuje się z węzłem HSS aby otrzymać informacje konieczne do właściwego wyboru węzła S-CSCF dla tego użytkownika (na podstawie jego identyfikatora). Węzeł HSS zwraca takie informacje do węzła I-CSCF.
 12. Węzeł I-CSCF dokonuje wyboru węzła S-CSCF dla użytkownika i kieruje do tego węzła wiadomość SIP REGISTER.
 13. Węzeł S-CSCF sprawdza odpowiedź i jeżeli uzna ją za zgodną ściągą z węzła HSS profil użytkownika.
 14. Węzeł S-CSCF potwierdza poprawność rejestracji wysyłając odpowiedź 200 OK.
 15. Węzeł I-CSCF przekazuje odpowiedź 200 OK dalej do kolejnego węzła na ścieżce tj. do węzła P-CSCF.
 16. Węzeł P-CSCF przekazuje odpowiedź 200 OK dalej do terminala użytkownika.

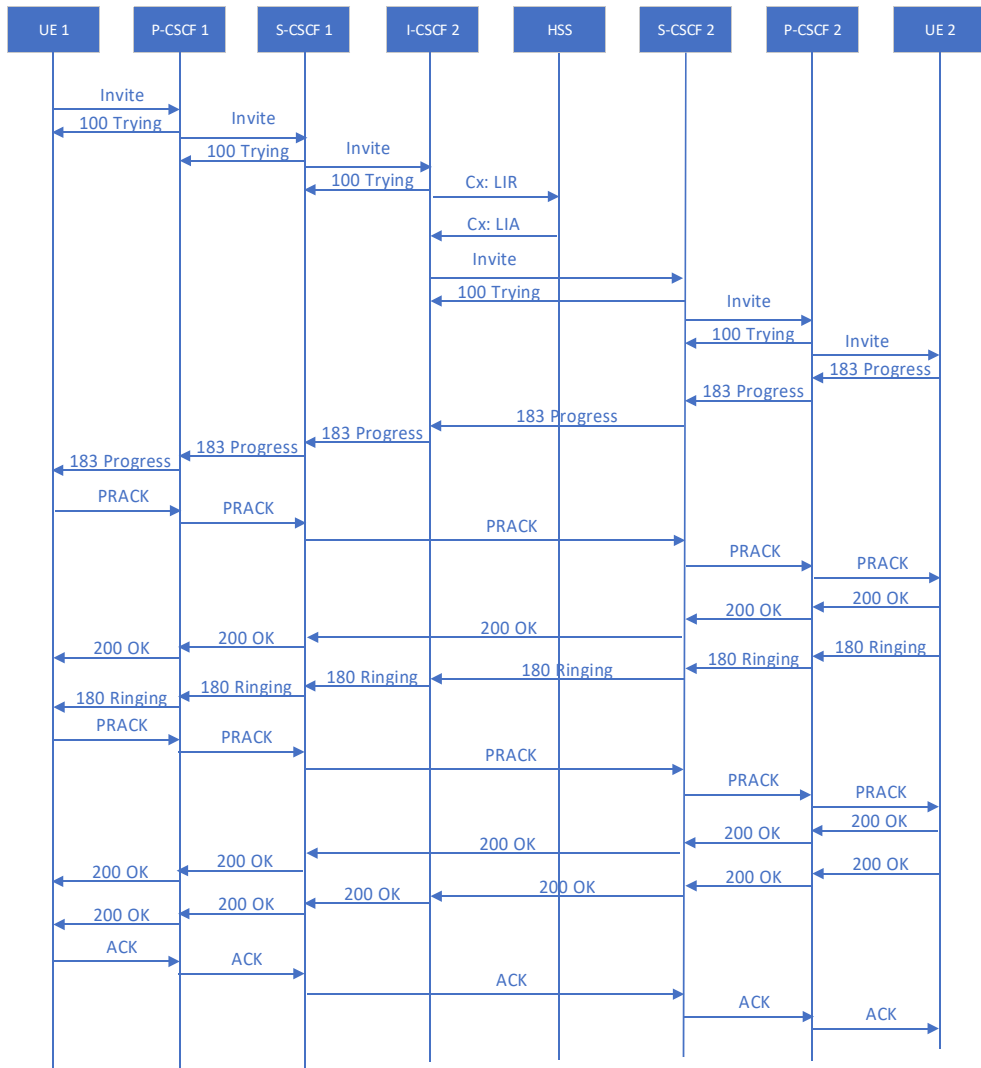
Po poprawnym zarejestrowaniu, terminal może inicjować, a także odbierać sesje. Podczas procedury rejestracji terminal oraz węzeł P-CSCF dowiadują się, który węzeł S-CSCF sieci IMS będzie obsługiwał dany terminal.

W celu utrzymania stanu rejestracji, terminal powinien ją cyklicznie odświeżać, poprzez okresowe wysyłanie wiadomości REGISTER. Jeżeli terminal nie odświeży swojej rejestracji, wówczas węzeł S-CSCF usunie taką rejestrację po upływie określonego czasu, ustalonego podczas rejestracji. Jeżeli terminal chce dokonać wyrejestrowania z systemu IMS, musi wysłać wiadomość REGISTER podając jako okres odświeżania rejestracji wartość 0.



Rysunek 2. Procedura rejestracji – użytkownik początkowo niezarejestrowany [19]

3.2. Zestawienie sesji pomiędzy użytkownikami różnych domen IMS



Rysunek 3. Procedura zestawiania sesji pomiędzy użytkownikami dwóch różnych domen sieci IMS [19]

Wymiana wiadomości sygnalizacyjnych w celu zestawienia sesji pomiędzy dwoma abonentami sieci IMS zarejestrowanymi w różnych domenach jest następująca (rysunek 3):

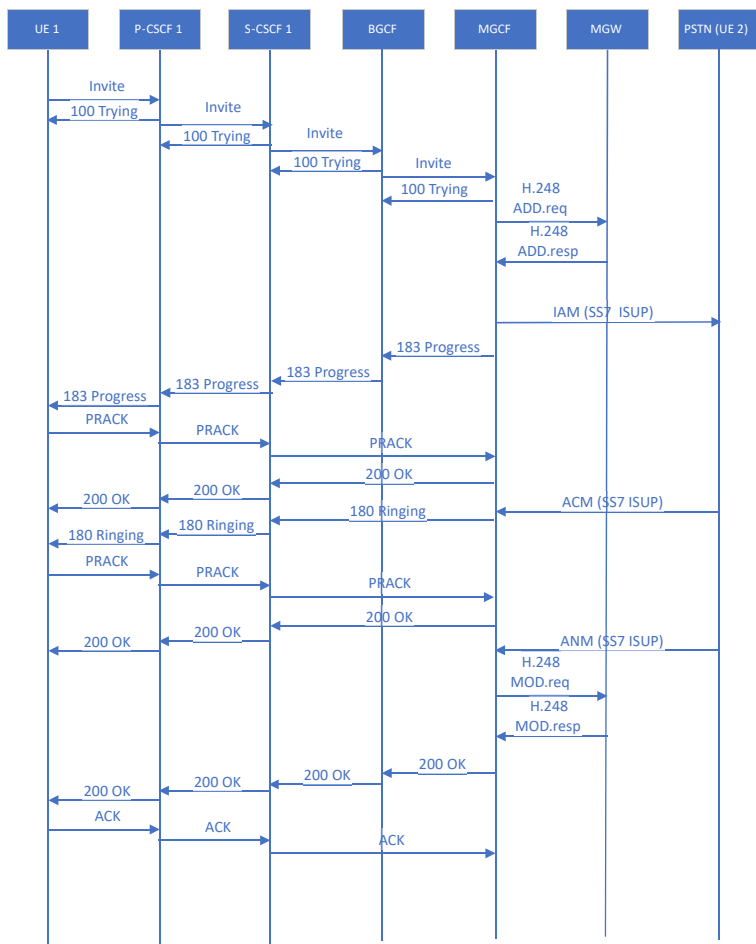
1. Z terminala UE1 wysyłana jest wiadomość Invite w celu zestawienia połączenia. Wiadomość jest wysyłana na adres punktu wejścia do sieci IMS (adres węzła P-CSCF 1), tj. jedyny adres który zna terminal UE1 w sieci IMS.
2. Z węzła P-CSCF 1 wiadomość Invite przekazywana jest do węzła S-CSCF 1 przypisanego, w procesie rejestracji, do obsługi tego konkretnego użytkownika (terminala UE1),
3. W wyniku analizy adresu docelowego (terminala UE2) węzeł S-CSCF 1 decyduje, że wiadomość Invite należy przekazać do domeny IMS 2. W związku z tym przekazuje wiadomość Invite na adres węzła I-CSCF, jedynego który zna w domenie IMS 2.
4. Węzeł I-CSCF 2 kontaktuje się z bazą HSS w celu znalezienia adresu węzła S-CSCF aktualnie obsługującego użytkownika (terminal UE 2) – wysyła pytanie: LIR a następnie odbiera odpowiedź: LIA.
5. Na podstawie informacji zwróconych z bazy HSS, węzeł I-CSCF 2 kieruje wiadomość Invite na adres węzła S-CSCF 2.
6. Z węzła S-CSCF 2 wiadomość Invite zostaje przekazana kolejno do węzła P-CSCF 2 a z niego do terminala docelowego UE2.
7. Na otrzymaną wiadomość Invite, terminal UE 2 odpowiada wiadomością „183 Session Progress”, która stanowi potwierdzenie trwającej procedury zestawiania sesji pomiędzy terminalami UE1 a UE 2. Odpowiedź „183 Session Progress” przechodzi przez te same węzły, przez które przechodziła wiadomość Invite. Informacja o pokonanej drodze (kolejnych węzłach) została zapisana i przeniesiona do terminala UE 2 w nagłówku SIP „Via”, do którego każdy kolejny węzeł na drodze od terminala UE1 do UE2 dopisywał własny adres. Jednocześnie kolejne węzły (z wyjątkiem węzła I-CSCF 2) dopisywały swoje adresy do nagłówka SIP „Record Route”, który został razem z nagłówkiem SIP „Via” przekopiowany z wiadomości Invite do odpowiedzi „183 Session Progress”. Celem nagłówka SIP „Record-Route” jest zwrotne przekazanie terminalowi UE 1 informacji o sekwencji węzłów, którą powinny pokonywać kolejne wiadomości sygnalizacyjne wysyłane przez niego do terminala UE 2.
8. Terminal UE 1 po odebraniu odpowiedzi „183 Session Progress” wysyła potwierdzenie PRACK (*Provisional Acknowledgement*). Obecność tej wiadomości w sekwencji sygnalizacyjnej zależy od ustawień terminali UE 1, UE 2.

- W przypadku wymagania potwierdzenia odpowiedzi wstępnych (*provisional*), takich jak „183 Session Progress”, terminal UE 1 powinien przekazać potwierdzenie odebrania odpowiedzi „183 Session Progress” poprzez wysłanie wiadomości PRACK. Wiadomość PRACK pokonuje drogę podobną do tej pokonanej przez wiadomość Invite z wyjątkiem węzłów I-CSCF oraz HSS, które nie zostały zapisane w nagłówku SIP „Record-Route”. Ominięcie tych węzłów jest celowe, ponieważ na tym etapie zestawiania połączenia węzeł S-CSCF 1 zna już adres węzła S-CSCF 2 i może komunikować się z nim bezpośrednio bez konieczności pośrednictwa węzła I-CSCF 2.
9. Terminal UE 2 w odpowiedzi na otrzymaną wiadomość PRACK wysła „200 OK”. Odpowiedź „200 OK” przemierza tą samą drogę, którą pokonała wiadomość PRACK tzn. omija węzeł I-CSCF 2, którego udział w ścieżce przekazywania wiadomości PRACK jest zbędny. Przebieg trasy (kolejnych węzłów) jest znany węzłowi UE 2, będącemu odbiorcą wiadomości PRACK, na podstawie zawartości nagłówka SIP „Via”. Dzięki informacji zawartej w tym nagłówku, odpowiedź „200 OK” może przejść tą samą drogą z powrotem do terminala UE 1.
 10. W momencie gdy w terminalu UE 2 rozlega się sygnał dzwonienia równocześnie wysyłana jest wiadomość „180 Ringing”. Wiadomość ta, podobnie jak „183 Session Progress” jest częścią transakcji rozpoczętej przez wiadomość „Invite”, zatem przemierza tą samą drogę, którą przemierzała odpowiedź „183 Session Progress”. Oznacza to, że odpowiedź „180 Ringing” również przechodzi przez węzeł I-CSCF 2.
 11. Terminal UE 1 po odebraniu odpowiedzi „180 Ringing” wysła potwierdzenie PRACK (*Provisional Acknowledgement*). Wiadomość PRACK potwierdzająca odebranie odpowiedzi „180 Ringing” pokonuje tą samą drogę, którą pokonała wcześniej wysłana wiadomość PRACK tj. omija węzeł I-CSCF 2 z tych samych powodów, które zostały wyjaśnione w punkcie 8 powyżej.
 12. Terminal UE 2 w odpowiedzi na otrzymaną wiadomość PRACK wysła „200 OK”. Odpowiedź „200 OK” przemierza tą samą drogę, którą pokonała wiadomość PRACK tzn. omija węzeł I-CSCF 2.
 13. W momencie odebrania połączenia, z terminala UE 2 wysyłana jest odpowiedź „200 OK”. Ze względu na fakt, że jest to finalna odpowiedź na wcześniej otrzymaną wiadomość „Invite” (tzn. „200 OK” kończy transakcję rozpoczętą

przez wiadomość „Invite”), droga którą przemierza jest taka sama, jak droga przebyta przez wiadomość „Invite”.

14. Terminal UE 1 po otrzymaniu odpowiedzi „200 OK” wysłała wiadomość ACK potwierdzającą jej odbiór. Wiadomość ACK przechodzi do terminala UE 2 z pominięciem węzła I-CSCF 2, tak jak wcześniej wysłane wiadomości PRACK.

3.3. Zestawienie sesji z sieci IMS do sieci PSTN



Rysunek 4. Procedura zestawiania sesji pomiędzy użytkownikiem sieci IMS a użytkownikiem sieci PSTN [35].

Wymiana wiadomości sygnalizacyjnych w celu zestawienia połączenia pomiędzy abonentem sieci IMS a abonentem sieci PSTN jest następująca (rysunek 4):

1. Z terminala UE1 wysyłana jest wiadomość „Invite” w celu zestawienia sesji. Wiadomość jest wysyłana na adres punktu wejścia do sieci IMS (adres węzła P-CSCF 1) tj. jedyny adres, który zna terminal UE1 w sieci IMS.
2. Z węzła P-CSCF 1 wiadomość „Invite” przekazywana jest do węzła S-CSCF 1 przypisanego, w procesie rejestracji, do obsługi tego konkretnego użytkownika (terminala UE1).
3. W wyniku analizy adresu docelowego (adresu terminala UE2) węzeł S-CSCF 1 konkluduje, że adresat znajduje się w sieci PSTN (tj. poza siecią IMS) wobec czego przekazuje wiadomość „Invite” do węzła BGCF.
4. Węzeł BGCF analizując adres docelowy (tj. adres terminala UE 2) decyduje o punkcie wyjścia do sieci PSTN. Jeżeli domena IMS posiada punkt styku z siecią PSTN, wówczas wiadomość „Invite” zostaje przekazana do węzła MGCF sterującego węzłem MGW, który posiada styk z siecią PSTN.
5. Po otrzymaniu wiadomości „Invite” z numerem terminala docelowego, węzeł MGCF zleca odpowiedniemu węzłowi MGW rezerwację zasobów po stronie sieci IMS (adres IP i port) oraz po stronie sieci PSTN (port TDM) celem zapewnienia drogi dla strumienia mediów. Następnie węzeł MGCF przesyła żądanie zestawienia połączenia do sieci PSTN (wiadomość IAM sygnalizacji SS7) oraz wysyła odpowiedź „183 Session Progress” adresując ją do terminala UE1 przez co sygnalizuje kontynuację procesu zestawiania sesji. Odpowiedź „183 Session Progress” przechodzi do węzła UE1 tą samą drogą, którą przysłała od niego wiadomość „Invite”. Informacja o pokonanej drodze (kolejnych węzłach) została zapisana i przeniesiona do terminala UE 2 w nagłówku SIP „Via”, do którego każdy kolejny węzeł na drodze od terminala UE1 do UE2 dopisywał własny adres. Jednocześnie kolejne węzły (z wyjątkiem węzła BGCF) dopisywały swoje adresy do nagłówka SIP „Record Route”, który został razem z nagłówkiem SIP „Via” przekopiowany z wiadomości „Invite” do odpowiedzi „183 Session Progress”. Celem nagłówka SIP „Record-Route” jest zwrotne przekazanie terminalowi UE 1 informacji o sekwencji węzłów którą powinny pokonywać kolejne wiadomości sygnalizacyjne wysyłane przez niego do terminala UE 2.

6. Terminal UE 1 po odebraniu odpowiedzi „183 Session Progress” wysyła potwierdzenie PRACK (*Provisional Acknowledgement*). Obecność tej wiadomości w sekwencji sygnalizacyjnej zależy od ustawień terminali UE 1 i UE 2. W przypadku wymagania potwierdzania odpowiedzi wstępnych (*provisional*), takich jak „183 Session Progress”, terminal UE 1 powinien przekazać potwierdzenie odebrania odpowiedzi „183 Session Progress” poprzez wysłanie wiadomości PRACK. Wiadomość PRACK pokonuje drogę podobną do tej pokonanej przez wiadomość „Invite” z wyjątkiem węzła BGCF, który nie został zapisany w nagłówku SIP „Record-Route”. Ominięcie tego węzła jest celowe, ponieważ na tym etapie zestawiania połączenia węzeł S-CSCF zna już adres węzła MGCF sterującego węzłem MGW zapewniającym styk z siecią PSTN i może komunikować się z nim bezpośrednio bez konieczności pośrednictwa węzła BGCF.
7. Węzeł MGCF w odpowiedzi na otrzymaną wiadomość PRACK wysyła „200 OK”. Odpowiedź „200 OK”, która przemierza tę samą drogę, którą pokonała wiadomość PRACK tzn. omija węzeł BGCF, ponieważ jego udział w ścieżce przekazywania wiadomości PRACK jest zbędny. Przebieg trasy (kolejnych węzłów) jest znany węzłowi UE 2 tzn. odbiorcy wiadomości PRACK na podstawie zawartości nagłówka SIP „Via”. Dzięki informacji zawartej w tym nagłówku, odpowiedź „200 OK” może przejść tą samą drogą z powrotem do terminala UE 1.
8. Po otrzymaniu z sieci PSTN wiadomości ACM (SS7), potwierdzającej odbiór wiadomości IAM w terminalu UE 2, węzeł MGCF wysyła do terminala UE 1 wiadomość „180 Ringing”, której zadaniem jest informacja zwrotną o wywoływaniu abonenta docelowego (generowaniu sygnału dzwonienia w terminalu UE 2).
9. Terminal UE 1 po odebraniu odpowiedzi „180 Ringing” wysyła potwierdzenie PRACK (*Provisional Acknowledgement*). Wiadomość PRACK potwierdzająca odebranie odpowiedzi „180 Ringing” pokonuje tę samą drogę, którą pokonała wcześniej wysłana wiadomość PRACK tj. omija węzeł BGCF z tych samych powodów, które zostały wyjaśnione w punkcie 6 powyżej.

10. Węzeł MGCF w odpowiedzi na otrzymaną wiadomość PRACK wysyła „200 OK”. Odpowiedź „200 OK” przemierza tą samą drogę, którą pokonała wiadomość PRACK tzn. omija węzeł BGCF.
11. W momencie odebrania połączenia, z terminala UE 2 (w sieci PSTN) wysyłana jest wiadomość ANM (SS7). Po dotarciu tej wiadomości do węzła MGCF, zleca on węzłowi MGW aktywację przetwarzania strumieni mediów. Od tego momentu droga dla strumieni mediów jest w pełni kompletna i może rozpocząć się przekazywanie próbek głosu pomiędzy terminalami UE 1 i UE 2. Jednocześnie węzeł MGCF wysyła odpowiedź „200 OK” zaadresowaną do terminala UE 1. Ze względu na fakt, że jest to finalna odpowiedź na wcześniej otrzymaną wiadomość „Invite”, czyli kończy transakcję rozpoczętą przez wiadomość „Invite”, droga którą przemierza jest taka sama jak droga przebyta przez wiadomość „Invite”.
12. Terminal UE 1 po otrzymaniu odpowiedzi „200 OK” wysyła wiadomość ACK potwierdzającą jej odbiór. Wiadomość ACK przechodzi do terminala UE 2 z pominięciem węzła BGCF, tak jak wcześniej wysyłane wiadomości PRACK.

3.4. Zestawienie sesji z sieci PSTN do sieci IMS

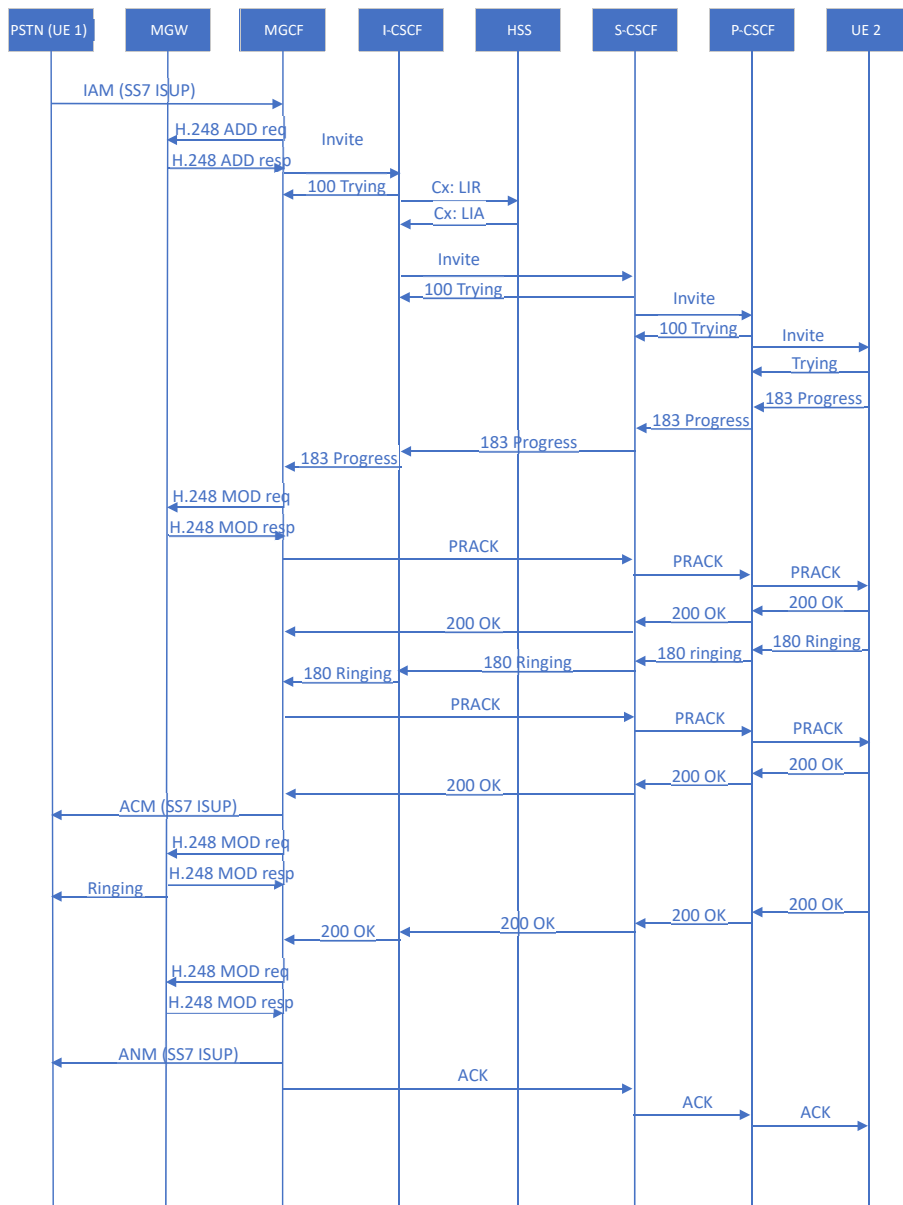
Wymiana wiadomości sygnalizacyjnych w celu zestawienia sesji pomiędzy abonentem sieci PSTN a abonentem sieci IMS jest następująca (rysunek 5):

1. Z terminala UE1 wysyłana jest wiadomość IAM (ISUP SS7) w celu zestawienia połączenia. Wiadomość ta dociera do węzła sieci MGCF na podstawie routing obowiązujecego w sieci PSTN. Węzeł MGCF wysyła do odpowiedniego węzła MGW żądanie rezerwacji zasobów po stronie sieci PSTN (port TDM) i po stronie sieci IMS (adres IP i port RTP). Następnie MGCF generuje wiadomość „Invite”, którą przesyła do węzła I-CSCF, ponieważ nie wie, który węzeł S-CSCF obsługuje abonenta docelowego. Węzeł I-CSCF po odebraniu wiadomości „Invite” wysyła zapytanie do węzła HSS (wiadomość „LIR”) w celu ustalenia adresu S-CSCF węzła obsługującego abonenta docelowego. HSS odpowiada przesyłając wiadomość „LIA” do węzła I-CSCF. Teraz węzeł I-

- CSCF znając adres węzła S-CSCF przesyła do niego wiadomość „Invite”. Następnie węzeł S-CSCF przesyła wiadomość „Invite” dalej do węzła P-CSCF, z którego wiadomość dociera do abonenta docelowego (terminala UE 2).
2. Na otrzymaną wiadomość „Invite”, terminal UE 2 odpowiada wiadomością „183 Session Progress”, która stanowi potwierdzenie zestawiania połączenia pomiędzy terminalami UE1 a UE 2. Odpowiedź „183 Session Progress” przechodzi przez te same węzły, przez które przechodziła wiadomość Invite. Informacja o pokonanej drodze (kolejnych węzłach) została zapisana i przeniesiona do terminala UE 2 w nagłówku SIP „Via”, do którego każdy kolejny węzeł na drodze od węzła MGCF do UE2 dopisywał własny adres. Jednocześnie kolejne węzły (z wyjątkiem węzła I-CSCF 2) dopisywały swoje adresy do nagłówka SIP „Record Route”, który został razem z nagłówkiem SIP „Via” przekopiowany z wiadomości Invite do odpowiedzi „183 Session Progress”. Celem nagłówka SIP „Record-Route” jest zwrotne przekazanie węzłowi MGCF informacji o sekwencji węzłów, którą powinny pokonywać kolejne wiadomości sygnalizacyjne wysyłane przez niego do terminala UE 2.
 3. Węzeł MGCF po odebraniu odpowiedzi „183 Session Progress” przekazuje węzłowi MGW informacje o adresie IP i porcie terminala UE 2 na potrzeby przesyłania strumienia mediów (wiadomość H.248 MOD req). Następnie wysyła potwierdzenie „PRACK” (*Provisional Acknowledgement*). Obecność tej wiadomości w sekwencji sygnalizacyjnej zależy od ustawień węzłów MGCF i UE 2. W przypadku wymagania potwierdzenia odpowiedzi wstępnych (*provisional*), takich jak „183 Session Progress”, węzeł MGCF powinien przekazać potwierdzenie odebrania odpowiedzi „183 Session Progress” poprzez wysłanie wiadomości PRACK. Wiadomość PRACK pokonuje drogę podobną do tej pokonanej przez wiadomość Invite z wyjątkiem węzłów I-CSCF oraz HSS, które nie zostały zapisane w nagłówku SIP „Record-Route”. Ominięcie tych węzłów jest celowe, ponieważ na tym etapie zestawiania połączenia węzeł MGCF zna już adres węzła S-CSCF i może komunikować się z nim bezpośrednio bez konieczności pośrednictwa węzła I-CSCF.
 4. Terminal UE 2 w odpowiedzi na otrzymaną wiadomość PRACK wysyła „200 OK”. Odpowiedź „200 OK” przemierza tą samą drogę, którą pokonała wia-

- domość PRACK tzn. omija węzeł I-CSCF, którego udział w ścieżce przekazywania wiadomości PRACK jest zbędny. Przebieg trasy (kolejnych węzłów) jest znany węzłowi UE 2, będącemu odbiorcą wiadomości PRACK na podstawie zawartości nagłówka SIP „Via”. Dzięki informacji zawartej w tym nagłówku, odpowiedź „200 OK” może przejść tą samą drogą z powrotem do węzła MGCF.
5. W momencie gdy w terminalu UE 2 rozlega się sygnał dzwonienia równocześnie wysyłana jest wiadomość „180 Ringing”. Wiadomość ta, podobnie jak „183 Session Progress”, jest częścią transakcji rozpoczętej przez wiadomość „Invite”, zatem przemierza tą samą drogę, którą przemierzała odpowiedź „183 Session Progress”. Oznacza to, że odpowiedź „180 Ringing” również przechodzi przez węzeł I-CSCF.
 6. Węzeł MGCF po odebraniu odpowiedzi „180 Ringing” wysyła potwierdzenie PRACK (*Provisional Acknowledgement*). Wiadomość PRACK potwierdzająca odebranie odpowiedzi „180 Ringing” pokonuje tą samą drogę, którą pokonała wcześniej wysłana wiadomość PRACK, tj. omija węzeł I-CSCF 2 z tych samych powodów, które zostały wyjaśnione w punkcie 3 powyżej.
 7. Terminal UE 2 w odpowiedzi na otrzymaną wiadomość PRACK wysyła „200 OK”. Odpowiedź „200 OK” przemierza tą samą drogę, którą pokonała wiadomość PRACK tzn. omija węzeł I-CSCF. Gdy węzeł MGCF odbierze tą odpowiedź, przesyła do terminala UE 1 wiadomość ACM (ISUP SS7) i jednocześnie zleca węzłowi MGW wygenerowanie tonu dzwonienia (wiadomość H.248 MOD req) w kierunku terminala UE 1.
 8. W momencie odebrania połączenia, z terminala UE 2 wysyłana jest odpowiedź „200 OK”. Ze względu na fakt, że jest to finalna odpowiedź na wcześniej otrzymaną wiadomość „Invite”, tzn. odpowiedź „200 OK” kończy transakcję rozpoczętą przez wiadomość „Invite”, droga którą przemierza jest taka sama jak droga przebyta przez wiadomość „Invite”.
 9. Gdy odpowiedź „200 OK” dotrze do węzła MGCF, zleca on węzłowi MGW (wiadomość H.248 MOD) wstrzymanie generowania tonu dzwonienia w kierunku terminala UE 1. Jednocześnie wysyła wiadomość ANM (SS7 ISUP) informując w ten sposób terminal UE 1, że użytkownik terminala UE 2 odebrał połączenie. Wysyła również wiadomość ACK potwierdzającą odbiór odpowiedzi „200 OK”.

Wiadomość ACK przechodzi do terminala UE 2 z pominięciem węzłów I-CSCF i HSS, tak jak wcześniej wysyłane wiadomości PRACK.



Rysunek 5. Procedura zestawiania sesji inicjowana od abonenta sieci PSTN do abonenta sieci IMS [35]

4. Realizacja usług w sieci IMS

W systemie IMS usługi są świadczone przez serwery aplikacyjne (*Application Servers; AS*) zlokalizowane w płaszczyźnie aplikacyjnej. Ogólna koncepcja wywoływania usług opiera się na przekazaniu sterowania z płaszczyzny sterowania, a dokładniej z węzła S-CSCF obsługującego danego abonenta, do płaszczyzny aplikacyjnej, czyli do konkretnego serwera aplikacyjnego w celu wykonania określonej logiki usługowej.

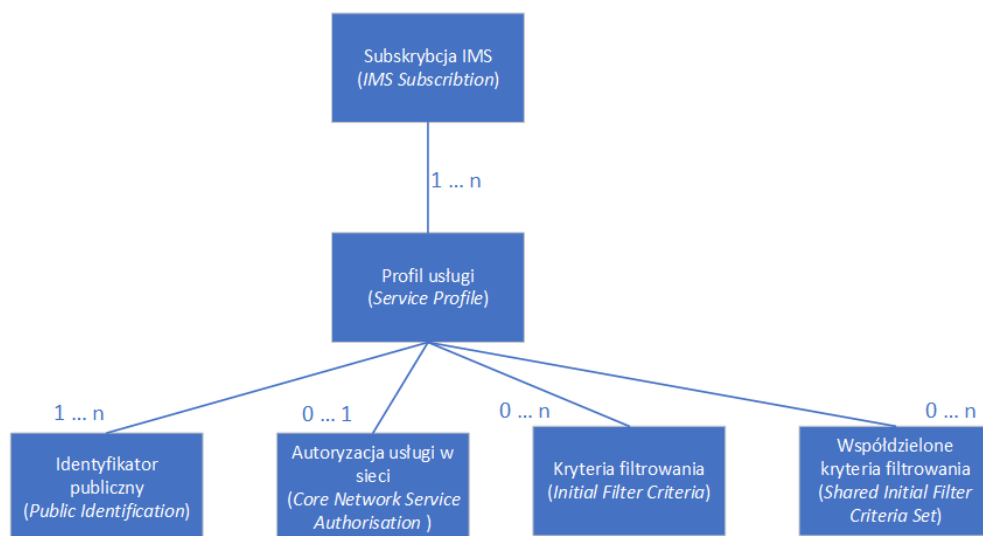
Tak zdefiniowany mechanizm wywoływania usług, podobnie jak w sieciach inteligentnych, z których ta koncepcja wywodzi się, wymaga określania warunków, w których ma dochodzić do wspomnianego przekazania sterowania czyli do przekierowania wiadomości sygnalizacyjnych SIP do odpowiedniego serwera aplikacyjnego. Informacja o warunkach decydujących o przekazaniu sterowania, przechowywana jest w tzw. początkowych kryteriach iFC (*initial Filter Criteria*), które zapisane są w profilu każdego abonenta sieci IMS. Kryteria iFC precyzują warunki wykonania przekierowania sygnalizacji poprzez odniesienie się do takich elementów wiadomości SIP jak użyta metoda np. Invite, zawartość adresu Request URI, zawartość nagłówków SIP, kierunek połączenia: wychodzące (*originating*) lub przychodzące (*terminating*).

Podczas procedury rejestracji abonenta w sieci IMS, profil użytkownika razem z kryteriami iFC jest kopiowany z miejsca przechowywania tj. z węzła HSS do węzła S-CSCF przypisanego do obsługi tego abonenta. Dzięki temu, węzeł S-CSCF, przez który przechodzi cała sygnalizacja wysyłana i odbierana przez danego abonenta, może weryfikować zaistnienie określonych warunków wywołania usługi opisanych w kryteriach iFC i w konsekwencji przekazać sterowanie do płaszczyzny aplikacyjnej.

4.1. Profil użytkownika

Profil użytkownika, oprócz kryteriów iFC zawiera informacje specyficzne dla danego abonenta. W systemie IMS, profil użytkownika, czyli pojedyncza subskrypcja, może zawierać jeden lub więcej profili usług (*Service profile*), z których każdy iden-

tyfikuje dostępną dla tego abonenta usługę oraz warunki jej wywoływania. Zależności pomiędzy profilem użytkownika, profilami usług oraz ich elementami pokazane są na rysunku 6 [30].



Rysunek 6. Struktura profilu użytkownika w systemie IMS

Operator sieci tworzy użytkownikowi profil w systemie IMS w momencie wykonania subskrypcji, czyli wykupienia abonamentu. Profil użytkownika jest jednoznacznie identyfikowany przez identyfikator prywatny IMPI (*IP Multimedia Private Identity*) i przenoszony z węzła HSS do węzła S-CSCF w przypadku dwóch operacji: SAA (*Server Assignment Answer*) oraz PPR (*Push Profile Request*). Fizycznie jest on przekazywany w jednym z atrybutów AVP (*Attribute Value Pair*) protokołu Diameter w postaci dokumentu XML.

Profil użytkownika składa się z profili usług, a każdy profil usługi zbudowany jest z 4 części:

- identyfikatora publicznego (*IMPU*);
- autoryzacja usługi w sieci (*Core Network Service Authorisation*);
- kryteriów filtrowania iFC (*initial Filter Criteria*);

- zestawu współdzielonych kryteriów filtrowania iFC (*Shared Initial Filter Criteria Set*).

Identyfikator publiczny wskazuje na czyją rzecz dana usługa ma być wykonana. Identyfikator publiczny może wskazywać na użytkownika (identyfikator publiczny użytkownika – *IMPU*) lub usługę (identyfikator publiczny usługi – *PSI* czyli *Public Service Identity*).

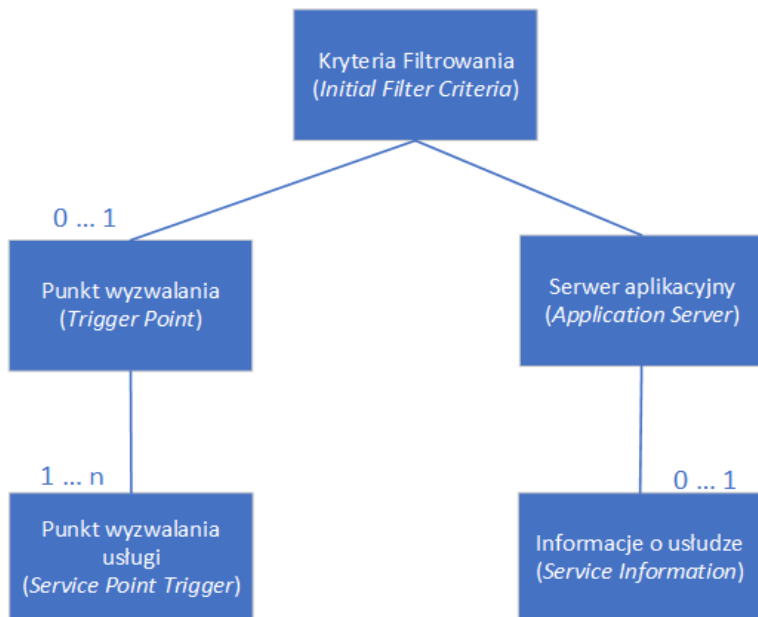
Każdy identyfikator publiczny użytkownika zawiera opcjonalną nazwę symboliczną oraz skojarzony wskaźnik określający czy identyfikator ten może być wykorzystywany w komunikacji w systemie IMS innej niż związana z rejestracją. Jeżeli nazwa symboliczna (*display name*) jest podana, wówczas jest ona komunikowana przez S-CSCF do terminala oraz do węzła P-CSCF podczas rejestracji. Publiczny identyfikator usługi może przybierać postać dokładnej nazwy (np. *pokojkonferencyjny@serwerkonferencji1.pl*) lub nazwy pasującej do wzorca (*Wildcarded*), np. *sip:chatlist!*!@jakasdomena.pl* będzie odpowiadać usługom których URI zaczyna się od *sip:chatlist* a kończy na *@jakasdomena.pl*.

Autoryzacja usługi (*Core Network Service Authorisation*) określa do jakich usług i w jakim zakresie abonent ma dostęp. Autoryzacja może odbywać się z wykorzystaniem list identyfikatorów usług komunikacyjnych IMS tzw. *ICSI* (*IMS Communicatin Service Identification*) lub polityki dostępu do mediów (*media policy*).

Pierwszy sposób opiera się na porównaniu identyfikatora usługi zapisanego w nagłówku P-Preferred-Service [31] wiadomości SIP z listą identyfikatorów usług dostępnych dla danego abonenta, która jest przechowywana w bazie HSS, a po rejestracji abonenta również w węzle S-CSCF. Po pozytywnej weryfikacji węzeł S-CSCF zamienia nagłówek P-Preffered-Service na P-Asserted-Service i przekazuje wiadomość dalej w celu wywołania usługi.

Drugi sposób autoryzacji (*media policy*) polega na ograniczaniu zakresu świadczenia usługi poprzez dopuszczenie używania tylko wskazanych kodeków lub parametrów przekazu strumieni opisanych w części SDP nagłówka SIP. W ten sposób można zrealizować różnicowanie klientów na klasy. Na przykład użytkownicy klasy Premium mogą korzystać z kodeków HD (*High Definition*), a klasy Standard tylko ze zwykłych kodeków. W innym rozwiązaniu klienci klasy Premium mogliby korzystać ze strumieni multimedialnych (audio i video), a klienci klasy Standard tylko ze strumieni audio.

Kryteria iFC (*initial Filter Criteria*) mają strukturę złożoną, która została pokazana na rysunku 7.



Rysunek 7. Struktura kryteriów iFC

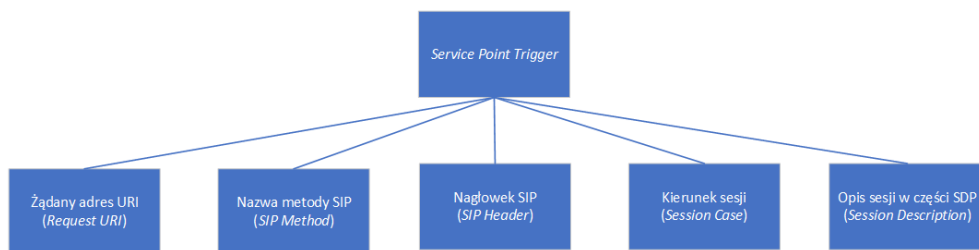
Według specyfikacji 3GPP TS 29.228 [30], kryteria iFC zawierają jeden lub zero punktów wyzwalania (*Trigger point*) oraz jeden serwer aplikacyjny. Każde kryterium iFC w obrębie jednego profilu usługi posiada unikalny priorytet (określony przez liczbę całkowitą), który wykorzystywany jest przez węzeł S-CSCF. W przypadku, gdy istnieje wiele kryteriów iFC, ich sprawdzenie odbywa się w kolejności wyznaczonej przez priorytet, zaczynając od najniższych liczb.

Punkt wyzwalania (*Trigger point*) opisuje warunki, które muszą zostać spełnione, aby zdecydować o wywołaniu usługi, tzn. przekazaniu sterowania do serwera aplikacyjnego. Jeżeli punkt wyzwalania nie został zdefiniowany, za każdym razem następować będzie bezwarunkowe odwołanie do serwera aplikacyjnego.

Każdy punkt wyzwalania zawiera jeden lub więcej punktów wyzwalania usługi (*Service point trigger*), co pokazano schematycznie na rysunku 7. Punkt wyzwalania usługi składa się z następujących elementów (rysunek 8):

- pole ‘Request-URI’ identyfikuje adresata z zapytania SIP np. `infosport@ims.pl`;
- pole ‘SIP method’ określa typ wiadomości SIP (np. INVITE lub MESSAGE);
- pole ‘SIP Header’ zawiera informacje związane z nagłówkami wiadomości SIP. Punkt wyzwalania usługi może być oparty o występowanie lub brak konkretnych pól nagłówka wiadomości lub ich treść. Treść pól nagłówka wiadomości SIP jest ciągiem tekstowym, który może być analizowany jak wyrażenie regularne, np. może to być wyszukiwanie konkretnego imienia „Jan” w nagłówku pola FROM;
- pole ‘Session Case’ może przyjmować jedną z 4 dozwolonych wartości, tj. “Originating”, “Terminating”, “Originating Unregistered” lub “Terminating Unregistered”, które wskazują na jakim etapie przekazywania wiadomości sygnalizacyjnych reguły iFC powinny być sprawdzane – czy to po stronie wywołującej usługę (*Originating*), po stronie wywoływanej (*Terminating*), czy dla użytkowników zarejestrowanych (*Registered*), czy niezarejestrowanych (*Unregistered*);
- Pole “Session description” definiuje punkt wyzwalania usługi w oparciu o treści przenoszone w protokole SDP (*Session Description Protocol*) w ramach wiadomości SIP.

Punkty wyzwalania usługi mogą być łączone za pomocą operatorów logicznych: “i”, “lub”, “negacja”.



Rysunek 8. Wewnętrzna struktura punktu wyzwalania usługi (*Service Point Trigger*)

4.2. Serwer aplikacyjny

W strukturze kryteriów iFC, pole AS (*Application Server*) definiuje aplikację, do której przekierowywana jest sygnalizacja SIP w przypadku spełnienia warunków zdefiniowanych w punktach wyzwalania. Pole to może zawierać również informację na temat domyślnego sposobu obsługi połączenia tzn. działań podejmowanych w przypadku niedostępności serwera aplikacyjnego. Domyślna obsługa połączenia może polegać na kończeniu sesji lub dalszym jej kontynuowaniu tj. przekazaniu sterowania do kolejnego elementu z pominięciem niedostępnego serwera aplikacyjnego.

Po otrzymaniu przekierowanego zapytania SIP z węzła S-CSCF, serwer aplikacyjny zaczyna właściwą usługę. W celu realizacji usługi serwer aplikacyjny może pracować w jednym z następujących trybów [32]:

- tryb klienta po stronie wywoływanej (*Terminating User Agent*) – w tym trybie węzeł AS działa jako terminal wywoływany. Ten tryb ma zastosowanie np. przy realizacji poczty głosowej;
- tryb klienta po stronie wywołującej (*Originating User Agent*) – w tym trybie węzeł AS działa jako oprogramowanie SIP na terminalu i może wysyłać zapytania SIP do użytkowników. Na przykład serwer konferencyjny może wysłać wiadomość SIP INVITE do zdefiniowanej grupy użytkowników o konkretnej godzinie w celu stworzenia połączenia telekonferencyjnego;
- tryb serwera przekierowującego (*Redirect server*) – węzeł AS informuje stronę wywołującą o nowej lokalizacji użytkownika wywoływanego lub o alternatywnych usługach, które mogą być dostarczone, żeby obsłużyć sesję. Ten tryb pracy węzła AS może być stosowany, aby przekierować stronę wywołującą pod inny adres np. na stronę WWW;
- tryb SIP-proxy – węzeł AS przetwarza zapytanie a następnie zwraca je do węzła S-CSCF (czyli działa jako pośrednik – proxy). Podczas przetwarzania węzeł AS może dodawać, usuwać nagłówki SIP oraz modyfikować ich treść zgodnie ze specyfikacją zawartą w [15];
- Tryb B2BUA (*Back-to-Back User Agent*) – węzeł AS generuje nowe zapytanie SIP w ramach nowego dialogu, które przesyła do węzła S-CSCF.

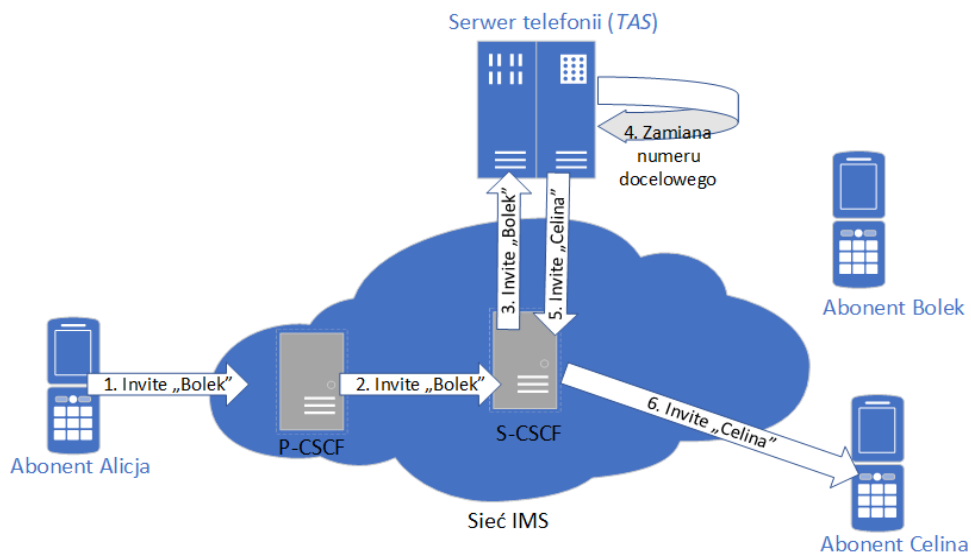
5. Przykład realizacji dodatkowej usługi telefonicznej na platformie OpenIMSCore

Komercyjne platformy IMS stosowane przez operatorów telekomunikacyjnych są bardzo kosztowne. Dla zastosowań akademickich takich jak dydaktyka lub badania dostępne są implementacje typu Open Source. Jedną z bardziej rozpowszechnionych platform tego typu jest OpenIMSCore [8], platforma rozwinięta w ramach projektu prowadzonego przez Instytut FOKUS Fraunhofer.

OpenIMSCore udostępniła tylko podzbiór funkcji zdefiniowanych w dokumentach 3GPP. W oprogramowaniu, które można pobrać ze strony projektu [8] dostępne są funkcje: P-CSCF, I-CSCF, S-CSCF oraz HSS. Oprogramowanie działa na systemach operacyjnych typu Linux, aczkolwiek rekomendowana jest konkretna dystrybucja – Ubuntu. Po pomyślnej instalacji oprogramowania, uruchomienie funkcji P-CSCF, I-CSCF, S-CSCF odbywa się poprzez wykonanie skryptów napisanych w powłocie: `p-cscf.sh`, `s-cscf.sh`, `i-cscf.sh` a węzła HSS poprzez wykonanie skryptu `startup.sh`. Do konfiguracji bazy HSS udostępnione jest GUI oparte na przeglądarce Web.

W celu prezentacji sposobu konfiguracji oraz działania platformy OpenIMSCore, poniżej został opisany przykład realizacji jednej z usług dodatkowych telefonii pakietowej. Usługa polega na bezwarunkowym przekierowaniu połączenia adresowanego do abonenta „Bolek” na numer abonenta „Celina”. W telekomunikacji usługa ta w skrócie nazywana jest CFU (*Call Forward Unconditional*) i stosowana na przykład przy tymczasowej zmianie lokalizacji (w sieci stacjonarnej) lub numeru (w sieciach mobilnych lub stacjonarnych) abonenta bez konieczności ujawniania tych zmian stronie wywołującej. Ogólny schemat przepływu danych w usłudze bezwarunkowego przekierowania połączenia, pokazany został na rysunku 9.

W systemie IMS usługa CFU uruchamiana jest na serwerze aplikacyjnym, który wykonuje logikę związaną ze zmianą kierowania połączenia. Serwer aplikacyjny przeznaczony do realizacji funkcji dodatkowych telefonii pakietowej określany jest mianem TAS (*Telephony Application Server*).



Rysunek 9. Scenariusz wymiany wiadomości dla usługi bezwarunkowego przekierowania połączenia

W schemacie przedstawionym na rysunku 9 abonent „Alicja” inicjuje połączenie wysyłając wiadomość SIP Invite z numerem adresata tj. abonenta „Bolek”, który ma uaktywnioną usługę przekierowania połączeń przychodzących na numer abonenta „Celina”. Wiadomość SIP Invite dociera do węzła P-CSCF, który jest punktem wejścia do systemu IMS, a z niego do węzła S-CSCF obsługującego abonenta „Bolek”. W węzle S-CSCF, w wyniku odpowiednio ustawionych kryteriów iFC dla połączeń przychodzących do abonenta „Bolek”, następuje wywołanie usługi poprzez skierowanie wiadomości SIP Invite do serwera TAS. W serwerze TAS następuje wykonanie logiki usługi bezwarunkowego przekierowania połączenia poprzez podstawienie numeru abonenta „Celina” jako adresata wiadomości SIP Invite. Wiadomość SIP Invite ze zmienionym adresem (polem Request-URI) wraca do węzła S-CSCF, a z niego jest kierowana do terminala abonenta „Celina”.

W naszej implementacji serwer TAS został zrealizowany z użyciem oprogramowanie Open Source rozwiniętego w ramach projektu Kamailio [33] w wersji 3.0.

Został on zainstalowany na maszynie wirtualnej z systemem operacyjnym Linux Debian w wersji 5. Oprogramowanie OpenIMSCore (HSS, P-CSCF, I-CSCF, S-CSCF) zostało zainstalowane na osobnej maszynie wirtualnej z systemem operacyjnym Linux Ubuntu w wersji 9. Jako oprogramowanie klienckie (softphone) została użyta aplikacja Boghe IMS Client. Prawidłowe działanie usługi wymagało uprzedniego skonfigurowania kryteriów iFC dla abonenta „Bolek” oraz serwera TAS.

5.1. Konfiguracja kryteriów iFC

Wszystkie opisane poniżej działania konfiguracyjne wykonane zostały poprzez interfejs GUI zrealizowany jako strona Web dostępna na serwerze HSS. Konfiguracja kryteriów iFC wymagała, aby użytkownicy, których one dotyczą byli uprzednio utworzeni i skonfigurowani w bazie HSS.

Private User Identity -IMPI-

ID	10
Identity*	alicja@open-ims.test
Secret Key*	alicja
Authentication Schemes*	
Digest-AKAv1 (3GPP)	<input checked="" type="checkbox"/>
Digest-AKAv2 (3GPP)	<input checked="" type="checkbox"/>
Digest-MD5 (FOKUS)	<input checked="" type="checkbox"/>
Digest (CableLabs)	<input checked="" type="checkbox"/>
SIP Digest (3GPP)	<input type="checkbox"/>
HTTP Digest (ETSI)	<input checked="" type="checkbox"/>
Early-IMS (3GPP)	<input checked="" type="checkbox"/>
NASS Bundled (ETSI)	<input checked="" type="checkbox"/>
All	<input type="checkbox"/>
Default	Digest-AKAv1-MD5
AMF*	0000

Associate an IMSU

IMSU Identity:

Associated IMSU

ID	IMSU Identity	Delete
7	alicja	<input type="checkbox"/>

Create & Bind new IMPU +

Associate IMPU(s)

IMPU Identity:

Warning: The current IMPI will be associated with all the corresponding IMPUs (within the same implicit-set)!

List of associated IMPUs

ID:	IMPU Identity:	Delete:
7	sip:alicja@open-ims.test	<input type="checkbox"/>

Push Cx Operation

Apply for:

Execute:

Rysunek 10. Widok menu „Private User Identity” do konfiguracji identyfikatora IMPI

Utworzenie użytkowników (abonentów) systemu IMS polegało na wykreowaniu identyfikatorów prywatnego – IMPI (*IP Multimedia Private Identity*) i publicznego

– IMPU (IP Multimedia Public Identity) oraz połączeniu ich w subskrypcję IMS (IMS subscription). Na rysunkach 10-12 pokazano szczegółową zawartość kolejnych menu służących do konfiguracji odpowiednio identyfikatorów IMPI, IMPU oraz IMSU. Pokazane menu wypełnione zostały przykładowymi danymi dla użytkownika „Alicja”.

Public User Identity -IMPU-

ID	7
Identity*	sip:alicja@open-ims.test
Barring	<input type="checkbox"/>
Service Profile*	default_sp
Implicit Set	7
Charging-Info Set	default_charging_set
Can Register	<input checked="" type="checkbox"/>
IMPU Type*	Public_User_Identity
Wildcard PSI	
PSI Activation	<input type="checkbox"/>
Display Name	Alicja
User-Status	REGISTERED

Mandatory fields were marked with "*"

Save Refresh Delete

Add IMPU(s) to Implicit-Set

IMPU Identity Add

List IMPUs from Implicit-Set

ID	IMPU Identity	Delete
7	sip:alicja@open-ims.test	<input type="checkbox"/>

Add Visited-Networks

Select Visited-Network...

List of Visited Networks

ID	Identity	Delete
1	open-ims.test	<input type="checkbox"/>

Associate IMPI(s) to IMPU

IMPI Identity

Warning: This IMPI will be associated with all the corresponding IMPUs (within the same implicit-set!)

List of associated IMPIs

ID	IMPI Identity	Delete
10	alicja@open-ims.test	<input type="checkbox"/>

Push Cx Operation

Apply for User-Data

Rysunek 11. Widok menu „Public User Identity” do konfiguracji identyfikatora IMPU

IMS Subscription -IMSU-

ID	7
Name*	alicja
Capabilities Set	cap_set1
Preferred S-CSCF	scscf1
S-CSCF Name	sip:scscf.open-ims.test:6060
Diameter Name	scscf.open-ims.test

Mandatory fields were marked with "*"

Save Refresh Delete

Create & Bind new IMPI +

Associate IMPI(s)

IMPI Identity

List of associated IMPIs

ID	IMPI Identity	Delete
10	alicja@open-ims.test	<input type="checkbox"/>

Rysunek 12. Widok menu „IMS Subscription”

Kryteria iFC, decydujące o przekazaniu sterowania do płaszczyzny aplikacyjnej, są częścią profilu usługi (*Service Profile*), którego konfiguracji dokonuje się w menu „Service->Service Profiles”. W zasadzie profil usługi to zestaw kryteriów iFC decydujących o kolejności wywoływania usług lub ich komponentów. Powiązanie pomiędzy abonentem a profilem usługi tj. określenie, z których usług może korzystać konkretny abonent, następuje w menu „User identities” -> „Public User Identity” (rysunek 11). Na rysunku 13 pokazano widok z konfiguracji profilu usługi „TAS_sp” (*TAS Service Profile*), w którym widać dodane tylko jedno kryterium iFC o nazwie „tas_ifc”.

Service Profile -SP-

ID	2
Name*	TAS_sp
Core Network Service Auth	0

Mandatory fields were marked with "*"

Attach IFC

Attach Shared-IFC-Set

List of attached IFCs

ID	IFC Name	Priority	Detach
2	tas_ifc	0	<input type="checkbox"/>

List of attached Shared-IFC-Sets

ID-Set	Name	Detach
--------	------	--------

Rysunek 13. Konfiguracja profilu usługi TAS_sp.

Konfiguracja kryteriów iFC odbywa się w menu „Initial Filter Criteria” i obejmuje ustalenie wartości następujących parametrów: nazwa (*Name*) identyfikująca kryterium iFC np. „tas_ifc”, nazwa powiązanego punktu wyzwalania (*Trigger Point*) np. „tas_tp”, nazwa identyfikująca serwer aplikacyjny (*Application Server*) np. „tas_as” oraz określenie wymagań dotyczących statusu użytkowników korzystających z tego konkretnego kryterium iFC (*Profile Part Indicator*) np. czy musi być zarejestrowany (*Registered*). Konfiguracja kryteriów iFC dla naszej usługi przekierowania CFU została pokazana na rysunku 14.

Initial Filter Criteria -iFC-

ID	2
Name*	tas_ifc
Trigger Point	tas_tp
Application Server*	TAS_as
Profile Part Indicator	Registered

Mandatory fields were marked with "*"

Rysunek 14. Konfiguracja kryteriów iFC dla usługi przekierowania CFU

Punkt wyzwalania (*Trigger Point*), który jest jednym z elementów kryteriów iFC, definiuje konkretne warunki, których spełnienie powoduje przekazanie sterowania do serwera aplikacyjnego. Konfiguracja punktu wyzwalania dla przykładu rozważanej usługi CFU, została pokazana na rysunku 15.

Trigger Point -TP-

ID	2
Name*	tas_tp
Condition Type CNF*	Disjunctive Normal Forma

Mandatory fields were marked with "*"

Attach IFC

Select IFC...

List of attached IFCs

ID	IFC Name	Detach
2	tas_ifc	<input type="checkbox"/>

Add SPTs to Trigger Point

Not	<input type="checkbox"/>	Request URI	sip:bolek@open-ims.test	<input type="button" value="Delete"/>
AND				
Not	<input type="checkbox"/>	SIP Method	INVITE	<input type="button" value="Delete"/>
AND				
Not	<input type="checkbox"/>	Session Case	Term - Req	<input type="button" value="Delete"/>
AND				
		Request-URI	<input type="button" value="Add"/>	
OR				
		Request-URI	<input type="button" value="Add"/>	

Rysunek 15. Konfiguracja parametrów punktu wyzwalania dla usługi przekierowania CFU

Definicja punktu wyzwalania (*Trigger Point*) obejmuje określenie jego unikalnej nazwy (*name*) np. „tas_tp”, powiązanie go z istniejącym kryterium iFC (*List of attached IFCs*) np. „tas_ifc” oraz określenie wartości dla konkretnych elementów wiadomości sygnalizacyjnej SIP, których wystąpienie spowoduje przekierowanie wiadomości do serwera aplikacyjnego. Elementy, których wartości możemy określać, obejmują adres „Request URI” decydujący o routingu wiadomości SIP, metodę SIP, dowolny nagłówek wiadomości SIP oraz kierunek połączenia (*Session Case*) określający czy analiza spełnienia warunków ma nastąpić po stronie inicjującej (*Origin – Req*) czy po stronie odbierającej (*Term – Req*).

Do konfiguracji usługi CFU dla użytkownika „Bolek” należy przypisać parametrom „Request URI”, „SIP Method” oraz „Session Case” takie wartości, jak pokazane na Rysunku 15. Z definicji usługi CFU dla użytkownika „Bolek” wynika, że powinna być ona wywoływana tylko dla użytkownika „Bolek”, podczas zestawiania do niego sesji. Dlatego element „Request URI” musi zawierać identyfikator publiczny (IMPU) użytkownika „Bolek”, a element „SIP Method” musi przyjąć wartość „Invite”.

Podczas rejestracji użytkownika w systemie IMS, zestaw kryteriów iFC (będący elementem profilu usługi powiązanego z użytkownikiem) ładowany jest z bazy HSS do węzła S-CSCF obsługującego danego użytkownika. W przypadku usługi CFU działającej na rzecz użytkownika „Bolek”, kryteria iFC z nią związane zostaną załadowane do tego węzła S-CSCF, który obsługuje użytkownika „Bolek”. Z tego powodu element „Session Case” ma ustaloną wartość „Term – Req”, czyli działa dla połączeń przychodzących, w domyśle do użytkownika „Bolek” (rysunek 15).

5.2. Konfiguracja serwera TAS

Konfiguracja Kamailio jako serwera TAS z usługą CFU wymaga stworzenia w lokalnej bazie danych w tabeli „usr_preferences” wpisu, który obędzie określać specyficzne zasady obsługi połączenia kierowanego do wskazanego użytkownika, którym w tym przypadku jest abonent „Bolek”. W tym celu należy wykonać poniższą komendę SQL INSERT, która doda do lokalnej bazy danych zrealizowanej w oparciu o system mysql, informację o zamianie adresów URI.

```
insert into usr_preferences VALUES (1,'','Bolek','open-ims.test','callfwd','0','sip:celina@open-ims.test','')
```

Wprowadzony wiersz definiuje dla użytkownika o nazwie „Bolek” nowy atrybut o nazwie „callfwd” i przypisuje mu wartość „sip:celina@open-ims.test”. Następnie w pliku `kamailio.cfg`, w którym zapisana jest cała logika routingu wiadomości sygnalizacyjnych SIP, w części odnoszącej się do akcji podejmowanych po odebraniu wiadomości SIP „Invite”, należy dodać fragment kodu sprawdzający czy dla użytkownika określonego przez nazwę w adresie „Request URI” wiadomości SIP „Invite” zdefiniowane zostały akcje zmiany zasad kierowania i ewentualnie wykonać je.

W naszym przypadku weryfikacja polega na sprawdzeniu czy w bazie „usr_preferences” dla użytkownika określonego przez nazwę w adresie „Request-URI” istnieje atrybut „callfwd”. To sprawdzenie zaimplementowane jest w następującej linii pliku `kamailio.cfg`:

```
if (avp_db_load("$ruri/username", "s:callfwd")) {
```

Jeżeli weryfikacja przebiegnie pozytywnie, wówczas należy zmienić zasady kierowania wiadomości SIP „Invite” według reguł określonych w odnalezionym wpisie tabeli „usr_preferences”. Oznacza to, że do adresu Request-URI otrzymanej wiadomości SIP „Invite” należy wstawić wartość przechowywaną w atrybucie „callfwd” odnalezionego wpisu. To zadanie realizuje następująca linia kodu z pliku `kamailio.cfg`:

```
avp_pushsto("$ruri", "s:callfwd");
```

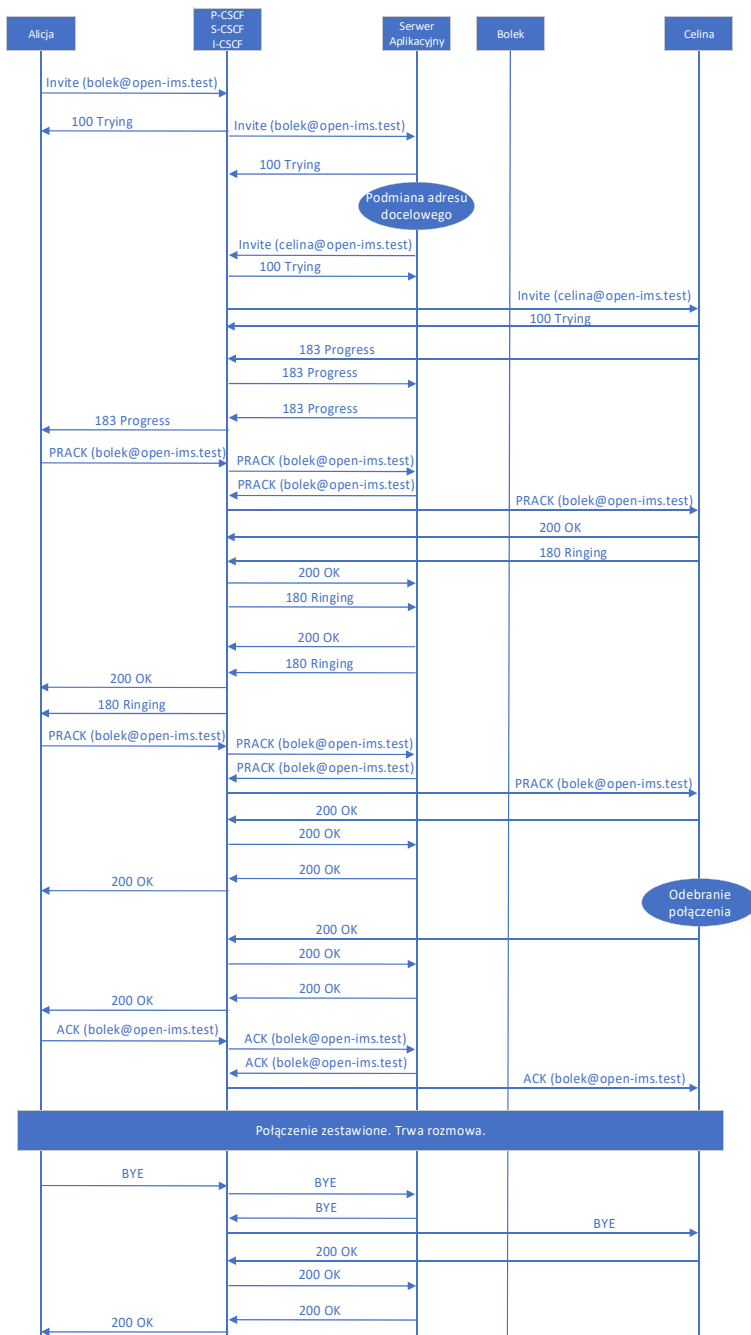
Przy konfiguracji określonej powyżej, odebranie w serwerze TAS wiadomości SIP „Invite” z nazwą „Bolek” w adresie „Request-URI”, spowoduje sprawdzenie i odnalezienie atrybutu „callfwd” oraz przepisanie do adresu „Request-URI” wartości „sip:celina@open-ims.test”. Natomiast odebranie wiadomości SIP „Invite” z jakkolwiek inną nazwą w adresie „Request-URI” nie spowoduje żadnych zmian. W efekcie tylko wiadomości SIP „Invite” kierowane do użytkownika „Bolek” będą przekierowywane na adres sip: celina@open-ims.test.

W opisany powyżej sposób, bardzo elastycznie można zmieniać zasady kierowania wiadomości SIP poprzez dodawanie odpowiednich wpisów w tabeli „usr_preferences”. Dzięki temu na platformie Kamailio 3.0 można zrealizować inne usługi dodatkowe telefonii np. przekierowanie w przypadku zajętości abo- nenta wywoływanego (*Call Forward on Busy*) lub w przypadku braku odpowie- dzi (*Call Forward No Answer*).

Na rysunku 16 przedstawiono wymianę wiadomości sygnalizacyjnych podczas zestawiania połączenia i wywołania usługi CFU. Ilustracja przedstawia wymianę wiadomości SIP faktycznie przesyłanych w sieci i zebranych za pomocą analizatora sieciowego Wireshark [34] na maszynie wirtualnej, na której zainstalowano plat- formę OpenIMSCore.

Z punktu widzenia obserwowanej wymiany wiadomości SIP jest to optymalny punkt przechwytywania ruchu SIP, ponieważ pozwala zaobserwować całą wymianę w jednym punkcie, tj. ruch od i do terminali, ruch od i do platformy OpenIMSCore oraz ruch od i do serwera aplikacyjnego Kamailio.

Należy podkreślić, że z powodu instalacji całej platformy OpenIMSCore na jed- nej maszynie wirtualnej, węzły P-CSCF, S-CSCF oraz I-CSCF związane są z tym samym interfejsem sieciowym i adresem IP różniąc się jedynie numerami portów UDP. Z tego powodu na rysunku 16 węzły P-CSCF, S-CSCF oraz I-CSCF reprezen- towane są jako jeden element, a wiadomości SIP wymieniane między nimi nie zo- stały przedstawione.



Rysunek 16. Wymiana wiadomości sygnalizacyjnych podczas wykonywania usługi CFU

6. Podsumowanie

W opracowaniu przedstawiono genezę oraz koncepcję systemu IP Multimedia Subsystem. W skróty sposób opisano jego architekturę oraz zasady działania. Na wykresach MSC (*Message Sequence Chart*) zilustrowano wymianę informacji w podstawowych scenariuszach sygnalizacyjnych, tj. podczas rejestracji użytkownika w systemie (rysunek 2), w czasie zestawiania połączenia pomiędzy dwoma abonentami sieci IMS (rysunek 3), a także podczas zestawiania połączenia z sieci IMS do PSTN (rysunek 4) oraz z sieci PSTN do IMS (rysunek 5). Analiza przedstawionych scenariuszy wymiany sygnalizacji miała na celu osiągnięcie efektu lepszego zrozumienia zasad działania systemu IMS oraz roli poszczególnych elementów z płaszczyzny sterowania. W rozdziale 4 omówiono sposób realizacji usług w systemie IMS, wyjaśniając rolę takich elementów konfiguracji jak: profil użytkownika, profil usługi, identyfikatory publiczny (*IMPU*) i prywatny (*IMPI*), kryteria filtrowania iFC, punkty wyzwalania (*Trigger Points*) oraz punkty wyzwalania usługi (*Service Point Triggers*). Opisano również rolę i tryby pracy serwerów aplikacyjnych. W rozdziale 5 przedstawiono proces kreacji i konfiguracji usługi bezwarunkowego przekierowania połączenia telefonicznego (*CFU*) na bazie oprogramowania OpenIMSCore oraz Kamailio. Przykład miał na celu skonkretyzowanie koncepcji przybliżanych w rozdziałach 1-4 oraz zapoznanie czytelników z konfiguracją platformy OpenIMSCore oraz wykorzystaniem oprogramowania Kamailio jako serwera telefonii (*Telephony Application Server; TAS*). Szczegółowo opisane kolejne kroki konfiguracji środowiska OpenIMSCore oraz implementacji usługi CFU pozwalają czytelnikom na samodzielne powtórzenie procesu wdrożenia usługi i w ten sposób nabycie umiejętności praktycznych związanych z obsługą wdrażania usług w systemie IMS.

Literatura

- [1] ITU-T Recommendation I.120, „Integrated Services Digital Networks (ISDNs)”, March 1993.
- [2] ITU-T Recommendation I.412, „ISDN user-network interfaces – Interface structures and access capabilities”, November 1988.

- [3] ITU-T Recommendation I.113, „Vocabulary of terms for broadband aspects of ISDN”, June 1997.
- [4] ATM-Forum, Technical Committee, “Traffic Management Specification, Version 4.0” – April 1996.
- [5] <http://www.3gpp.org>
- [6] 3GPP TR 21.101, „Technical Specifications and Technical Reports for a UTRAN-based 3GPP system”.
- [7] Spec 3GPP TS 24.302 version 11.7.0 Release 11
- [8] <http://www.openimscore.org>
- [9] 3GPP TS 22.228, “Service Requirements for the Internet Protocol (IP) Multimedia Core Network Subsystem; Stage 1”.
- [10] G. Camarillo, M.A. García-Martín, *The 3G IP multimedia subsystem (IMS): merging the Internet and the cellular worlds*, 3rd ed. Chichester, West Sussex: Wiley, 2008.
- [11] ITU-T Recommendation Q.1208 „General aspects of the Intelligent Network Application protocol”.
- [12] ITU-T Recommendation Q.1201 „Principles of IN Architecture”.
- [13] ITU-T Recommendation Q.1202 „IN Service Plane Architecture”.
- [14] ITU-T Recommendation Q.1203 „IN Global Functional Plane”.
- [15] Rosenberg, J., et al., “SIP: Session Initiation Protocol” IETF RFC-3261, June 2002.
- [16] ETSI, ETS 300 374-1, „IN CS-1; Core Intelligent Network Application Protocol (INAP); Part 1 - protocol specification”, September 1994.
- [17] ETSI, TS 101 046 V5.5.0, „Digital cellular telecommunications system (Phase 2+); Customized Applications for Mobile network Enhanced Logic (CAMEL); CAMEL Application Part (CAP) specification”, July 1998.
- [18] 3GPP TS 23.002: „Network Architecture”.
- [19] 3GPP TS 23.228, „IP Multimedia Subsystem (IMS); Stage 2”.
- [20] Fajardo V. et al., “Diameter Base Protocol”, IETF RFC 6733, October, 2012.
- [21] ITU-T Recommendation H.248.1, March 2013.
- [22] ITU-T Recommendation Q.700, „Introduction to CCITT Signalling System No. 7”, March 1993.

- [23] ITU-T Recommendation Q. 701, „Functional description of the message transfer part (MTP) of Signalling System No. 7”, June 1993.
- [24] Stewart R., „Stream Control Transmission Protocol”, IETF RFC 4960, September 2007.
- [25] 3GPP TS 09.02, „Mobile Application Part (MAP) Specification”.
- [26] ITU-T Recommendation Q.1901, „Bearer independent call control protocol”, June 2000.
- [27] ITU-T Recommendation Q.761, „Signalling system No. 7 – ISDN user part functional description”, December 1999.
- [28] 3GPP, „Customized Applications for Mobile network Enhanced Logic (CAMEL); Service definition (Stage 1)”, 3rd Generation Partnership Project (3GPP), TS 02.78, June 1996.
- [29] 3GPP TS 29.198-1: „Open Service Access (OSA); Application Programming Interface (API); Part 1: Overview”.
- [30] 3GPP TS 29.228: „IP Multimedia (IM) Subsystem Cx and Dx interfaces; Signalling flows and message contents ”.
- [31] Jennings C. et al., „Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks”, IETF RFC-3325, November 2002.
- [32] 3GPP TS 24.229: „IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3”.
- [33] <http://www.kamailio.org>
- [34] <http://www.wireshark.org>
- [35] 3GPP TS 24.228, „Signalling flows for the IP multimedia call control based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3”.

Architecture and principle of IP Multimedia Subsystem

Abstract

This paper describes the main idea of IP Multimedia Subsystem, the overview of its architecture, operating principles, basic signalling scenarios and the service provisioning process. The explained concepts are accompanied by an example configuration of the so called „call forward unconditional” supplementary voice service deployed on OpenIMSCore platform with support of Kamailio software serving as an application server.

Keywords – IP Multimedia Subsystem, OpenIMSCore, SIP, Kamailio