Filip Majerowski
Bartłomiej Kowalczyk
Wojciech Wojciechowicz**
Henryk Gierszal*
* Uniwersytet im. Adama Mickiewicza, ul. Umultowska 85, 61-614 Poznań
** Instytut Informatyki, Politechnika Poznańska, ul. Piotrowo 2, 60-965 Poznań
ITTI, ul. Rubież 46, 61-612 Poznań
Filip.Majerowski@itti.com.pl

Wrocław, 10-12 czerwca 2013

# WYKORZYSTANIE PLATFORMY IMS DO INTEGRACJI USŁUG W BRAMIE INTEROPERACYJNEJ

Streszczenie: **W publikacji zaprezentowano podejście do budowy bramy interoperacyjnej dla zapewnienia współpracy między systemami łączności wykorzystywanymi przez np. służby bezpieczeństwa, porządku publicznego oraz ratownictwa, które oparto na platformie IMS jako warstwie sterującej odpowiedzialnej za obsługę połączeń i ewentualną translację protokołów i przesyłanej treści. Wdrożony przykład zapewnia dwukierunkową komunikację między terminalem GSM, terminalem VoIP oraz POTS.**

## 1. WSTĘP

Interoperacyjność, czyli zdolność systemów telekomunikacyjnych do efektywnej wymiany informacji, jest bardzo ważnym czynnikiem zapewnienia łączności w sytuacjach kryzysowych [1]. Znaczna część materiałów faktograficznych dotyczących przebiegu sytuacji kryzysowych wskazuje problemy z interoperacyjnością jako istotnie utrudniające prowadzenie akcji ratowniczej. Jest to także model budowy radiowych sieci rozległych przyjęty w USA po zamachach w dniu 11 września 2001 r. W dziedzinie interoperacyjności istnieje silny nacisk na rozwiązania bazujące na protokole IP. Praktycznie wszystkie duże firmy działające w branży telekomunikacyjnej tj. Ericsson, Nokia Siemens Networks, Motorola czy Alcatel-Lucent, produkują urządzenia umożliwiające integrację systemów komórkowych z sieciami IP (ang. *Internet Protocol*). Niektóre oferują także osprzęt do innych systemów jak np. WIMAX (ang. *Worldwide Interoperability for Microwave Access*). Część dostawców sprzętu telekomunikacyjnego na te potrzeby oferuje bramy medialne MGW (ang. *Media GateWay*). Wprowadzenie węzłów komutacyjnych typu *softswitch* ułatwia wówczas transformację jednej technologii transmisyjnej (z komutacją łączy) na drugą (z komutacją pakietów) zapewniając sterowanie m.in. węzłami MGW oraz innymi rozproszonymi elementami sieci obejmującej niehomogeniczne systemy telekomunikacyjne oferujące różne, nawet niekompatybilne usługi bazujące na różnych technikach transmisyjnych.

Celem projektu HIT-GATE (ang. *Heterogeneous Interoperable Transportable GATEway for First-Responders*) realizowanego w ramach 7. Programu ramowego (program FP7-SECURITY, nr 284940) jest opracowanie technicznego rozwiązania umożliwiającego techniczną interoperacyjność w komunikacji między sieciami służb bezpieczeństwa i porządku publicznego PPDR (ang. *Public Protection and Disaster Relief*), wliczając w to także scenariusze angażujące działania transgraniczne [2]. Zostanie to osiągnięte poprzez opracowanie rozwiązania technicznego, które zapewni połączenie wszystkich istniejących systemów komunikacji za pośrednictwem dedykowanego węzła pełniącego rolę bramy, oraz które zapewni interoperacyjność wszystkich systemów wymaganych podczas akcji bez modyfikacji terminali ani głównej infrastruktury komunikacyjnej.

## 2. INTEROPERACYJNOŚĆ

Według Europejskich Ram Interoperacyjności [3] (w kontekście świadczenia europejskich usług użyteczności publicznej) interoperacyjność oznacza możliwość współdziałania różnych odrębnych organizacji na rzecz osiągnięcia uzgodnionych i korzystnych dla wszystkich stron celów, przy jednoczesnym dzieleniu się informacjami i wiedzą pomiędzy tymi organizacjami poprzez wspierane przez nie procesy biznesowe, za pomocą wymiany danych za pośrednictwem odpowiednich systemów. Z kolei zgodnie z ustawą Prawo telekomunikacyjne [4], interoperacyjność sieci to zdolność sieci telekomunikacyjnych do efektywnej współpracy w celu zapewnienia wzajemnego dostępu użytkowników do usług świadczonych w tych sieciach.

Duża różnorodność heterogenicznych systemów i urządzeń nabytych i wykorzystywanych przez służby bezpieczeństwa i porządku publicznego przynależnych do europejskich organizacji bezpieczeństwa publicznego, manifestuje się wieloma zagadnieniami dotyczącymi interoperacyjności na jej najbardziej podstawowym poziomie, czyli na poziomie komunikacji między systemami. W ramach projektu HIT-GATE proponuje się rozwiązanie problemu interoperacyjności w krótkiej perspektywie czasowej, tzn. opracowanie bramy, która będzie łączyć różne sieci i która zawiera wszystkie niezbędne protokoły translacji i usługi umożliwiające komunikację między interweniującymi ekipami.

Rozwiązaniami umożliwiającymi integrację systemów bezprzewodowych jest brama MOTOBRIDGE firmy Motorola, rozwiązanie VIDA (ang. *Voice Interworking Data Access*) oferowane przez firmę M/A COM czy urządzenie TETRANode firmy Rohill. W kraju takie rozwiązania oferuje już m.in. firma DGT — Zintegrowany System Łączności DGT-MCS (ang. *Multifunctional Communication System*), a także firma Mindmade. Prace nad tego typu węzłami prowadzone są w ramach licznych projektów 7. Programu ramowego, np. SECRICOM [1], FREESIC czy HELP, a także w ramach innych programów badawczo-wdrożeniowych, m.in. Celtic-Plus, np. projekt HNPS.

## 3. PROJEKT HIT-GATE

Głównym celem projektu HIT-GATE (www.hit-gate.eu) jest opracowanie uniwersalnej bramy, która umożliwi komunikację w sieciach obecnie wykorzystywanych przez służby bezpieczeństwa i porządku publicznego w Europie. Wiadomo powszechnie, że obecne sieci łączności służb bezpieczeństwa i porządku publicznego w całej Europie wykorzystują wiele różnych i niekompatybilnych technologii/standardów co uniemożliwia sprawną koordynację wspólnych działań (transgranicznych lub lokalnych w zakresie zarządzania kryzysowego kiedy podczas akcji muszą współdziałać różne służby). Wiadomo także, że europejskie

organizacje zajmujące się bezpieczeństwem publicznym zainwestowały w dedykowane systemy telekomunikacyjne będące infrastrukturą krytyczną (w celu zapewnienia wysokiej dostępności i niezawodności). Obejmuje to wyspecjalizowane sieci takie jak PMR (ang. *Professional Mobile Radio*), czyli np. standard TETRA (ang. *TErrestrial Trunked RAdio*) lub TETRAPOL. Ponadto, wraz z szybkim rozwojem technologii komunikacyjnych, liderzy wśród służb bezpieczeństwa i porządku publicznego zaadaptowali i wdrożyli wiele nowych cech funkcjonalnych systemów łączności, czyli m.in. szerokopasmowe sieci kratowe *ad hoc* zdolne zagwarantować lub poszerzyć zasięg radiowy na niesprzyjających obszarach (np. pod ziemią lub na zniszczonych terenach) oraz zapewnić dużą przepustowość (większą niż 5 Mbit/s).

Aby odpowiedzieć na potrzeby służb bezpieczeństwa i porządku publicznego, w ramach projektu HIT-GATE zostanie opracowane rozwiązanie obsługujące różne technologie/standardy wykorzystywane dziś przez organizacje związane z bezpieczeństwem publicznym oraz ratownictwem, które będzie obsługiwać zarówno klasyczne systemy PMR (głównie analogowe), sieci standardu TETRA/TETRAPOL, jak i sieci nowej generacji. Dzięki temu organizacje bezpieczeństwa publicznego i ratownictwa mogą zachować swoje dotychczasowe systemy i zaadaptować nowe technologie, ponieważ proponowane rozwiązanie HIT-GATE zapewni komunikacyjną interoperacyjność między tymi sieciami (ograniczoną oczywiście do możliwości funkcjonalnych danego interfejsu radiowego i przenoszonych usług każdej sieci). Brama HIT-GATE umożliwi zatem komunikację pomiędzy heterogenicznymi sieciami i służbami bezpieczeństwa i porządku publicznego podczas różnego rodzaju operacji (oczywiście w powiązaniu z odpowiednimi procedurami). Po podłączeniu rozwiązania HIT-GATE do swoich sieci, służby bezpieczeństwa i porządku publicznego mogą nadal użytkować swoje obecne terminale, stacje bazowe i infrastrukturę, a jednocześnie komunikować się między sobą.

Zarówno na poziomie europejskim, jak i krajowym organizacje bezpieczeństwa publicznego i służby ratownicze wdrożyły do eksploatacji szereg systemów, urządzeń i technologii, co doprowadziło do wielości sieci, które nie współpracują ze sobą. Ponieważ obecne działania dotyczące bezpieczeństwa i ratownictwa często angażują wielonarodowe zespoły tych służb (np. akcje ratownicze wywołane klęskami żywiołowymi realizowane jako operacje transgraniczne), ważne jest zapewnienie skutecznego rozwiązania technicznego umożliwiającego komunikację rozmówną oraz wymianę danych między nimi.

## 4. BRAMA HIT-GATE

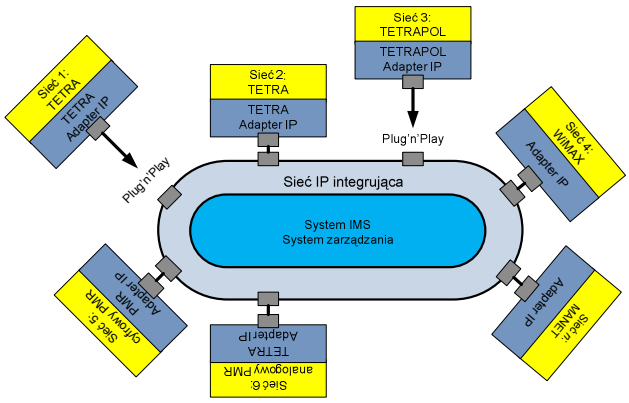
Brama HIT-GATE zapewni „przeźroczystą” dla użytkowników ciągłość realizacji usług oraz zintegruje dla służb bezpieczeństwa i ratownictwa heterogeniczne technologie komunikacji, z których każda zawiera określone zestawy protokołów, usług i cech. Jednocześnie rozwiązanie to podczas prowadzenia akcji umożliwi spełnienie typowych dla działań ratowniczych kluczowych wymagań, które dotyczą także sfery aplikacji przydatnych do komunikacji między służbami, a także takich parametrów jak: wysoka dostępność, niezawodność, bezpieczeństwo oraz łatwość do uruchomienia w wysoce dynamicznym i nieprzewidywalnym otoczeniu łączności ruchomej, co jest szczególnie przydatne w przypadku służb ratowniczych, bezpieczeństwa i porządku publicznego [1]. Ta ostatnia cecha wiąże się z faktem, że istniejące infrastruktury transmisyjne mogą mieć ograniczone możliwości (np. zdegradowaną pojemność czy przepływność w wyniku natłoku) lub być zniszczone na skutek wypadków czy innych przyczyn losowych.

Aby osiągnąć interoperacyjność techniczną dzięki bramie HIT-GATE zakłada się, że:

- brama HIT-GATE zapewni interoperacyjność techniczną między sieciami opartymi na standardowych protokołach, aby ułatwić wdrażanie i standaryzację. Będzie obsługiwać sieci różnych technologii (co najmniej TETRA, TETRAPOL, PMR, WiMAX oraz połączenia z komutacją łączy) oraz tej samej technologii (np. TETRA-TETRA);
- system HIT-GATE dostarczy rozwiązania do translacji protokółów i usług w sieciach poprzez wprowadzenie wspólnych protokołów i usług w zależności od stopnia kompatybilności każdej sieci. Oznacza to, że urządzenie HIT-GATE może umożliwić połączenia rozmówne w sieciach, ale nie zapewni cyfrowej transmisji danych między sieciami szerokopasmowymi oraz analogowymi sieciami PMR, ponieważ te ostatnie tego nie umożliwiają;
- brama HIT-GATE połączy sieci w trybie pełnego dupleksu i półdupleksu oraz będzie obsługiwać rozmowy grupowe w sieciach pozwalających na pracę w pełnym dupleksie: PLMN (ang. *Public Land Mobile Network*), PSTN (ang. *Public Switch Telephony Network*), ISDN (ang. *Integrated Service Digital Network*) itp.;
- interfejs radiowy każdej technologii nie zostanie zmieniony wliczając w to istniejące stacje bazowe i infrastruktury sieciowe. Oznacza to, że radiowe terminale ruchome i stacje bazowe działają w ten sam sposób bez lub z bramą HIT-GATE. Ten aspekt ogranicza zakres problemów technicznych wymagających rozwiązania, a także zapewnia zgodność z istniejącymi urządzeniami;
- urządzenie HIT-GATE umożliwi dynamiczne dołączanie się do sieci i będzie zawierać automatycznie adaptujące się mechanizmy zapewniające nieprzerwany dostęp do sieci. Właściwości te określa się jako „podłącz i używaj” ("*Plug'n'Play*") oraz „dołącz w trakcie” ("*on-the-fly*"). Drogą do osiągnięcia tych właściwości jest protokół IP używany z uwagi na łatwość konfiguracji, powszechność rozwiązań oraz udowodnioną zdolność łączenia wielu heterogenicznych urządzeń;
- brama HIT-GATE to nie tylko rozwiązanie sprzętowe — jest to bowiem system zapewniający interoperacyjność, który wykorzystuje zarówno sprzęt, jak i oprogramowanie. Urządzenie HIT-GATE zawiera adaptery, które łączą każdą przyłączaną sieć łączności do integrującej sieci IP. Adapter tłumaczy specyficzny protokół każdej technologii na protokół IP pozwalając na szybkie zestawienia połączenia i bardziej elastyczny sposób łączenia wielu sieci. Ponadto, rozproszone bramy HIT-GATE mogą być połączone ze sobą, w wyniku czego powstaje sieć urządzeń HIT-GATE łączących wszystkie takie rozproszone podsieci we wspólną sieć komunikacji między różnymi służbami zaangażowanymi w wielu miejscach. Takie podejście zapewnia również środki do realizacji łączności internetowej, a zatem globalnego dostępu do centralnych centrów operacyjnych w odległych lokalizacjach.

Innowacyjność bramy interoperacyjnej polega na wykorzystaniu platformy IP: SIP (ang. *Session Initiation Protocol*) i IMS (ang. *IP Multimedia Sub-System*), a także innych rozwiązań otwartych jak standard ODINI (ang. *On-Demand*

*Intelligent Network Interface*) do integracji sieci łączności trankingowej/dyspozytorskiej analogowych i cyfrowych, jak i sieci transmisji danych. Pozwoli to szybko zapewnić usługi łączności użytkownikom uczestniczącym w sytuacjach kryzysowych w dowolnym miejscu, także dzięki łatwym możliwościom transportowania i zasilania bramy HIT-GATE. Brama ta będzie ponadto cechowała się parametrami typowymi dla sprzętu przeznaczonego do obsługi operacji krytycznych. Poniższa ilustracja (rys. 1) prezentuje koncepcje HIT-GATE.




*Rys. 1 Koncepcja HIT-GATE*

## 5. ŚRODOWISKO IMS

W ramach prac wdrożeniowych realizowanych w projekcie HIT-GATE stworzono w laboratorium ITTI platformę IMS, w ramach której uruchomiono także serwer aplikacji. Wybrano rozwiązanie platformy IMS — The Open IMS Core grupy Fraunhofer FOKUS (www.openimscore.org) oraz serwer aplikacji — Mobicents (www.mobicents.org).

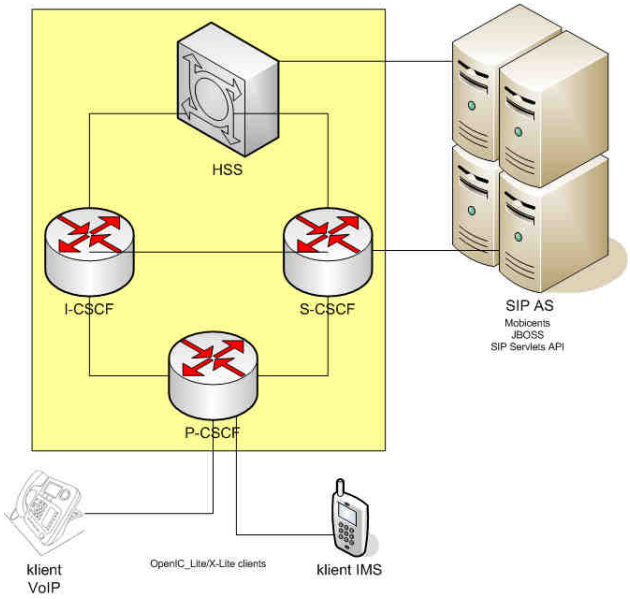
Do instalacji platformy The Open IMS Core użyto gotowego obrazu systemu operacyjnego Ubuntu dostępnego pod adresem www.openimscore.org/vm, który został uruchomiony w programie VMWare Player. Oprogramowanie zostało skonfigurowane zgodnie z własnymi potrzebami, m.in. z publiczną adresacją IP powiązaną z własną domeną RIPE. Do obsługi klientów IMS posłużono się telefonami programowymi *softphone*: OpenIC_lite w systemie Ubuntu i X-Lite zgodnym z protokołem SIP w systemach Windows / Mac OS X. Następnie dla środowiska IMS uruchomiono serwer aplikacji. Wybrano wersję serwera aplikacji Mobicents, która korzysta z serwera JBoss i która obsługuje technologię SIP Servlets. W przygotowanej konfiguracji był to serwer JBoss 5.0.1.GA ze środowiskiem Mobicents SIP Servlets (MSS) 1.5.0.FINAL.

SIP Servlets to jedno z rozwiązań stosowanych przy tworzeniu aplikacji dla platformy IMS. Jakkolwiek inne technologie, takie jak Java APIs for Integrated Networks (JAIN) Service Logic Execution Environment (SLEG) czy Parlay X, oferują znacznie szersze możliwości (ale są przez to bardziej skomplikowane), środowisko SIP Servlets jest cenione za prostotę i strukturę zorientowaną na obsługę protokołu SIP. Jest to interfejs API języka JAVA składający się z obiektów oraz funkcji, które odpowiadają przesyłanym wiadomościom SIP takim jak: zaproszenie INVITE, rejestracja REGISTER, anulowanie CANCEL itp. Aby obsłużyć taką wiadomość, programista musi jedynie nadpisać odpowiednią funkcję. Dla przykładu, wiadomości INVITE odpowiada funkcja `doInvite()`.

Przetestowano aplikację zamieszczoną na stronie projektu Mobicents (www.mobicents.org/mss-diameter_sh.html), co wymagało modyfikacji adresacji IP w kodzie oprogramowania dostosowującą ją do adresów wykorzystywanych w sieci LAN. Dla odpowiednio skonfigurowanych użytkowników — *Alice* (ID: sip:alice@<domena>.pl) i *Bob* (ID: sip:bob@<domena>.pl) — przeprowadzono szereg testów mających pozwolić ocenić poprawność konfiguracji i działania utworzonej sieci IMS. Następnie rozbudowano opracowany system w celu umożliwienia tworzenia własnych usług/aplikacji, wykorzystując do tego celu środowisko Eclipse Integrated Development Environment (IDE) (Eclipse 3.4 dla Java Enterprise Edition (JEE) oraz wtyczkę *plugin* Maven (do kompilacji plików `.war` obsługiwanych przez serwer JBoss). Stworzono kilka przykładowych aplikacji obsługujących podstawowe wiadomości SIP weryfikując ich poprawność w środowisku Open IMS Core na serwerze JBoss Mobicents korzystając z użytkowników *Alice* i *Bob* (np. konwersja formatu treści przesyłanych między obu użytkownikami).

Na rys. 2 pokazano architekturę stworzonego środowiska IMS [5]. Mamy tu trzy moduły z funkcjami sterowania sesją połączenia CSCF (ang. *Session Control Function*). Komponent P-CSCF (ang. *Proxy CSCF*) jest serwerem *proxy*, który jest pierwszym punktem przyjęcia przesyłanych komunikatów pełniąc także rolę zapory sieciowej *firewall* na poziomie aplikacji (tylko zarejestrowane węzły użytkowników mogą wprowadzić wiadomość do sieci IMS, a ponadto ten element potwierdza tożsamość użytkownika). Serwer ten zestawia bezpieczne kanały indywidualnie dla każdego węzła użytkownika UE (ang. *User Endpoint*), który obsługuje. Aby nadzorować zarejestrowanych użytkowników, zawiera on wewnętrzny układ rejestrowania, który jest uaktualniany poprzez przechwytywanie procesu rejestracji, a później poprzez zapisanie się do modułu rejestracyjnego w węźle S-CSCF i otrzymywanie powiadomień. W ramach sygnalizacji związanej z inicjowanym połączeniem, węzeł ten generuje unikatowe wektory taryfikacyjne oraz wprowadza identyfikatory sieci i ścieżki, które są potrzebne dla dalszego poprawnego przetwarzania wiadomości SIP. Po poprawnie zrealizowanym procesie rejestracji do sieci IMS, kolejne wiadomości użytkownika są kierowane opierając się na informacjach systemu DNS (ang. *Domain Name System*) do żądanej sieci IMS. Odnośnie zagadnień translacji adresów NAT (ang. *Network Address Translation*) dla sygnalizacji SIP przekazywanej w kierunku węzła użytkownika, komponent P-CSCF może działać jako router. Element S-CSCF (ang. *Serving CSCF*) jest centralnym węzłem odpowiedzialnym za obsługę sygnalizacji. Jest to serwer SIP, lecz realizuje on także sterowanie sesją. Może on wykorzystać dane z pobranego profilu użytkownika, aby zastosować specyficzne zasady routingu w ramach protokołu SIP. Węzeł I-CSCF (ang. *Interrogating CSCF*) jest kolejnym komponentem obsługi protokołu SIP odpowiedzialnym za obsługę zgłoszeń. Jego adres IP jest publikowany w systemie DNS danej domeny, co pozwala innym serwerom odnaleźć ten węzeł i wykorzystać go jako punkt przekierowania pakietów SIP (np. na potrzeby rejestracji wywołań). Ponadto w środowisku IMS występuje serwer HSS (ang. *Home Subscriber Server*), który jest główną bazą danych o użytkownikach odpowiedzialną za wsparcie sieci IMS obsługującej połączenia. Serwer ten zawiera informacje odnoszące się do abonamentów (tzn. profil abonenta), realizuje uwierzytelniania i autoryzację użytkowników oraz może

dostarczyć informację o położeniu abonenta oraz dane IP skojarzone z połączeniem. Serwer I-CSCF wykorzystując publiczne identyfikatory strony dzwoniącej lub wywoływanej, odpytuje serwer HSS i bazując na uzyskanej odpowiedzi kieruje wiadomość do właściwego węzła S-CSCF. Serwer S-CSCF komunikuje się z serwerem HSS, aby odtworzyć dane uwierzytelniające, uaktualnić informacje rejestracyjne oraz pobrać profil użytkownika. Serwer aplikacji AS (ang. *Application Server*) obsługuje usługi oraz zapewnia komunikację z węzłem S-CSCF poprzez protokół SIP.



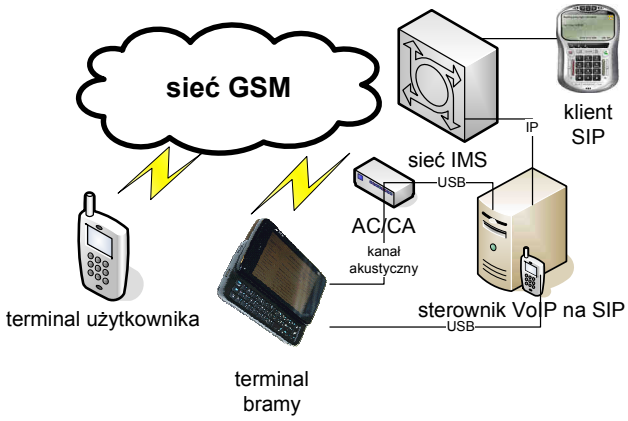

*Rys. 2 Integracja platformy Open IMS Core z serwerem Mobicents*

Poszczególne serwery sieci IMS uruchomiono jako maszyny wirtualne na jednym komputerze gospodarzu (*host*). Wymiana komunikatów między komponentami odbywa się w ramach wirtualnej sieci LAN skonfigurowanej w ramach środowiska wirtualizacji.

Na rys. 3 pokazano schemat systemu IMS, który rozbudowano o możliwość współpracy z siecią GSM (ang. *Global System for Mobile communication*) w zakresie komunikacji rozmównej oraz przesyłania wiadomości SMS (ang. *Short Messaging Service*). Jako terminal bramy zastosowano urządzenie Nokia N900 z system operacyjnym Maemo 5 (Linux). Transmisja kanału akustycznego z/do terminala jest realizowana analogowo, a następnie sygnał jest przetwarzany cyfrowo w przetworniku analogowo-cyfrowym i przesyłany przez port USB (ang. *Universal Serial Bus*) do sterownika VoIP (ang. *Voice over IP*) opartego na systemie Ubuntu pełniącego rolę klienta SIP. Sterowanie terminalem realizowane jest z wykorzystywaniem drugiego portu USB.

W tak skonfigurowanym środowisku testowym można zestawiać połączenia rozmówne między terminalem użytkownika i klientem SIP, a także przesyłać wiadomości SMS z terminala, które wyświetlane są na komunikatorze klienta SIP, a także w drugim kierunku. Całą automatyzacją procesów w sterowniki VoIP realizuje oprogramowanie `Node.js`.

Pojemność samej platformy IMS jest limitowana jedynie możliwościami np. adresacji węzłów, co *de facto* nie stanowi dużego ograniczenia. Z kolei możliwości ruchowe takiego podejścia są ograniczone pojemnością rozwiązań obsługujących interfejs radiowy. W tym przypadku jeden terminal GSM zapewni łączność grupie użytkowników liczącej typowo co najwyżej 8 użytkowników (ograniczenie przy tworzeniu połączeń wielostronnych). W przypadku sieci standardu TETRA, terminal dołączony do takiej platformy i pracujący w trybie DMO może obsłużyć do czterech kanałów rozmównych i zależnie od producenta sprzętu naraz jedynie kilka zdefiniowanych grup użytkowników.




*Rys. 3 Schemat systemu IMS współpracującego z terminalem GSM*

## 6. PODSUMOWANIE

Zbudowane środowisko IMS pozwoliło opracować prototyp bramy interoperacyjnej zapewniającej obsługę podstawowych usług komunikacyjnych świadczonych w sieci GSM. Wykorzystana platforma IMS okazała się łatwa w instalacji, uruchomieniu i konfiguracji. Wdrażanie nowych usług zapewniających integrację systemów łączności wymaga znajomości języka Java i specyfiki danego terminala w zakresie komend sterujących jego pracą. Przyjęty model funkcjonowania bramy nie zapewnia pożądanej niezawodności (brak redundancji). Ponadto cechuje go ograniczenie pojemnościowe związane z liczbą użytkowników obsługiwanych jednocześnie, co wynika z możliwości interfejsu radiowego (m.in. liczba szczelin czasowych), ograniczeń systemowych (liczba członków połączeń wielostronnych), możliwości terminali (liczba grup użytkowników), jak i konfiguracji usług komunikacyjnych definiowanej przez operatorów sieci.

Opracowana demonstracja miała posłużyć jedynie do oceny przydatności platformy IMS w tworzeniu bardziej rozbudowanych układów służących zapewnieniu technicznej interoperacyjności między różnymi systemami łączności. Jak zaznaczono na wstępie środowisko IMS jest wykorzystywane do tworzenia, konfiguracji i zarządzania usługami integrującymi komunikację między służbami bezpieczeństwa i porządku publicznego. Odrębna warstwa docelowej bramy interoperacyjnej zapewnia odpowiednią translację tych usług na usługi komunikacyjne oferowane przez poszczególne systemy łączności.

## SPIS LITERATURY


[1] W. Wojciechowicz *et al.* "Information and Communication Technology and Crisis Management", Technical Sciences No. 15(1)/2012, 2012

[2] *Description of Work*, HIT-GATE, no: 284940, 2011-10-20 [SEC-2011.5.2-1]

[3] *W kierunku interoperacyjności europejskich usług użyteczności publicznej*, KE, KOM(2010) 744

[4] Ustawa *Prawo telekomunikacyjne* z dnia 16.07.2004 r. (Dz.U.2004.171.1800)

[5] www.fokus.fraunhofer.de/en/fokus_testbeds/open_ims_playground