

**Zestawienie odpowiedzi  
na pytania Urzędu Komunikacji Elektronicznej zadane środowisku w ramach  
konsultacji „nomadyczność VoIP”.**

***Pytanie: 1.***

***Jakie ograniczenia występują przy nomadycznym korzystaniu z VoIP ? (Czy, a jeżeli tak to w jaki sposób z usług VoIP korzystają mogą użytkownicy, którzy znajdują się za NAT i/lub firewall'em?)***

***Odpowiedzi:***

**Alcatel.**

Możliwość realizacji usługi VoIP w trybie „nomadycznym” jest przedmiotem prac standaryzacyjnych w grupach 3GPP i TISPAN. Standardy te definiują sposób budowy sieci w taki sposób, by usługa VoIP mogła być dostępna w tym trybie z dowolnego miejsca. Kwestie ograniczeń sieci, poprzez którą abonent osiąga własną sieć można podzielić na dwie zasadnicze grupy:

- dostępność usługi

Istnieje szereg zagadnień związanych z możliwością realizacji usługi VoIP poprzez sieci inne niż sieć „domowa” abonenta. Są to głównie kwestie związane z adresacją i translacją adresu, przenoszeniem protokołów/sygnalizacji itp.

- zapewnienie jakości głosu

Zagadnienia związane z zapewnieniem jakości przenoszenie informacji (zapewnienia stabilnej transmisji z odpowiednią przepływnością).

Podsumowując realizacja usługi w trybie nomadycznym z odpowiednią jakością może zostać zapewniona wyłącznie w sytuacji, gdy zarówno sieć „domowa” jak i „wizytująca” są przygotowane pod względem technicznym. W przypadku standardowych sieci IP abonent ma duże szansę (które szacujemy na 95%), że usługa w trybie nomadycznym będzie dostępna, niemniej jednak mogą wystąpić problemy z jakością połączenia.

**Astercity.**

Teoretycznie Internet nie zna granic i w związku z tym w sieci Internet powinna występować pełna nomadyczność numeracji. Niemniej jednak występuje kilka rodzajów ograniczeń. Pierwszym z nich jest ograniczenie fizyczne: gateway IP, telefon IP lub komputer z zainstalowanym oprogramowaniem należy zabrać ze sobą w miejsce gdzie się chce korzystać z danej usługi przy wykorzystaniu swojego sprzętu. Oczywiście istnieje możliwość dostępu lokalnie do dowolnego komputera i zainstalowanie na nim aplikacji z podaniem danych swojego konta VoIP jak i wymaganej konfiguracji, ale niesie to za sobą ryzyko niepowołanego dostępu przez osoby trzecie na koszt użytkownika.

Drugim ograniczeniem jest przepustowość łącza. Rozmowa w technologii VoIP jak każda inna transmisja IP wymaga zapewnienie pewnej minimalnej przepustowości. Z tego powodu łącze z którego korzystamy musi spełniać pewne warunki techniczne pod kątem przepustowości.

Kolejnym, trzecim ograniczeniem jest „odległość” od miejsca w którym się znajdujemy do serwera usługodawcy VoIP. Tutaj mówimy o takich parametrach jak ilość przeskoków czy czas dotarcia informacji do serwera (ping). Im większa ilość przeskoków oraz im dłuższy

ping, tym większe ryzyko, iż wiele pakietów IP po drodze zostanie „zgubionych” (opóźnienie ich będzie tak duże, że serwer je zignoruje) a co za tym idzie jakość rozmowy będzie na tyle zła, iż nie da się swobodnie prowadzić konwersacji. Drugim objawem (nawet przy zachowaniu jakości dźwięku) będą duże opóźnienia w czasie pomiędzy nadawcą a odbiorcą informacji, co również wpływa negatywnie na możliwość prowadzenia swobodnej rozmowy. Przyjmuje, iż aby rozmowa była akceptowalnej jakości „zginąć” może maksymalnie 5 do 7% pakietów a opóźnienie nie może być większe niż 200 ms (milisekund – milisekunda = 1/1000 sekundy). Są to dane oparte na doświadczeniach użytkowników a nie na standardach.

Kwestia jakości połączenia oraz problemów w prowadzeniu konwersacji z opóźnieniami jest bardzo indywidualna i zależy od każdego użytkownika.

Dodatkowo parametry te i ich akceptowalny margines strat jest również zależny od zastosowanych kodeków. Istnieją rozwiązania „inteligentne”, które potrafią wygładzić przerwę spowodowaną utratą pakietu poprzez płynne przejście dźwięku między jednym a drugim pakietem. Zniekształca to nieco rozmowę, ale daje lepszy efekt niż szum lub cisza.

Tego typu prosty mechanizm powoduje zwiększenie akceptowalnych strat pakietów o kilka punktów procentowych (maksymalnie jednak 7%).

Istnieją inne proste mechanizmy minimalizujące efekt gubienia pakietów. Podstawowym jest założenie buforu o pojemności kilkanaście – kilkadziesiąt ms. Bufor taki powoduje, iż w przypadku utraty pakietu serwer może ponownie odpytać o jego przesłanie, a opóźnienie kilkadziesiąt ms w prowadzeniu rozmowy jest opóźnieniem akceptowalnym.

Jeśli chodzi o połączenie za firewall'em lub NATem, to istotnie w niektórych sytuacjach może być to problem nie do obejścia bez ingerencji administratora systemu.

W tej chwili są stosowane głównie dwa protokoły w transmisji VoIP: AIX oraz SIP. O ile AIX ze standardowym (podstawowym) NAT'em jest sobie w stanie poradzić o tyle SIP już nie jest na tyle elastyczny.

Jeśli chodzi o firewall, to transmisja VoIP aby była dwukierunkowa musi się odbywać poprzez otwarte porty. Standardowo pewne zakresy portów są na firewall'u otwarte w celu zapewnienia podstawowej funkcjonalności Internetu (choćby przeglądanie stron www czy obsługa e-maila). Jeśli jednak okaże się, że należy otworzyć inne zakresy portów na firewall'u lub przekonfigurować NAT nie ma możliwości uruchomienia usługi VoIP bez ingerencji administratora systemu.

## **Dialog.**

Jeżeli użytkownik korzystający z usług VoIP posiada pełen (nie translowany) dostęp do sieci Internet, na bazie publicznego adresu IP, wówczas bez przeszkód może realizować połączenia VoIP za pośrednictwem wybranego przez siebie operatora. Oczywiście w tym jak i każdym innym rozwiązaniu, wykorzystującym sieć Internet, mogą wystąpić problemy jakościowe, związane z opóźnieniami w transmisji danych lub utratami pakietów. Nie bez znaczenia dla jakości połączenia VoIP jest także fizyczna odległość między terminalami VoIP. Jednak rosnąca w ostatnich latach popularność szerokopasmowego dostępu do Internetu oraz dostępność kodeków głosowych z wysoką kompresją w aplikacjach i urządzeniach VoIP sprawia, że jakość rozmów VoIP realizowanych za pośrednictwem sieci Internet rośnie.

Na krótkotrwałe trudności mogą natrafić także użytkownicy dostępu do Internetu ze zmiennym adresem IP i krótkim czasem trwania sesji dostępowej. Jeżeli po zerwaniu i ponownym nawiązaniu sesji dostępowej (np. PPP - dla usług dialup, PPPoE/PPPoA - dla usług szerokopasmowych) nastąpi zmiana adresu IP, a terminal IP nie dokona w międzyczasie ponownego zarejestrowania się w serwerze SIP z nowymi ustawieniami, wówczas wszystkie połączenia przychodzącego abonenta VoIP, będą kierowane na adres IP z poprzedniej sesji, co uniemożliwi zasygnalizowanie połączenia przychodzącego.

Zdecydowanie więcej trudności sprawia korzystanie z usług VoIP użytkownikom znajdującym się za urządzeniami typu Firewall/NAT. W tym przypadku terminal VoIP posiada prywatny adres IP, z którym rejestruje się w serwerze SIP zlokalizowanym w sieci publicznej. Niedostępność adresu prywatnego z sieci publicznej oznacza brak dostępności usług VoIP. Usunięcie powyższego ograniczenia zapewnia:

- implementacja klienta protokołu STUN po stronie abonenckiej, w celu określenia adresu publicznego klienta, z którym dokonywana jest rejestracja terminala w serwerze SIP lub

- wsparcie dla NAT po stronie operatora (w serwerze SIP oraz bramkach VoIP-to-PSTN), dzięki czemu adres IP używany do rejestracji klienta w serwerze oraz adres dla strumienia głosowego są pobierane z nagłówka pakietu IP, a nie z wiadomości protokołu SIP pochodzące od abonenta.

### **Gabriel Grzesik.**

Nie ma żadnych ograniczeń o charakterze wspomnianym w pytaniu. Są ograniczenia w przypadku łącza transmitującego pakiety ze stałym dużym opóźnieniem lub transmitującego pakiety z dużym losowym opóźnieniem. Mam na myśli usługi dostępu do internetu przez GPRS, typu Blue Connect i iPlus, gdzie telefonia VOIP nie ma szans bez wsparcia ze strony operatora GSM.

### **GTS Energis.**

Główne ograniczenia w nomadycznym korzystaniu to:

FireWall – ogranicza dostępu do określonych portów IP/UDP wyłącza możliwość korzystania z usługi.

NAT – w szczególnych przypadkach może powodować ograniczenia dostępu do usługi. Użytkownicy znajdujący się na FireWalle mogą korzystać z usług telefonicznych opartych o VoIP po udostępnieniu odpowiednich portów IP/UDP.

### **Internet Group.**

Ograniczeniem rozwoju usługi VoIP jest bardziej stosunkowo małe rozpowszechnienie szerokopasmowego dostępu do sieci Internet wśród osób indywidualnych, niż problemy z połączeniami z za NAT czy firewall'a. Praktycznie każda z firm, świadczących tego typu usługi, poradziła sobie z obejściem problemu pracy swoich klientów na niepublicznych adresach IP. Zazwyczaj nie ma także problemu z odblokowaniem koniecznych portów w firewall'u dla poprawnej, dwustronnej komunikacji głosowej. W sporadycznych przypadkach, gdy administrator nie godzi się na odblokowaniem niczego ponad porty dedykowane dla WWW, faktycznie powstaje problem. Póki co radzi sobie z nim komunikator Skype, który jednak nie udostępnia swoich rozwiązań. Na rynku jest także dostępna technologia AnyFirewall (firmy Eyeball Networks), jednak wykorzystanie jej jest obłożone bardzo wysokimi kosztami, stawiającymi pod znakiem zapytania celowość jej stosowania.

### **Junisoftex.**

Nie notujemy problemów lub ograniczeń przy korzystaniu z naszych usług za NATem lub firewalem. Użytkownicy za NATem wykorzystują właściwości protokołu SIPv2 omijając problem translacji adresów. Natomiast użytkownicy z firewallem odblokowują odpowiednie porty.

### **KIGEiT**

*powinno być:*

- ENUM tak jak numeracja krajowa danego kraju powinien być administrowany przez UKE (a nie przez jednego z przedsiębiorców)
- możliwość bezproblemowego skomunikowania się z użytkownikami różnych platform/operatorów
- możliwość skorzystania z usługi VoIP wykorzystując dowolne łącze internetowe/dowolnego operatora
- każdy z operatorów powinien zapewniać jakość łącza internetowego umożliwiającego korzystanie z usług VoIP (np. brak dropowania/opóźniania pakietów)
- oferta operatorów powinna być ofertą bezpieczną, tzn. zabezpieczenie przed: niekontrolowanym obejściem systemów zabezpieczeń Klienta (np. skanowanie portu), zachowaniem typu obecnie znany dialer.

*obecnie:*

Nomadyczności usług stoją na przeszkodzie ograniczenia techniczne:

- brak kompatybilności pomiędzy rozwiązaniami różnych operatorów (brak interoperability)
  - różnorodność rozwiązań klienckich (sieć/LAN/PC/NAT/Firewall)

### **Dariusz Bakuła (pracownik Lucent).**

Podstawowe ograniczenia przy nomadycznym korzystaniu z usług VoIP wynikają z (a) trudności w jednoznacznej identyfikacji abonenta oraz z (b) zapewnienia niezawodnych połączeń na numery alarmowe, stosownie do aktualnej lokalizacji abonenta VoIP. Dodatkowo w punkcie (c) omówiono problematykę NAT/firewall.

(a) W ogólności nie istnieją mechanizmy pozwalające na jednoznaczną identyfikację nomadycznego abonenta VoIP (patrz też odpowiedź na dalsze pytania). I tak na przykład, identyfikatory URI (*Uniform Resource Identifiers*) zawierają pole FROM, zawierające adres własny abonenta, w szczególności adres SIP URI w postaci np. sip:<nazwa\_abonenta>@<domena\_abonenta>.com. Nie istnieją jak dotąd standardowe rozwiązania pozwalające jednoznacznie zweryfikować, czy dane adresowe wskazane w polu FROM rzeczywiście należą do danego, określonego użytkownika. Dane zawarte w polu FROM nie są typowo modyfikowane przez sieć i przesyłane są w sposób transparentny. Może to otwierać pole do nadużyć, powodować problemy z jednoznaczną identyfikacją połączeń złośliwych (tzw. *Malicious Call Trace*), czy innych problemów z niepożądanymi połączeniami, np. reklamowymi (tzw. SPIT - *Spam over Internet Telephony*). Problemy związane z niezawodną i jednoznaczną rejestracją i identyfikacją abonenta są dobrze rozpoznane i badane przez wiele organizacji standaryzacyjnych, zwłaszcza w odniesieniu do sieci IMS.

(b) Patrz odpowiedź na pytanie 6.

(c) Dla prawidłowego funkcjonowania VoIP w przypadku abonentów wykorzystujących funkcje NAT i/lub firewall wymagane jest, aby urządzenia NAT/Firewall „rozumiały” protokół sygnalizacyjny stosowany w telefonii IP. W tym celu stosuje się funkcję logiczną określaną mianem bramy ALG (*Application Layer Gateway*). I tak, w przypadku protokołu SIP, ALG pełni funkcję SIP B2BUA (*Back To Back User Agent*) i pozwala na przenoszenie sygnalizacji SIP poprzez firewall. Również NAT z wbudowaną funkcją ALG pozwala na taką modyfikację wiadomości sygnalizacyjnych, aby możliwe było zestawienie połączeń VoIP.

### **NASK**

Rozwiązania typu NAT i FW (sprzętowy bądź programowy) są przy obecnym stopniu zagrożeń w sieci stosowane na coraz większą skalę i nie można pomijać aspektu

funkcjonowania telefonii VoIP w takich sytuacjach. Rozwiązania techniczne w rodzaju STUN, NAT helper, itp. są w stanie rozwiązać problemy przy komunikacji z użyciem NAT/FW. Pracujące w ramach systemów telefonii IP serwery STUN na drodze dodatkowych zapytań sprawdzają sposób podłączenie terminala klienta do sieci IP, a następnie wykorzystują tę wiedzę przy zestawianiu połączeń głosowych.

### **Net Telecom**

Obecnie wykorzystywane przez użytkownika urządzenia końcowe takie jak adaptory, routery z funkcjonalnością VoIP czy też telefony VoIP zapewniają w zdecydowanej większości wypadków bezproblemowe korzystanie z usług VoIP.

### **Onet**

Główne ograniczenia w nomadycznym korzystaniu to:

FireWall – ogranicza dostępu do określonych portów IP/UDP wyłącza możliwość korzystania z usługi.

NAT – w szczególnych przypadkach może powodować ograniczenia dostępu do usługi.

### **Inotel**

W przypadku INOTEL SA nie ma problemów z NAT, do poprawnego działania usługi wymagane jest otwarcie na firewallu portów UDP 5060-5061 (SIP) i portów do strumienia RTP najczęściej 8000-8005 i 16000-17000.

### **TPSA**

Abonenci indywidualni usługi VoIP w sieci TP, aby korzystać z usługi wykorzystują urządzenie Livebox. Urządzenie to pełni funkcję routera i modemu DSL, które jest odpowiednio skonfigurowane do obsługi usługi na łączach neostrada tp. W tym przypadku nie ma problemu korzystania z usługi.

Natomiast jeśli weźmiemy pod uwagę aplikacje pozwalające na realizowanie połączeń VoIP takie problemy mogą wystąpić, jeśli użytkownik usługi nie ma uprawnień do modyfikowania ustawień firewalla, routera, NAT. W sytuacji posiadania uprawnień do konfigurowania urządzeń i sieci nie ma przeszkód w korzystaniu z VoIPa.

W przypadku usług VoIP oferowanych przez TP do dużych klientów biznesowych transmisja głosu w postaci pakietowej VoIP jest realizowana w oparciu o sieć IP VPN. Użytkownicy usługi znajdujący się za NAT/PAT mają możliwość korzystania z usługi VoIP. Architektura sieci IP VPN narzuca klientowi adresowanie sieci wewnętrznej LAN klienta adresacją prywatną, co wymusza stosowanie NAT. Ze względu na definicję sieci VPN nie ma potrzeby stosowania firewall'ingu w każdym z oddziałów klienta. Jedynym miejscem gdzie może on być zastosowany do oddział HQ, który zapewnia dostęp do Internetu, nie ma to jednak wpływu na korzystanie z usługi VoIP.

Dla mniejszych i średnich przedsiębiorstw transmisja głosu w postaci pakietowej VoIP, pomimo podłączenia modemu do sieci Internet, będzie odbywała się osobnym kanałem, VC, który terminowany będzie w dedykowanej sieci VPN Service, która będzie podłączona do platformy usługowej CL4/CL5 przez urządzenie SBC.

Problemem w nomadycznym korzystaniu VoIP są poza wyżej wymienionymi kwestiami również następujące zagadnienia:

- Informacja o lokalizacji – wiarygodność informacji o lokalizacji, patrz pkt. 6
- Realizacja połączeń alarmowych – (patrz pkt. 6) co jest konsekwencją braku możliwości lokalizowania abonenta oraz niemożności routowania połączeń alarmowych

- Właściwości sieci i właściwości łącza – wydaje się, że z racji stosowania różnych technologii i urządzeń końcowych mogą występować problemy w nawiązaniu połączenia z Internetem, zachowaniem jakości usług (QoS), identyfikacją użytkownika
- Numeracja – zasady przyznawania numeracji dla usług nomadycznych nie zostały sprecyzowane. W tym momencie w Polsce, mimo przyznania numeracji 039 dla usług IP, usługi VoIP oferowane są zarówno w oparciu o numery geograficzne jak i niegeograficzne. Brak jasnych reguł w zakresie przyznawania numeracji powoduje bariery w korzystaniu z usługi, w szczególności w nawiązywaniu połączeń do takich numerów – gdyż zwykle cena połączeń kojarzona jest z rodzajem numeru

### **Skype Technologies S.A.**

Oprogramowanie *peer-to-peer* firmy Skype, które funkcjonuje w niezależny sposób przy wykorzystaniu Internetu, zostało zaprojektowane w sposób pozwalający uniknąć problemów związanych z pokonywaniem NAT i zapór ogniowych (*firewalli*).

Dzięki temu program Skype przestaje działać wyłącznie w przypadku, jeżeli podjęte zostaną pewne bardzo konkretne środki mające na celu zablokowanie lub ograniczenie działania programu.

Zachęcamy UKE do zapoznania się z komentarzami, które Skype złożył w odpowiedzi na prośbę Komisji Europejskiej o wkład w przegląd ram regulacyjnych UE w 2006 r. W komentarzach tych poruszono kwestie związane z blokowaniem i ograniczaniem działania VoIP<sup>1</sup>.

### **Polkomtel**

Zakres ograniczeń zależy od przyjętego rozwiązania i konfiguracji. Użytkownicy, realizujący połączenia z podsieci "znajdujących się za" NAT/Firewall, mogą mieć problemy z dostępem do usługi VoIP. Wymagana jest odpowiednia konfiguracja Firewall-a podsieci do której aktualnie połączony jest użytkownik. Problem NAT-a może być rozwiązany poprzez stosowanie terminali wyposażonych w funkcje "poznawania" swojego publicznego adresu IP, jednak na dzień dzisiejszy nie wypracowano niezawodnego mechanizmu ominięcia tego problemu.

### **Fone**

W systemach pracujących w technologii SIP pokonywanie NAT wymaga stosowania SIP Proxy lub serwera STUN. W przypadku firewall'i sprawa jest bardziej skomplikowana. W praktyce wymagane jest odblokowanie dedykowanych portów TCP/IP.

### **Wimax Telecom AG**

W zakresie sposobu korzystania z usługi VoIP można wyróżnić dwa rodzaje - VoIP bezpośrednio jako usługa dla użytkownika końcowego oraz VoIP jako technologia transportowa z analogowym interface'm. Aplikacje VoIP z reguły przygotowane i skonfigurowane są do uruchomienia na zasadzie plug&play niezależnie od tego, czy aplikacja pracuje za NAT czy też firewall. W przypadku realizacji obsługi VoIP poprzez dołączenie aparatów analogowych (a więc za pośrednictwem tzw. bramki) lub nawet cyfrowych (np.

---

<sup>1</sup> [http://europa.eu.int/information\\_society/policy/ecommm/info\\_centre/documentation/public\\_consult/review/index\\_en.htm](http://europa.eu.int/information_society/policy/ecommm/info_centre/documentation/public_consult/review/index_en.htm)

bezprzewodowych aparatów VoIP) ważne jest aby usługodawca obsługiwał protokół STUN (Simple Traversal of UDP through NATs).

**Pytanie: 2.**

*W jaki sposób jest identyfikowany użytkownik VoIP i jak sprawdzane są jego uprawnienia? (Czy stosuje się szyfrowanie, certyfikaty, kanały VPN lub wsparcie sprzętowe?)*

**Odpowiedzi:**

**Alcatel.**

Użytkownik VoIP posiadać powinien unikalny identyfikator, który może mieć format:

- standardowego numeru telefonicznego (np. +48 22 1234567}
- standardowego numeru telefonicznego uzupełnionego nazwą domeny (np. +48 22 1 234567@tpsa.pl)
- identyfikatora URL (np. Jan.Kowalski@nazwadomeny.pl)

Dodatkowo każdy użytkownik może mieć przydzielonych kilka identyfikatorów. Zarówno w momencie rejestracji w sieci, jak i realizacji poszczególnych połączeń uprawnienia użytkownika identyfikowane przez w/w identyfikator są weryfikowane. Komunikacja ta w celu zwiększenia bezpieczeństwa może zostać wzbogacona o następujące mechanizmy:

- zabezpieczenie hasłem (funkcja terminala abonenckiego i sieci „domowej”)
- szyfrowanie komunikacji (funkcja terminala abonenckiego i sieci)

Uprawnienie użytkownika do realizacji połączeń mogą również zależeć od sieci „wizytującej”, przez którą próbuje on realizować usługę,

**Astercity**

Istnieje możliwość zastosowania wszelkich dostępnych dziś środków autoryzacji transmisji IP. Niemniej jednak podstawową weryfikacją jest to unikalny login połączony z unikalnym hasłem. Pozwala to na swobodne i bezproblemowe przenoszenie usługi pomiędzy różnymi urządzeniami czy punktami dostępu. Dodatkowo zastosowanie kodowania transmisji danych powoduje zwiększenie wymaganej mocy obliczeniowej serwerów VoIP, co automatycznie łączy się z podwyższonymi kosztami sprzętu dla operatorów VoIP, co przy aktualnych stawkach i marżach nie jest ekonomicznie opłacalne. Dodatkowo (na chwilę obecną) zjawisko łamania kodów do kont VoIP jest zjawiskiem śladowym (osobiście się nie spotkałem z taką sytuacją ani razu), co oczywiście nie jest podstawą aby już na początku nie zwiększyć sposobów zabezpieczenia interesów abonentów.

Należy jednak pamiętać, iż każde dodatkowe zabezpieczenie zwiększa wymogi wobec użytkownika: większa ilość parametrów do konfiguracji, większy stopień skomplikowania uruchomienia usługi oraz zwiększenie zapotrzebowania w moc obliczeniową jednostki z której korzysta abonent.

Jego uprawnienia są zapisane na serwerze operatora VoIP i po zalogowaniu (autoryzacji poprzez login i hasło) serwer automatycznie daje dostęp do wszystkich dostępnych usług. Przeważnie użytkownik sam konfiguruje dostępne dla siebie usługi poprzez interfejs WWW na serwerze operatora – a to może jedynie osoba powołana do administracją danego konta (znów znajomość loginu oraz hasła).

Kanały VPN są stosowane w przesyłaniu głosu w technologii VoIP szczególnie przy większych klientach (firmy od kilkunastu kont). Zastosowanie tej technologii pozwala na

zoptymalizowanie ścieżki przebiegu pakietów IP (odpowiedź na pytanie 1), a co za tym idzie zwiększenie prawdopodobieństwa połączeń lepszej jakości (te same opóźnienia między pakietami IP, mniejsza ilość straconych pakietów).

### **Dialog.**

W protokole SIP v. 2.0, który jest obecnie szeroko stosowany w usługach VoIP, oferowanych na bazie sieci Internet użytkownik jest identyfikowany w fazie logowania (tzw. Metoda REGISTER} poprzez podanie nazwy użytkownika (tzw. SIP URI) i hasła. Format nazwy użytkownika zbliżony jest do adresu e-mail, tj.: user@domain.

W większości implementacji usług, w fazie autentykacji użytkownika wykorzystywany jest asymetryczny algorytm szyfrowania, co uniemożliwia odczytanie nazwy użytkownika i hasła przez osoby niepowołane. Ze względu na to, że komunikaty protokołu SIP są przesyłane w formie tekstowej, a kanał rozmowny jest tylko kompresowany, co daje potencjalne możliwości podsłuchu, w pewnych sytuacjach stosować można dodatkowe szyfrowanie całości komunikacji użytkownik-sieć, np. protokołem IPSec. Autoryzacja użytkownika, czyli weryfikacja jego uprawnień do wykonania określonych operacji, następuje poprzez porównanie żądanej operacji z zasubskrybowanymi usługami (w centralnej bazie danych). Modyfikacja parametrów usług może być dokonywana przez użytkownika, poprzez interfejs WWW lub za pomocą kodów wysyłanych do systemu przez komunikaty SIP (odpowiednik DTMF w PSTN). W systemach typu pre-paid autoryzacja użytkownika do wykonania połączenia odbywa się po wybraniu przez niego numeru docelowego i sprawdzeniu przez system AAA, czy kwota na koncie klienta jest wystarczająca do zrealizowania połączenia w wymaganej relacji.

### **Gabriel Grzesik.**

Pytanie sugeruje całkowitą nieznajomość zagadnienia. Tutaj znaleźć można wyczerpujące informacje: <http://pl.wikipedia.org/wiki/VoIP> <http://www.voip-info.org/wiki/>

### **GTS Energis.**

Użytkownik w sieci VoIP może być identyfikowany na trzy sposoby:

1. Numer telefoniczny
2. Nazwa konta użytkownika: w szczególnym przypadku jest nazwa konta może być jednoznaczna z numerem telefonicznym
3. Adresacja IP

Każdy identyfikator w sieci jest skojarzony z odpowiednim profilem uprawnień określającym między innymi:

- dostępne kategorie połączeń;
- dostępne usługi dodane;
- sposób rozliczeń (opłaty z góry, z dołu).

Do identyfikacji i uwierzytelnienia użytkownika wykorzystuje się z bezpieczne protokoły z szyfrowaniem obecnie tylko sesji sygnalizacyjnych. Obecne zabezpieczenia oraz metody uwierzytelniania oceniamy jako wystarczające.

Celu zapewniania takiego samego standardu usług wszyscy dostawcy usługi powinni stosować te metody uwierzytelniania z szyfrowaniem transmisji.

Należy również zwrócić uwagę na wymaganie stosowanie przez operatorów zabezpieczeń samej platformy sieciowej VoIP przez atakami i próbami włamań.

Brak odpowiednich zabezpieczeń platformy może powodować utratę ważnych danych o połączeniach i użytkownikach w sytuacjach ewentualnego dochodzenia odpowiedzialności. Obecnie istnieją odpowiednie środki oraz procedury umożliwiające pełne zabezpieczenie platformy niepowołanym dostępem.

### **Internet Group.**

W naszej usłudze, opartej o technologię VoIP, klient jest identyfikowany poprzez nazwę konta telefonii internetowej oraz hasło. Nazwa konta jest dostępna w postaci jawnej, hasło zakodowane. Przed wykonaniem jakiegokolwiek połączenia, klient musi podłączyć się do naszego systemu tzn. pozwolić na weryfikację nazwy konta i hasła. Hasło jest kodowane z wykorzystaniem algorytmu MD.5

Nazwa konta i hasło może być wpisane albo do bramki VoIP czy telefonu IP, jak i programu komunikatora. Ograniczeniem w naszej sieci jest możliwość korzystania jedynie z udostępnianego przez nas komunikatora HaloNet.

### **Junisoftex**

Użytkownik identyfikowany jest poprzez przyznany mu unikalny identyfikator i hasło, będący jednocześnie numerem "wewnętrznym" naszej sieci. Dla połączeń wychodzących nie stosujemy szyfrowania certyfikatów itp. Użytkownicy korzystający z naszych bramek VOIP mogą używać połączeń szyfrowanych w ramach sieci (wsparcie sprzętowe przez urządzenie).

### **KIGEiT**

#### ***powinno być:***

- identyfikacja do wyboru - jednym z pól ENUM
- przydział ENUM na zasadach dzisiejszego przydziału numeru (umowa abonencka)
- zabezpieczanie ruchu VoIP (opcjonalnie) - zależnie do wariantu usługi - poza regulacjami

#### ***obecnie:***

- identyfikacja po numerze PNK przydzielonym przez operatora na potrzeby usługi VoIP (zależnie do usługi)

### **Dariusz Bakula (pracownik Lucent).**

W przypadku najczęściej stosowanego w telefonii VoIP protokołu SIP, do identyfikacji stosuje się parametr nagłówka URI, który może występować w postaci (a) Tel URI lub (b) SIP URI

(a) Tel URI: tel:+48523491293

(b) SIP URI w jednej z czterech postaci:

sip:+48523491293@<domena\_lokalna>;user=phone,

sip:<id\_użytkownika>@<operator\_macierzysty>, lub

sip:<id\_użytkownika>@<domena\_użytkownika>, lub

sip:<adres\_IP>

Jako „id\_użytkownika” stosowany może być numer E.164.

W ramach sieci IMS, zgodnie ze standardem określonym przez 3GPP możliwa jest jednoznaczna rejestracja i identyfikacja abonenta na podstawie informacji (w tym nr E.164) zawartych w bazie danych HSS (*Home Subscriber Server*) – z zastrzeżeniem co do

ograniczonych możliwości weryfikacji danych w przypadku przypadkowej lub celowej ingerencji w informacje zawarte w identyfikatorze URI. W przypadku VoIP w sieci publicznej jednoznaczna identyfikacja nie jest obecnie możliwa - patrz odp. na pytanie 1 (a).

### **NASK**

2. W chwili obecnej stosowana jest jedynie prosta autoryzacja na bazie identyfikatora użytkownika (stanowiącego jednocześnie numer telefoniczny) oraz statycznego hasła. Nie jest to rozwiązanie bezpieczne, jednakże stosowanie dodatkowych metod zabezpieczania w znaczącym stopniu podniosłoby koszt instalacji abonenckiej. Podniesienie poziomu bezpieczeństwa poprzez stosowanie szyfrowania i rozwiązań VPN ma miejsce dla usług telefonii IP nie-nomadycznej.

### **Net Telecom**

W sieci Actio użytkownik identyfikowany jest poprzez przyznany numer telefonu (login) oraz hasło SIP. System nasz wymusza na użytkowniku co miesięczną zmianę hasła, natomiast dostęp do bilingu online jest szyfrowany. Oczywiście duża część bezpieczeństwa pracy użytkownika leży po jego stronie. Należy zwrócić tu uwagę na fakt iż użytkownik musi zabezpieczać swoim własnym hasłem dostęp do adaptera VoIP lub innego podobnego urządzenia, które to z kolei przechowuje wspomniane dane osobowe użytkownika tj numer telefonu i hasło SIP. W przeciwnym wypadku potencjalny włamywacz może przechwycić dane użytkownika i dzwonić na jego koszt.

### **Onet**

Użytkownik w sieci VoIP może być identyfikowany na dwa sposoby (Identyfikator):

1. Numer telefoniczny
2. Nazwa konta użytkownika: w szczególnym przypadku jest nazwa konta może być jednoznaczna z numer telefonicznym

Każdy Identyfikator w sieci jest skojarzony z odpowiednim profilem uprawnień określającym między innymi:

- dostępnymi kategoriami połączeń;
- dostępnymi usługami dodanymi;
- sposobem rozliczeń (opłaty z góry, z dołu).

Do identyfikacji użytkownika wykorzystuje się bezpieczne protokoły.

### **Inotel**

Użytkownik identyfikowany jest podczas logowania na platformie jego konta SIP przy pomocy Loginu i hasła,

### **TPSA**

Identyfikacja w różnych rozwiązaniach wygląda różnie. Zazwyczaj w celu identyfikacji abonentów używa się loginu i hasła powiązanych z numerem telefonu, niekiedy również wykorzystuje się adresy IP. Możliwa jest również identyfikacja użytkownika na podstawie MAC adresu jego urządzenia, przy czym metoda ta stosowana samodzielnie nie jest w pełni wiarygodna ze względu na łatwość modyfikacji MAC adresów.

W sieci TP dla klientów indywidualnych identyfikacja użytkownika usługi VoIP i weryfikacja jego uprawnień następuje na podstawie numerów identyfikacyjnych nadanych urządzeniom Livebox (Numer seryjny + MAC address), skojarzonych z numerem VoIP.

Dla dużych klientów biznesowych ze względu na charakter usługi, pojęcie bezpieczeństwa zamyka się w definicji sieci VPN, sieć VPN klienta jest identyfikowana poprzez *community\_name* czyli vrf a następnie mapowana do VLAN-u, który transportowany jest do platformy VoIP CL5 gdzie następuje weryfikacja uprawnień. Urządzeniem oddzielającym VPN-y klienckie jest Session Border Controller.

Dla mniejszych klientów biznesowych identyfikacja użytkownika VoIP jako końcówki klienckiej będzie odbywać się poprzez adres IP oraz numer E.164. Nie będzie stosowane szyfrowanie, certyfikaty, wsparcie sprzętowe. Każdy modem będzie korzystał dwóch kanałów wirtualnych, 1 - Internet, 2 - dedykowane dla VoIP terminowane w Service VPN.

### **Skype Technologies S.A.**

Funkcja identyfikacji i autoryzacji użytkownika została wbudowana w aplikację *peer-to-peer* firmy Skype, która funkcjonuje w niezależny sposób przy wykorzystaniu Internetu.

Stosowany przez Skype system identyfikacji i autoryzacji użytkownika opiera się wyłącznie na szyfrowaniu standardowym. Został on uznany przez niezależnych ekspertów za znacznie lepszy od stosowanego w tradycyjnej publicznej komutowanej sieci telefonicznej (PSTN) oraz od innych rozwiązań stosowanych w technologii VoIP.

Dzięki zastosowaniu własnego weryfikatora certyfikatów (*Certificate Authority*) i systemu wydawania certyfikatów, Skype jest w stanie w skuteczny sposób zapewnić, by żaden z użytkowników nie mógł podać się za innego użytkownika Skype.

Weryfikacja użytkownika następuje w oparciu o powszechnie stosowane klucze publiczne, na podstawie których program Skype może błyskawicznie potwierdzić tożsamość użytkownika bez konieczności łączenia się z serwerem centralnym.

Poza identyfikacją i autoryzacją Skype zapewnia także ochronę prywatności użytkowników poprzez szyfrowanie sesji *peer-to-peer* przy zastosowaniu blokowego systemu szyfrowania AES (*Advanced Encryption System*) w 256-bitowym trybie licznikowym, operującym na liczbach całkowitych. W celu ustanowienia szyfrowanej za pomocą AES sesji między dwoma użytkownikami, ich komputery muszą uzgodnić wspólny klucz sesji. Program Skype dzieli zadanie wygenerowania klucza na dwa zadania cząstkowe. Każdy klient otrzymuje jedno z zadań cząstkowych, polegających na wygenerowaniu 128 bitów z 256-bitowego klucza. Oznacza to, że w procedurze brak jest jakiegokolwiek możliwości zmuszenia programu do skorzystania ze słabego klucza.

Na stronie internetowej Skype znajduje się specjalna sekcja, w której w bezpośredni sposób porusza się kwestie związane z bezpieczeństwem (jest to doskonała ilustracja otwartego dialogu, jaki Skype prowadzi z własnej inicjatywy ze swoimi użytkownikami i nabywcami). Z podobną otwartością zamieszczono w sekcji pełną wersję sprawozdania z auditu bezpieczeństwa przeprowadzonego przez niezależnego zewnętrznego eksperta. Sprawozdanie to jest dostępne bezpośrednio na stronie <http://www.skype.com/security/files/2005-031securityevaluation.pdf>.

### **Polkomtel**

Identyfikacja użytkownika odbywa się na podstawie Nazwy i Hasła, dodatkowym zabezpieczeniem jest szyfrowanie połączenia.

## **Fone**

W systemach SIP jest szereg metod autentykacji użytkownika, jednak w praktyce sprowadza się to do podania odpowiednich identyfikatorów i haseł w procesie rejestracji urządzenia lub oprogramowania SIP. Używamy również systemów, które sprzętowo wspierają autentykację. W systemach tych każdy terminal posiada unikalny identyfikator, który stanowi jeden z elementów autoryzacji. Identyfikator ten jest "zaszywany" hardware'owo. Uprawnienia związane z danym terminalem ustawiane są bezpośrednio na platformach VoIP. Platforma autoryzując terminal (softphone) sprawdza ustawienia konta dla tego terminala i tym samym pozwala realizować tylko te usługi, które zostały aktywowane dla takiego konta. Tylko dedykowane systemy, które wspierają identyfikację użytkownika VoIP sprzętowo pozwalają na stosunkowo bezpieczną transmisję głosu przez otwarty Internet. Najczęściej takie połączenia są szyfrowane. Próba podszycia się pod którykolwiek z terminali takich systemów jest bardzo trudna, z uwagi na to że często stosowane są w takich przypadkach niestandardowe protokoły komunikacji poszczególnych elementów systemu. Rozwiązania bazujące na technologii SIP są stosunkowo mniej bezpieczne, jednak z uwagi na niską cenę terminali końcowych ten aspekt często jest ignorowany przez nabywców.

## **Wimax Telecom AG**

W przypadku usługi VoIP na zasadzie aplikacji identyfikacja następuje poprzez login i hasło. W przypadku usługi analogowej realizowanej poprzez transport VoIP istnieje możliwość dodatkowych mechanizmów autentykacji poprzez rozwiązania sprzętowe adaptera telefonicznego (ATA).

### ***Pytanie: 3.***

***W jaki sposób przyznany użytkownikowi VoIP numer telefoniczny jest wykorzystywany do adresowania użytkownika i realizacji połączeń? (Czy jest on jednocześnie identyfikatorem użytkownika?)***

### ***Odpowiedzi:***

#### **Alcatel.**

Użytkownik VoIP posiadać powinien unikalny identyfikator, który może mieć format:

- standardowego numeru telefonicznego (+48 22 1234567)
- standardowego numeru telefonicznego uzupełnionego nazwą domeny (+48 22 1 234567@nazwadomeny.pl)
- identyfikatora URL (np. Jan.Kowalski@nazwadomeny.pl)

Dodatkowo każdy użytkownik może mieć przydzielonych kilka identyfikatorowi np.+48 22 1 234567 oraz Jan.Kowalski@nazwadomeny.pl) Sposób osiągania abonenta VoIP zależy od terminala inicjującego połączenie: dla terminali telefonicznych (tradycyjnych i oraz VoIP) można uzyskać wszystkie standardowe cechy tradycyjnego (sieci PSTN) planu numeracji.

#### **Astercity**

Istnieje możliwość skorelowania numeru telefonicznego z jego identyfikatorem, lecz nie jest to stosowane. Główny powód, to fakt, iż nie każdy użytkownik chce mieć numer geograficzny przypisany do swojego konta VoIP. Jeśli konto nie posiada przypisanego takiego numeru, wtedy służy ono jedynie do realizowania połączeń wychodzących.

Użytkownicy decydują się na takie rozwiązania, gdyż przeważnie posiadanie takiego numeru wiąże się z kosztami.

Rozwiązanie to jest natomiast szerzej stosowane na rynku firm i instytucji – tam komunikacja przeważnie odbywa się dwustronnie.

Drugim powodem jest zwiększenie poufności danych – gdyby numer telefoniczny był zarazem loginem użytkownika, to każdy znałby już połowę danych potrzebnych do korzystania z jego konta (login i hasło).

Również w takim przypadku należałoby stosować pełen numer wraz z kierunkowym na dany kraj – w innym przypadku mogło by wystąpić dublowanie numerów między krajami a co za tym idzie potencjalne konflikty między serwerami różnych operatorów, bądź w ramach jednego serwera operatora świadczącego usługi w wielu krajach.

Numer telefoniczny jest wykorzystywany do adresowania użytkownika jedynie w przypadku realizacji połączeń przychodzących. Oczywiście warunkiem tutaj jest, aby w momencie inicjowania połączenia przychodzącego użytkownik miał uruchomiony sprzęt oraz był zalogowany do sieci.

### **Dialog.**

Obie formy są stosowane w aktualnie dostępnych usługach. W jednym przypadku nazwa użytkownika może zawierać numer telefoniczny, np.: 0717780001@dialnet.pl, wówczas w/w nazwa jest wykorzystywana w fazie logowania, a pierwszy człon nazwy stanowi jednocześnie numer telefoniczny. Numer ten jest wykorzystywany jako numer źródłowy w połączeniach wychodzących.

W drugim przypadku użytkownik w fazie logowania może wykorzystać login typu j.nowak@domena, zaś numer telefoniczny lub kilka numerów mogą zostać mu przypisane poprzez dodatkowe pole AOR.

### **Gabriel Grzesik.**

Tak, jest jednoznacznie identyfikatorem użytkownika. Nie mniej niż w przypadku telefonów postpaid/prepaid GSM.

### **GTS Energis.**

Przyznany numer telefoniczny, może, ale nie musi być jednocześnie identyfikatorem użytkownika. Jeśli identyfikatorem jest nazwa konta użytkownika to numer telefoniczny jest tłumaczony na odpowiadające mu konto użytkownika i na tej podstawie kierowane jest połączenie.

Umożliwia to wirtualizację użytkownika (dostępność użytkownika jednocześnie pod wieloma numerami).

Jednoznacznym identyfikatorem użytkownika powinien być login użytkownika, do którego może być przywiązanych wiele numerów telefonicznych.

Jako dodatkowy identyfikator należy również wykorzystać adres IP użytkownika, który generował połączenia.

Powinien istnieć zakaz zmiany numeracji użytkownika na inną numerację.

### **Internet Group.**

Opcjonalnie numer telefonu jest przypisywany do konta telefonii internetowej. Nie jest on konieczny do nawiązywania połączeń wychodzących, a jedynie umożliwia dodzwanianie się do klienta z sieci telefonicznej (stacjonarnej bądź komórkowej). Do danej nazwy konta może być przypisana nieograniczona liczba numerów telefonicznych, co umożliwia przykładowo

telefonowanie do danego klienta z różnych stref numeracyjnych, po lokalnych stawkach połączenia.

### **Junisoftex**

Przyznany użytkownikowi publiczny numer telefoniczny nie jest wykorzystywany do adresowania użytkownika i realizacji połączeń.

### **KIGeIT**

*powinno być:*

- wykorzystanie ENUM ureguje kwestie podniesione w pytaniu

*obecnie:*

- identyfikacja po numerze PNK przydzielonym przez operatora na potrzeby usługi VoIP (zależnie do usługi)

### **Dariusz Bakula (pracownik Lucent).**

Patrz odpowiedź na pytanie 2. W przypadku stosowania numerów E.164, możliwe są w sieciach NGN dwa modele marszrutowania (routing):

(a) krok-po-kroku, gdzie z analizy cyfr wynika adres SIP Proxy dla każdego etapu połączenia (punktu styku)

(b) konwersja numeru E.164 na adres SIP Proxy odpowiedzialnego za obsługę abonenta B oraz odzwierciedlenie tego adresu na adres IP z wykorzystaniem serwera DNS. Wymagane jest zatem wykorzystanie funkcji ENUM.

Dla sieci NGN szczegóły związane z kierowaniem połączeń z wykorzystaniem numerów E.164 standaryzowane są przez TISPAN, a stosowne prace są w toku. \

### **NASK**

Z punktu widzenia praktycznej obsługi użytkowników numer telefoniczny przyznany użytkownikowi jest jednocześnie jego numerem identyfikacyjnym używanym w procesie autoryzacji. Zmniejsza to liczbę danych, które abonent musi znać aby korzystać z usługi. Upraszcza to także zarządzanie samą usługą.

### **Net Telecom**

Tak - w sieci Actio przyznany numer telefoniczny jest jednocześnie identyfikatorem użytkownika.

### **Onet**

Brak opinii.

### **Inotel**

W INOTEL numer jest aliasem do konta SIP, nie jest identyfikatorem klienta.

### **TPSA**

Nie jesteśmy w stanie powiedzieć jak działa usługa u innych operatorów. Dla klientów indywidualnych w sieci TP numer przydzielony abonentowi służy do identyfikacji użytkownika dla połączeń przychodzących z sieci IP oraz publicznej sieci telefonicznej. Dla klientów biznesowych przyznany numer użytkownikowi jednoznacznie identyfikuje użytkownika w sieci i nigdzie nie jest zmieniany.

### **Skype Technologies S.A.**

Podstawowa metoda adresowania użytkownika w Skype opiera się na wykorzystaniu utworzonego przez użytkownika identyfikatora SkypeID oraz dodatkowych informacji podanych przez użytkownika w procesie rejestracji identyfikatora SkypeID.

W przypadku opcjonalnych, dodatkowo płatnych funkcji dodatkowych, w celu identyfikacji użytkownika Skype może także skorzystać z informacji podanych przez niego podczas dokonywania płatności.

Skype nie wykorzystuje numerów telefonicznych do identyfikacji użytkowników.

Niemniej jednak partnerzy Skype (podmioty świadczące usługi łączności elektronicznej, obsługujące bramki do tradycyjnych publicznych komutowanych sieci telefonicznych) wykorzystują numery telefoniczne do identyfikacji użytkowników oraz do kierowania i transportowania połączeń w publicznych komutowanych sieciach telefonicznych (PSTN).

### **Polkomtel**

Numer telefoniczny z zakresu numeracji strefowej jest i powinien być stosowany tylko i wyłącznie w przypadku stacjonarnych użytkowników VoIP.

Implementacja rozwiązania umożliwiającego prezentowanie się numerem strefowym w zależności od strefy numeracyjnej, z której połączenie jest inicjowane przez użytkownika nomadycznej usługi VoIP jest niewykonalna technicznie, dlatego użytkownicy VoIP którzy posiadają możliwość nomadycznego korzystania z usług, powinni korzystać z wydzielonego wskaźnika AB, zgodnie z PNK (AB=39). Właściwa prezentacja numeru abonenta A jest kluczowa dla wielu usług wykorzystujących numer abonenta A, jako parametr wejściowy w logice usługi. Brak lub niepoprawna informacja adresowa o numerze abonenta A jest znaczącym utrudnieniem w przypadku żądania informacji przez "podmioty uprawnione", dotyczy to oczywiście również usługi CLIR.

### **Fone**

Przyznany numer telefoniczny może być wykorzystywany do adresowania użytkownika jednak nie jest to niezbędne. Każdy z systemów VoIP posiada różne metody adresowania użytkowników wewnątrz systemu VoIP i praktycznie nie ma najmniejszego problemu w zmianach numerów telefonicznych. Z punktu widzenia technologii numer telefoniczny w żaden sposób nie musi być równocześnie adresem użytkownika. Jest to szczególnie widoczne w usługach, gdzie klient VoIP posiada więcej niż jeden numer przypisany do swojego konta VoIP. Praktycznie nie ma żadnych ograniczeń co do ilości takich numerów oraz ich zasięgu geograficznego (dotyczy to zarówno numerów krajowych jak i zagranicznych DID).

### **Wimax Telecom AG**

Numer jest dostępny lokalnie (w kraju) jak i międzynarodowo do realizowania połączeń przychodzących i wychodzących. Numer telefoniczny może, lecz nie musi być jednocześnie identyfikatorem użytkownika.

**Pytanie: 4.**

**Czy w ramach VoIP oraz współpracy VoIP z PSTN są poprawnie realizowane usługi CLIP i CLIR?**

**Odpowiedzi:**

**Alcatel.**

Istnieją standardy i mechanizmy poprawnej realizacji w/w funkcji, ich praktyczna implementacja zależy od sposobu realizacji sieci. Przykładem takiego standardu jest: Q.1912,5 „Interworking between Session Initiation Protocol (SIP) and Bearer Independent Call Control protocol or ISDN User Part” definiujący zasady współpracy sieci PSTN/ISDN i VoIP (SIP)

**Astercity**

Technicznie nie ma najmniejszej przeszkody, aby wymiana sygnalizacyjna pomiędzy sieciami PSTN a VoIP była pełna, czyli były przekazywane nie tylko sygnały CLIP i CLIR ale również wszystkie inne zgodne z przyjętym standardem. Kodowanie / dekodowanie i analiza tych sygnałów jednak musiałyby się odbywać na serwerze operatora VoIP, a co za tym idzie znów poruszamy się w zakresie zwiększenia mocy obliczeniowej sprzętu. Również celowość innych sygnałów poza CLIP i CLIR jest dyskusyjna. Wydaje się, iż pomimo przekazania pełnej sygnalizacji (np. ISDN) nie wszystkie sygnały można wykorzystać lub nie widać w tym celowości.

Niemniej sygnały CLIP i CLIR są na tyle popularne i szeroko stosowane, iż na chwilę obecną nie jest to temat problematyczny czy dyskusyjny. Oczywiście przy założeniu, że wszyscy operatorzy pośredni przekazują tę sygnalizację prawidłowo.

**Dialog.**

Usługi CLIP i CLIR są realizowane w sieciach VoIP, jednak zależy to od funkcjonalności danej usługi oferowanej przez operatora VoIP. W prostych implementacjach usług VoIP, funkcje CLIP i CLIR mogą być realizowane przez urządzenia lub aplikacje abonenckie. Jednak dla zachowania pełnej kontroli nad CLIP i CLIR przez operatora VoIP, subskrypcja w/w usług odbywa się przez portal WWW.

**Gabriel Grzesik.**

Tak, poprawność działania CLIP i CLIR jest niemal całkowita. Wyjątkiem są sytuacje kiedy operator nie korzysta z oficjalnego i drogiego interkonektu z sieciami komórkowymi, a robi to w inny sposób, taniej, jednocześnie obniżając klientom ceny połączeń do sieci komórkowych. Nie będę donosicielem, więc nie napiszę kto to robi i w jaki sposób, życząc dużo zdrowia i prosperity firmom próbującym obejść chore regulacje mające swój początek w monopolistycznym podziale tortu pomiędzy kilku dużych graczy.

**GTS Energis.**

Obecnie istnieją środki techniczne zapewniające możliwość poprawnego realizowania usług CLIP oraz CLIR.

Doświadczenia wskazują, że nie zawsze operatorzy zapewniają realizację tej usługi.

Przykładem mogą być usługi oparte rozwiązania bazujących na oprogramowaniu VoIP gdzie nie zawsze do konta abonenta jest przypisany numer geograficzny.

Usługa CLIP oraz CLIR powinna być również zawsze dostępna regulowana na podobnych zasadach jak ma to miejsce w zakresie klasycznych usług telefonicznych.

Wskazane jest również, aby stosowane metody zapewniające jednoznaczną identyfikację prezentacji użytkownika poprzez jego numer CLI uzyskany od operatora.

#### **Internet Group.**

W naszej sieci klient ma możliwość skonfigurowania (aktywacji lub blokady) opcji CLIP. Każdy klient bezpłatnie określa więc czy chce aby jego numer wyświetlał się na telefonie odbiorcy.

#### **Junisoftex**

Poprawnie jest realizowany tylko CLIP. Na dzień dzisiejszy nie mamy technicznej możliwości realizacji CLIR.

#### **KIGeIT**

##### ***powinno być:***

- CLIP i CLIR powinny być poprawnie realizowane

##### ***obecnie:***

- pomiędzy platformami nie ma współpracy również w zakresie CLIP/CLIR

- na styku sieci IP i PSTN dostępność CLIP/CLIR zależy od platformy/operatora - niektóre platformy nie realizują identyfikacji w ogóle, inne prezentują numer główny bramy IP/PSTN, a jeszcze inne prezentują poprawnie

#### **Dariusz Bakula (pracownik Lucent).**

Usługa CLIP i CLIR oferowana jest typowo w sieciach VoIP. Tym niemniej, jednoznacznie poprawna realizacja usługi CLIP i CLIR możliwa jest przy spełnieniu dwóch warunków: transparentnym przesłaniu numeru E.164 oraz możliwości zweryfikowania poprawności informacji adresowej abonenta A. Patrz odp. na pytanie 2 i 5.

#### **NASK**

Funkcjonowanie usług CLIP i CLIR jest całkowicie niezależne od stosowanych terminali VoIP i w pełni realizowane po stronie systemu telefonii IP. Od rodzaju terminala zależy jedynie prezentacja numeru strony B. Współpraca z siecią PSTN jest realizowana prawidłowo.

#### **Net Telecom**

Tak - w sieci Actio w są pełni wspierane i realizowane usługi CLIP i CLIR.

#### **Onet**

Usługi są z reguły realizowane poprawnie, o ile operator nie terminuje ruchu przez bramki GSM.

#### **Inotel**

TAK

## **TPSA**

Nie jesteśmy w stanie powiedzieć jak działa usługa u innych operatorów. W sieci TP usługi te są poprawnie realizowane dla abonentów VoIP.

## **Skype Technologies S.A.**

Przede wszystkim należy podkreślić, że Skype działa w oparciu o „listę przyjaciół” składającą się z użytkowników (korzystających z samodzielnie utworzonych identyfikatorów SkypeID), którzy pozostają między sobą w relacji zaufania. Funkcje CLIP/CLIR nie są zatem istotne z punktu widzenia Skype.

Skype nie wykorzystuje numerów telefonicznych do identyfikacji użytkowników.

Niemniej jednak partnerzy Skype (podmioty świadczące usługi łączności elektronicznej, obsługujące bramki do tradycyjnych publicznych komutowanych sieci telefonicznych) wykorzystują numery telefoniczne do identyfikacji użytkowników oraz do kierowania i transportowania połączeń w publicznych komutowanych sieciach telefonicznych (PSTN).

Obecnie partnerzy Skype nie udostępniają funkcji CLIP/CLIR w przypadku usługi SkypeOUT, natomiast zazwyczaj udostępniają je w przypadku usługi SkypeIN. Rozwiązanie to spotyka się z zadowoleniem wszystkich zainteresowanych stron.

## **Polkomtel**

Z doświadczenia Polkomtela wynika że często występują problemy głównie z usługą CLIP, powoduje to duże niezadowolenie klientów, reklamacje, błędne działanie niektórych usług, w których parametrem wejściowym w logice usługi jest numer abonenta A (wywołującego). Brak lub niepoprawna informacja adresowa o numerze abonenta A jest znaczącym utrudnieniem w przypadku żądania informacji przez "podmioty uprawnione", dotyczy to oczywiście również usługi CLIR.

## **Fone**

Realizacja tej usługi zależy wyłącznie od świadomości technologicznej operatora VoIP oraz jego możliwości technicznych (szczególnie dotyczy to możliwości terminacji połączeń w sieci PSTN z wykorzystaniem sygnalizacji SS7). Z uwagi na niską cenę użytkownicy końcowi zostali "przyzwyczajeni", że połączenia są realizowane z CLIR. Dlatego też usługi CLIP i CLIR nie stanowią szczególnych utrudnień dla użytkownika końcowego. W przypadku połączeń w ramach tej samej platformy VoIP to operator decyduje czy identyfikator użytkownika jest prezentowany na terminalu drugiej strony połączenia.

## **Wimax Telecom AG**

To zależy od usługodawcy, ale co do zasady usługi te realizowane są w pełni poprawnie. Dla wygody użytkownika i obsługa może być zarządzana z poziomu przeglądarki internetowej.

**Pytanie: 5.**

***Czy identyfikacja numeru abonenta wywołującego (użytkownika VoIP) jest wiarygodna? (Czy numery przydzielone użytkownikowi są przekazywane do sieci PSTN i nie zamieniane na wejściu do sieci PSTN?)***

**Odpowiedzi:**

**Alcatel.**

Istnieją standardy np. w/wym. Q. 1912.5 i mechanizmy poprawnej realizacji w/w funkcji, ich praktyczna implementacja zależy od sposobu realizacji sieci. Wiarygodność prezentacji zależy od standardów, jakie stosuje Operator. W przypadku abonentów z klasycznymi terminalami analogowymi/ISDN podłączonymi poprzez bramy dostępowe, (które to bramy należą do operatora sieci), identyfikacja abonenta wywołującego jest wiarygodna, natomiast w przypadku, gdy abonent podłączony jest bezpośrednio poprzez terminal SIP lub bramy rezydentne (residential access gateways) lub inne urządzenia dostępowe IP (IP access devices), które znajdują się w gestii abonenta (customer premises), w takim przypadku wymagana jest autentykacja takiego użytkownika poprzez mechanizmy, które musi zapewnić operator sieci (np. http digest).

**Astercity**

Na to pytanie nie ma jednoznacznej odpowiedzi. Technicznie nie ma przeszkód, aby informacja CLI była przekazywana poprawnie, niemniej zawsze istnieje możliwość, iż operator pośredni usunie informacje, przekłamie ją lub podstawí swoją. Niemniej zjawisko to może wystąpić również w transmisji PSTN – PSTN i fakt, iż jedna strona rozmowy korzysta z technologii VoIP nic tu nie zmienia. Zjawisko to można często zaobserwować, gdy klienci lub operatorzy korzystają z bramek GSM do terminacji ruchu komórkowego wychodzącego. Połączenia GSM – GSM są w tej chwili tańsze (między kartami SIM) niż stawka interconnectowa PSTN – GSM.

**Dialog.**

Wiarygodność identyfikacji zależy bezpośrednio od implementacji usług VoIP przez konkretnego operatora. Z reguły, jeżeli prezentacja numeru jest zapewniona przez operatora wówczas jest ona wiarygodna. W innym przypadku (aby uniknąć prezentacji numeru wiodącego wiązki) najczęściej połączenia wychodzące z sieci VoIP do sieci PSTN są pozbawione prezentacji numeru źródłowego.

**Gabriel Grzesik.**

Jest wiarygodna. Bardziej niż w TP SA.

**GTS Energis.**

Użytkownik może prezentować się pod innym numerem niż numer przypisany do identyfikatora. Zmiana numeru prezentowanego jeszcze przed centralą PSTN możliwa jest na bramie VoIP (VoIP Gateway).

Umożliwia to z jednej strony definiowanie odpowiedników „numerów wiodących”, z drugiej strony jednak czyni prezentowany numer niewiarygodnym, co tworzy zagrożenie wyłudzeń i problemy z identyfikacją abonenta generującego połączenia.

Zmiana numeru prezentowanego dozwolona powinna być więc jedynie w obrębie numeracji przydzielonej klientowi końcowemu. Jednocześnie powinny istnieć mechanizmy rejestracji

IP, z którego połączenie było realizowane (z dokładnością do najbliższego, względem użytkownika, IP publicznego) patrz: punkt 6.

### **Internet Group.**

Identyfikacja numeru jest o tyle wiarygodna, że pokazuje numer przypisany do danego konta telefonii internetowej. Nie mówi ona oczywiście nic o lokalizacji danego klienta. W przypadku większej liczby numerów, przypisanych do danego konta telefonii internetowej, klient sam określa, który z nich ma być wyświetlany u odbiorcy połączenia.

Nasz firma nie dokonuje żadnych zmian w przesyłanej numeracji zarówno przez sieć IP jak i PSTN.

### **Junisoftex**

W związku z brakiem CLIR nie ma na razie problemu tego typu identyfikacji.

### **KIGEiT**

- zgodnie z uwagą 1 i 4

#### **obecnie:**

- przydzielana numeracja VoIP w większości przypadków nie jest przekazywana do sieci PSTN - zależnie do rozwiązania technicznego lub rodzaju usługi oferowanej przez operatora

### **Dariusz Bakula (pracownik Lucent).**

Tak w sieci IMS tak, z wykorzystaniem informacji zawartych w profilu abonenta zdefiniowanym w bazie danych HSS. W innych przypadkach nie ma takiej gwarancji. W zależności od zastosowanych rozwiązań możliwe jest w ogólności transparentne przesyłanie numeru E.164 będącego elementem identyfikatora URI poprzez punkty styku IP-IP oraz IP-TDM do sieci PSTN. W przypadku abonenta nomadycznego poruszającego się w publicznej sieci internetowej nie ma gwarancji, że numer abonenta zostanie przekazany przez punkty styku będące poza kontrolą operatora świadczonego usługę, dlatego najczęściej podstawiany jest numer fikcyjny (*dummy number*).

### **NASK**

Identyfikacja numeru abonenta jest wiarygodna. Każde połączenie abonenta telefonii IP ma nadawany numer strony A przez system telefonii IP, niezależnie od tego jaki numer prezentuje terminal abonenta w trakcie zestawiania połączenia. Numer ten jest zgodny z PNK i jako taki nie jest w żaden sposób zamieniany na wejściu do sieci PSTN.

### **Net Telecom**

Tak - identyfikacja użytkownika jest wiarygodna co oznacza iż numer przydzielony użytkownikowi jest w pełni przekazywany do sieci PSTN

### **Onet**

Generalnie nie są zmienione. Ale odpowiedzialni za rozpoczęcie połączenia mogą teoretycznie zrobić wszystko.

Warto by wpłynąć regulacje tej kwestii.

### **Inotel**

TAK, nie są zmieniane na styku z PSTN

## **TPSA**

W tym przypadku również, TP nie może wypowiadać się na temat wiarygodności identyfikacji w sieciach innych operatorów. W sieci TP identyfikacja jest wiarygodna.

## **Skype Technologies S.A.**

Skype nie wykorzystuje numerów telefonicznych do identyfikacji użytkowników.

Obecnie partnerzy Skype nie udostępniają funkcji CLIP w przypadku usługi SkypeOUT, ponieważ w momencie wykonywania przez użytkownika połączenia w trybie SkypeOUT identyfikatorowi SkypeID nie jest przypisany żaden numer telefonu.

## **Polkomtel**

Z doświadczeń Polkomtel wynika że nie jest wiarygodna to informacja wiarygodna, numer wywołujący jest bardzo często podmieniany lub kasowany, powinien istnieć odpowiedni zapis ustawowy w Prawie Telekomunikacyjnym zabraniający zmian numeru abonenta A, który uniemożliwia jednoznaczną identyfikację abonenta wywołującego.

## **Fone**

Z uwagi na możliwości technologiczne identyfikacja abonenta wywołującego nie jest wiarygodna. Dotyczy to zarówno możliwości samych systemów VoIP jak również stosowanych metod terminacji takich połączeń. Z mojego punktu widzenia nie należy traktować tej informacji jako wiarygodnej.

## **Wimax Telecom AG**

Identyfikacja jest w pełni wiarygodna, jeśli usługodawca posiada kontrole nad infrastrukturą VoIP i prawidłowy mapping do sieci PSTN.

### ***Pytanie: 6.***

***Czy dostawca umożliwi realizację połączeń użytkowników VoIP z numerami alarmowymi? Jeśli tak, to w jaki sposób określana jest lokalizacja geograficzna użytkownika?***

### ***Odpowiedzi:***

#### **Alcatel.**

Tak, istnieją bowiem standardy i mechanizmy poprawnej realizacji takiej funkcji, ich praktyczne wdrożenie zależy jednak od sposobu realizacji sieci.

Na dzień dzisiejszy jest to realizowane w sposób następujący: w momencie rejestracji w sieci, następuje korelacja identyfikatora (ów) abonenta z adresem IP, pod którym w danym momencie się znajduje. W momencie realizacji połączenia do służb alarmowych urządzenia sieciowe, na podstawie adresu IP określają geograficzną lokalizację abonenta i stosują odpowiednie kierowanie połączenia by osiągnąć najbliższą służbę alarmową. Jest to mechanizm posiadający szereg ograniczeń, ale powszechnie stosowany w sieciach VoIP na świecie.

W dalszej perspektywie czasowej standardy TISPAN przewidują, że urządzenia sieci „wizytującej” będą generowały dla sesji VoIP dodatkowy parametr przesyłany w sygnalizacji, który pozwoli bezpośrednio określić lokalizację abonenta.

### **Astercity**

Istnieje możliwość realizowania połączeń z VoIP'a na telefony alarmowe. Niemniej nie ma jednego niezawodnego sposobu określenia położenia geograficznego skąd jest inicjowane połączenie.

Istnieją mapy sieci IP (każdy kraj i operator ma przypisany pewien zakres adresacji) niemniej nie ma możliwości skorzystania z tych informacji do określenia położenia geograficznego.

Wyjątkiem mogą być tu małe, osiedlowe sieci dostępu do Internetu, ale np. Neostrada oferuje dynamiczne adresy IP, co już niweluje taką możliwość.

Wydaje się, że najlepszym rozwiązaniem jest przekierowanie połączeń przychodzących na numery alarmowe do jednego, dedykowanego centrum ogólnopolskiego i dzwoniący musi określić swoją pozycję. W takim układzie można zastosować ograniczenia do wywołań tylko z danego kraju, lecz oczywiście nie gwarantuje to zabezpieczenia przed „dowcipniami”.

Osoby znające się lepiej na sieciach IP oraz serwerach są w stanie podszyć się pod dowolny adres IP i wtedy serwery i system nie rozpoznają innego kraju oryginacji połączenia.

### **Dialog.**

Nieliczni operatorzy VoIP oferują aktualnie prawidłową obsługę numerów alarmowych (112). W istniejących na rynku implementacjach zakłada się, że każdy abonent VoIP, niezależnie od swojego loginu (numeru geograficznego lub nie geograficznego) może np. poprzez interfejs WWW wybrać dowolny powiatowy numer alarmowy, z którym zostanie połączony po wybraniu numeru 112 ze swojego terminala.

Translacja numeru 112 na Numer Kierowania Alarmowego odbywa się w systemie operatora VoIP, który przekierowuje połączenie do sieci PSTN wg reguł zdefiniowanych przez abonenta. Oznacza to, że np. abonent VoIP o numerze 0227780001 (strefa warszawska), który aktualnie znajduje się w Sieradzu (nr kierunkowy 043), zostanie połączony z numerem docelowym 043-C-100-112.

### **Gabriel Grzesik.**

Umożliwia. Przez podanie numeru kierunkowego. Osoby zbierające informacje w w/w zakresie zapraszam do selektywnej lektury wiadomości na grupie alt.pl.voip

### **GTS Energis.**

Dostawcy z usług z reguły ograniczają możliwość realizacji połączeń użytkowników z numerami alarmowymi w sieci VoIP.

Głównym powodem tego ograniczenia jest brak technicznych możliwości określenia lokalizacji abonenta i baz danych o numerach geograficznych do odpowiednich służb alarmowych.

W sytuacji, gdy usługa jest dostarczona poprzez adapter VoIP, do którego jest dołączony tradycyjny telefon (np.: analogowy), przypadkowy użytkownik może nie mieć świadomości tych ograniczeniach. W sytuacji wymagających wezwania służb, brak możliwości realizacji tego typu połączeń może w typowych sytuacjach wprowadzać użytkownika w błąd.

W przypadku użytkowników usług bazujących na oprogramowaniu instalowanym na komputerze, powyższy problem ma mniejsze znaczenie gdyż użytkownik takiej usługi jest świadomy, a metoda dostępu do usługi wyraźnie dywersyfikuje usługi.

Innym problemem jest w brak technicznych możliwości określenie geograficznej lokalizacji użytkownika, w przypadkach zagrożenia wymagających szybkiego określenia jego lokalizacji.

Metodą rozwiązania tego problemu może być wprowadzenie na wzór operatorów zagranicznych określania miejsca świadczenia usługi z dokładnym podaniem adresu w umowie między dostawcą a abonentem.

Pośrednią metodą na określenie miejsca realizacji usług przez abonentów powinna być rejestracja adresów IP dołączenia hosta dla każdego wywoływanego połączenia.

Rejestracja adresów IP powinna być stosowana dla każdego rodzaju usługi realizowanej w sieci Internet z wykorzystaniem połączeń VoIP.

Użytkownik VoIP mimo ograniczeń technicznych powinien mieć zawsze możliwość realizacji połączeń na numery alarmowe bez ograniczeń. Uzasadnieniem takiego stanowiska jest przyjęcia, co zasady, zapewnienie jak najszerzego i najłatwiejszego dostępu Użytkowników do służb alarmowych w celu ratowania życia i zdrowia.

### **Internet Group.**

Problem nieokreśloności miejsca przebywania danego klienta hamuje nas przed udostępnieniem numeracji alarmowej. Rozważamy taką możliwość, zastrzegając jednak wymóg określenia przez klienta dokładnego adresu, pod jakim się znajduje. Nie wiemy czy zostanie to pozytywnie odebrane przez naszych klientów. Musielibyśmy także blokować możliwość korzystania z połączeń alarmowych tym klientom, którzy nie zdecydują się na przekazanie nam stosownych danych.

### **Junisoftex**

Na dzień dzisiejszy nie ma możliwości połączeń z numerami alarmowymi. Taka usługa będzie wprowadzona w najbliższym czasie.

Użytkownik aby zadzwonić na numer alarmowy będzie musiał określić swoją lokalizację w panelu sterowania usługą.

### **KIGeIT**

#### ***powinno być:***

możliwy jedno z dwóch scenariuszy:

1. wymagana każdorazowa rejestracja przez użytkownika aktualnej lokalizacji geograficznej
2. stworzenie numeru alarmowego w sieci IP (jednoznaczna identyfikacja geograficzna wywołania)

#### ***obecnie:***

- dostępne warianty:

- A. dostawca nie umożliwi realizacji połączeń użytkowników VoIP z numerami alarmowymi
- B. dostawca umożliwi realizację połączeń użytkowników VoIP z numerami alarmowymi poprzez każdorazowe lub okresowe określanie lokalizacji geograficznej (statyczne).

### **Dariusz Bakula (pracownik Lucent).**

Prawidłowa realizacja połączeń VoIP z numerami alarmowymi wymaga spełnienia przez sieć realizującą takie połączenia wielu warunków, w szczególności:

- Zidentyfikowania danego połączenia jako połączenia z numerem alarmowym;
- Określenia lokalizacji abonenta wywołującego (Ab. A);
- Kierowania połączenia do właściwego centrum alarmowego (powiadamiania ratunkowego) określonego na podstawie lokalizacji Ab. A;

- Umożliwienie realizacji połączenia zwrotnego do Ab.A;
- Umożliwienie priorytetowego zestawiania połączeń z numerami alarmowymi w stosunku do innych połączeń (*priority calling*);
- Umożliwienie realizacji połączeń bezpłatnych na numery alarmowe, tj. bez ponoszenia kosztów przez Ab.A lub zapewnienie możliwości refundacji tych kosztów.

Na obecnym etapie nie jest możliwe spełnienie wszystkich powyższych warunków, zwłaszcza w przypadku nomadyzmu. Istnieją intensywne prace standaryzacyjne zmierzające do rozwiązania tego problemu. Najbardziej zaawansowane są projekty realizowane w USA przez *National Emergency Numer Association* (opracowywana architektura sieci NENA i2 oraz i3), [http://www.nena9-1-1.org/VoIP\\_IP/index.htm](http://www.nena9-1-1.org/VoIP_IP/index.htm). Ponadto działania standaryzacyjne podejmowane są przez organizacje IETF, 3GPP Release 7, TISAPN.

Można w tym miejscu nadmienić, że w USA tamtejszy organ regulacyjny, FCC (*Federal Communications Commission*), w regulacji z dnia 3 czerwca 2005 wskazał na konieczność zapewnienia przez operatorów usług VoIP dostępu do numeru alarmowego 911 poprzez połączenie sieci IP z tradycyjną siecią telefoniczną PSTN, kierowanie połączeń alarmowych VoIP do tej sieci i dalszą obsługę połączenia alarmowego poprzez PSTN. W szczególności, połączenia alarmowe powinny być kierowane do lokalnego centrum alarmowego PSAP (*Public Safety Answering Point*) właściwego dla lokalizacji (fizycznego adresu) abonenta Ab. A, wskazywanego podczas rejestracji usługi. Główne problemy przy takiej realizacji połączeń alarmowych: (1) Nie jest możliwe prawidłowe kierowanie połączeń przy zmianie lokalizacji (nomadyzm nie jest obsługiwany), a ponadto (2) Operatorzy usługi VoIP zmuszeni są często – w celu realizacji zalecenia - do korzystania z sieci PSTN, która jest obsługiwana przez operatora konkurencyjnego (najczęściej operatora dominującego).

### **NASK**

Usługodawca oferuje realizację wszystkich rodzajów połączeń, także do numerów alarmowych. Lokalizacja geograficzna użytkownika jest określana na podstawie danych teleadresowych zawartych w umowie na świadczenie usług telekomunikacyjnych.

### **Net Telecom**

Tak - w usłudze Actio użytkownicy mogą korzystać z wszystkich numerów specjalnych w tym numerów alarmowych. Użytkownik wybierając numer alarmowy łączony jest z numerem zgodnym ze strefą z której posiada numer telefoniczny.

### **Onet**

Dostawcy z usług z reguły ograniczają możliwość realizacji połączeń użytkowników z numerami alarmowymi w sieci VoIP.

Głównym powodem tego ograniczenia jest brak technicznych możliwości określenia lokalizacji abonenta i baz danych o numerach geograficznych do odpowiednich służb alarmowych.

W sytuacji, gdy usługa jest dostarczona poprzez adapter VoIP, do którego jest dołączony tradycyjny telefon (np.: analogowy), przypadkowy użytkownik może nie mieć świadomości tych ograniczeniach. W sytuacji wymagających wezwania służb, brak możliwości realizacji tego typu połączeń może w typowych sytuacjach wprowadzać użytkownika w błąd.

W przypadku użytkowników usług bazujących na oprogramowaniu instalowanym na komputerze, powyższy problem ma mniejsze znaczenie gdyż użytkownik takiej usługi jest świadomy, a metoda dostępu do usługi wyraźnie zdywersyfikuje usługi.

Innym problemem jest w brak technicznych możliwości określenie geograficznej lokalizacji użytkownika, w przypadkach zagrożenia wymagających szybkiego określenia jego lokalizacji.

Metodą rozwiązania tego problemu może być wprowadzenie na wzór operatorów zagranicznych (Vonage) określania miejsca świadczenia usługi z dokładnym podaniem adresu w umowie między dostawcą a abonentem.

Pośrednią metodą na określenie miejsca realizacji usług przez abonentów powinna być rejestracja adresów IP dołączenia hosta dla każdego wywoływanego połączenia.

Metoda ta powinna być stosowana dla każdego rodzaju usługi realizowanej w sieci Internet.

### **Inotel**

TAK, INOTEL umożliwia połączenia z nr 112, numery 997, 998 i 999 są przemapowane na 112. Użytkownik podczas rejestracji wskazuje najbliższe jemu geograficznie Centrum Ratunkowe nr 112.

### **TPSA**

Większość operatorów, w szczególności posługujący się aplikacjami VoIP (tzw. Softphone) nie realizuje połączeń alarmowych (rozumianych jako możliwość wybrania numeru alarmowego, uzyskania połączenia z najbliższym miejscem przebywania centrum ratunkowym, przy zidentyfikowaniu użytkownika). Dzieje się tak z dwóch powodów:

- Braku gwarancji zasilania do wykonania takiego połączenia
- Braku możliwości określenia lokalizacji abonentów

Brak gwarancji zasilania ma związek z faktem, iż nie wszystkie urządzenia posiadają zasilanie awaryjne (bateryjne lub alternatywne łącze energetyczne). Szczególnie problematyczne jest to przy urządzeniach, które mają zezwalać na nomadyczny charakter – wymagany jest mały rozmiar i waga, komfort w transporcie. Zakładając nawet, że można byłoby wyposażać wszystkie urządzenia w takie awaryjne zasilanie, i tak operator nie ma pewności funkcjonowania tego rozwiązania, bo jest częściowo zależne od użytkownika (np. naładowanie baterii).

Brak możliwości pewnego określenia lokalizacji abonenta VoIP występuje w sieciach stacjonarnych, gdzie znany jest adres abonenta. Np. Gdy abonent wdzwaniania się do sieci VPN służby alarmowe (przy założeniu, że informacja o lokalizacji abonenta związana jest z adresem IP) otrzymają informację o lokalizacji przypisanej do adresu IP sieci VPN, a nie miejsca skąd dzwoni abonent.

Problem braku możliwości określenia lokalizacji, o ile pierwotnie zidentyfikowany w sieciach stacjonarnych, jest obecny również w sieciach radiowych, w szczególności punkt-wielopunkt. Trudno wyobrazić sobie określanie lokalizacji abonenta z dokładnością do stacji bazowej, bo w takich warunkach akcja ratunkowa wiązałaby się z poszukiwaniem abonenta.

Problemem związanym z realizowaniem połączeń alarmowych jest również ich routing. W sytuacji, gdy dla usług VoIP przydzielane są numery niezwiązane z lokalizacją abonenta routing może odbywać się jedynie na poziomie punktu styku sieci PSTN i VoIP. Odbywa się zatem z dokładnością do stref numeracyjnych obsługiwanych przez dany punkt styku. Z racji nikłej skali używania VoIP punkty styku z siecią PSTN są nieliczne. Przyjmując nawet, że znajdowałyby się w każdej strefie numeracyjnej, w danej strefie wszystkie wywołania

z numerów VoIP byłyby kierowane do jednego centrum ratunkowego, bez względu na to, czy to właśnie najbliżej niego znajduje się abonent.

TP nie umożliwia realizacji połączeń alarmowych w usłudze VoIP dla klientów indywidualnych, ze względu na to że nie jest możliwe określenie lokalizacji abonenta. Powodem jest „nomadyczna” cecha urządzenia VoIP (jakkolwiek nie jest komunikowana może być wykorzystywana przez abonentów) – możliwe jest przeniesienie urządzenia Livebox na inne łącze neostrada i dalsze korzystanie z usług VoIP. Dzieje się tak w związku z faktem, iż uprawnienia abonenta przypisane są do numeru VoIP, a ten z kolei powiązany jest z identyfikatorami Liveboxa (czyli MAC adresem i numerem seryjnym). W czasie gdy urządzenie jest przeniesione na inną linię, abonent nadal korzysta ze swojego numeru VoIP, a opłaty za połączenia naliczane są na jego konto (a nie właściciela linii DSL).

Dla klientów biznesowych, ze względu na inny charakter usługi i inne rozwiązania techniczne, TP będzie umożliwiała użytkownikowi VoIP poprawne połączenia z numerami alarmowymi, zasada działania została wypracowana oraz będzie realizowana z wykorzystaniem mechanizmu Numerów Routingowych dla służb alarmowych.

### **Skype Technologies S.A.**

Skype celowo nie oferuje dostępu do numerów alarmowych, ponieważ nie jest w stanie zagwarantować skutecznej realizacji połączenia z numerem alarmowym ani w wiarygodny sposób określić lokalizacji użytkowników Skype.

Użytkownicy są bardzo wyraźnie informowani o braku możliwości połączenia przez Skype z numerami alarmowymi. Jesteśmy przekonani, że charakterystyka produktów Skype nie pozwala użytkownikom błędnie postrzegać Skype jako usługi telefonicznej.

Skype jest aplikacją typu *peer-to-peer*, która znajduje się na komputerach użytkowników i która funkcjonuje wyłącznie przy bezpośrednim wykorzystaniu Internetu. Awaria komputera użytkownika (na poziomie sprzętowym, oprogramowania, w tym złośliwego oprogramowania), awaria lub ograniczenie przepustowości łącza internetowego, przerwa w dostawie prądu itp. są czynnikami, na które Skype nie ma wpływu. Skype nie jest zatem w stanie zagwarantować skutecznego wykonania połączenia, ponieważ awarie lub ograniczenia w działaniu (w tym przejściowe zapchanie sieci dostawców Internetu lub internetowych sieci szkieletowych, na które Skype nie ma wpływu) mogą zdarzyć się i zdarzają się w rzeczywistości. Większość użytkowników VoIP ma już za sobą tego typu awarię lub ograniczenie działania.

Skype jest zdania, że obecnie byłoby rzeczą nieodpowiedzialną zapewniać (lub twierdzić, że zapewnia) dostęp do numerów alarmowych, ponieważ dostęp ten z pewnością nie byłby ciągły, a kierowanie połączeń mogłoby spowodować, że niektóre z połączeń mogłyby być przekierowane do niewłaściwych centrów alarmowych (krajowych lub międzynarodowych).

Skype jest zdania, że w obecnych okolicznościach i w perspektywie najbliższej przyszłości organy legislacyjne, rządowe czy urzędy regulacyjne wykazałyby się brakiem rozwagi zezwalając na oferowanie dostępu do numerów alarmowych podmiotom, które nie są w stanie pod względem technicznym zapewnić bezbłędnej realizacji i kierowania połączeń. W opinii Skype, mając świadomość tego, że niektóre połączenia mogą nie zostać prawidłowo zrealizowane, oferowanie użytkownikom nieuzasadnionego poczucia bezpieczeństwa byłoby znacznie gorsze niż obecny stan rzeczy. UKE powinien natomiast pozwolić firmie Skype rzetelnie informować swoich użytkowników stwierdzając jednoznacznie, że nie oferuje

dostępu do numerów alarmowych. Zezwolenie na realizację połączeń alarmowych byłoby źródłem niemożliwych do spełnienia oczekiwań użytkowników.

### **Polkomtel**

Użytkownik VoIPa powinien się wdzwaniać na właściwą służbę alarmową w zależności od gminy, w której aktualnie się znajduje (jeżeli przebywa na terytorium RP) zgodnie z formatem Krajowego Numeru Alarmowego opublikowanego na stronie UKE. [http://www.uke.gov.pl/urtip/index.jsp?place=Lead08&news\\_cat\\_id=151&news\\_id=752&layout=3&page=text](http://www.uke.gov.pl/urtip/index.jsp?place=Lead08&news_cat_id=151&news_id=752&layout=3&page=text).

Określenie faktycznej lokalizacji użytkownika VoIP, który łączy się z sieci Internet, jest bardzo trudne, ponieważ adresy IP nie "mapują się" jednoznacznie na położenie geograficzne (np. abonent korzystający z bezprzewodowego Internetu, ma adres IP z tej samej puli niezależnie w jakim miejscu się znajduje). W związku z tym, nie jest możliwe właściwe kierowanie połączeń alarmowych dla użytkowników nomadycznych VoIP i właściwe wypełnienie obowiązków wynikających z zapisów art. 78 i 129 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne. W szczególności nie jest możliwe prawidłowe kierowanie ruchu zgodnie z dokumentem przygotowanym przez Ministerstwo Spraw Wewnętrznych i Administracji gdzie dla wszystkich powiatów na terenie RP określono wykaz lokalizacji służb przewidzianych do obsługi wywołań na numer „112”. Po przygotowaniu przez stosowne Ministerstwa wykazów dla pozostałych numerów alarmowych (zgodnie z ich wykazem w planie numeracji krajowej) ich stosowanie również nie będzie wykonalne dla nomadycznych użytkowników VoIP.

### **Fone**

W praktyce lokalizację geograficzną musi określić sam użytkownik VoIP. W odpowiednim profilu swojego konta wskazuje on strefę numeracyjną, do której powinny być kierowane wszystkie wywołania alarmowe. Z uwagi na to, że użytkownik VoIP może korzystać ze swojego konta praktycznie w dowolnym miejscu kuli ziemskiej nie ma technicznych możliwości zautomatyzowania tego procesu i zarządzania tego typu połączeniami bez potrzeby angażowania użytkownika. Drugą metodą jest potrzeba poprzedzenia przez użytkownika numeru alarmowego numerem strefy, w której się w danej chwili znajduje. Praktycznie brak jest uregulowań technicznych, które pozwalały by ten problem rozwiązać w sposób systemowy.

### **Wimax Telecom AG**

To zależy od kilku czynników - przede wszystkim od tego w jak dalekim stopniu usługodawca VoIP ma wpływ i zarządza siecią dostępową oraz jakiego typu jest to sieć. Jeżeli usługodawca VoIP posiada sieć dostępu typu stacjonarnego wówczas realizacja takich połączeń odbywać się może jak w sieci PSTN, w przypadku sieci umożliwiającej realizację funkcjonalności przenośności/nomadyczności usług - połączenia połączeń z numerami alarmowymi realizowane są podobnie jak w przypadku sieci mobilnych. Jeżeli usługodawca VoIP nie dysponuje własną siecią dostępową identyfikacja danej lokalizacji geograficznej użytkownika może się odbywać na podstawie skomplikowanego mechanizmu analizy adresu IP, z którego pochodzi ruch jednak nie daje to wystarczającej i w pełni wiarygodnej informacji o jego lokalizacji.