



República Federativa do Brasil
Ministério da Economia
Instituto Nacional da Propriedade Industrial

(11) PI 0722242-4 B1



(22) Data do Depósito: 30/11/2007

(45) Data de Concessão: 24/12/2019

(54) Título: MÉTODO E SISTEMA PARA PROVER SERVIÇOS DE TELECOMUNICAÇÃO

(51) Int.Cl.: H04L 29/12; H04L 29/06; H04L 29/08; H04M 3/493; H04M 7/12.

(52) CPC: H04L 29/12066; H04L 29/1216; H04L 29/12594; H04L 61/1511; H04L 61/157; (...).

(73) Titular(es): TELECOM ITALIA S.P.A..

(72) Inventor(es): PAOLO DE LUTII; FRANCESCO SILLETTA.

(86) Pedido PCT: PCT EP2007063081 de 30/11/2007

(87) Publicação PCT: WO 2009/068111 de 04/06/2009

(85) Data do Início da Fase Nacional: 31/05/2010

(57) Resumo: MÉTODO E SISTEMA PARA PROVER SERVIÇOS DE TELECOMUNICAÇÃO Um método de prover serviços de telecomunicação compreendendo: gerar uma informação de contato fictícia univocamente associada com um número de telefone atribuído a um assinante; armazenar a informação de contato fictícia em uma base de dados; em resposta a uma solicitação recebida de um solicitante de uma informação de contato correspondendo a dito número de telefone e adaptada para permitir contato através da Internet com o cessionário do assinante de dito número de telefone, ter a base de dados provendo dita informação de contato fictícia; condicionar uma resolução da informação de contato fictícia para o aprovisionamento da informação de contato para a satisfação de pelo menos uma regra de segurança adaptada para avaliar propriedades de pelo menos um dentre dito solicitante e dita solicitação, e no caso da solicitação do solicitante satisfazer dita pelo menos uma regra de segurança, resolver a informação de contato fictícia e prover ao solicitante a informação de contato.

MÉTODO E SISTEMA PARA PROVER SERVIÇOS DE TELECOMUNICAÇÃO

Conhecimento da Invenção

Campo da Invenção

[001] A presente invenção geralmente se refere aos sistemas de comunicação. Em particular, a presente invenção pertence à melhoria da segurança de ENUM (Mapeamento de Número Telefônico).

Descrição da arte relacionada

[002] Hoje em dia, redes de telefone está começando a se mover da antiga Rede de Telefonia Comutada Pública (PSTN) em direção às redes de telefone com base em IP (Protocolo de Internet).

[003] A mudança de plataforma tecnológica gera novos desafios. Um deles é por exemplo oferecer serviços baseados na Internet, com Voz sobre Protocolo de Internet (VoIP), serviços de telefonia, em uma maneira que, a partir de uma perspectiva de aceitação do cliente, não implicam mudanças para o modo que chamadas telefônicas são tradicionalmente feitas; de fato, a maneira que telefones são normalmente usados tornou-se tão trivial que mudanças não seriam bem vinda para as pessoas.

[004] Por conseguinte, técnicas são necessária para localizar telefones da parte chamada na Internet usando simplesmente o número de telefone tradicional entrado por um usuário quando colocando uma chamada, independente do fato que será tratado com uma chamada de VoIP.

[005] Uma abordagem para endereçar esses problemas é representado através de ENUM.

[006] ENUM é o nome de um protocolo que permite a convergência entre o padrão internacional E.164 para numeração de telefone, sancionado pela International Telecommunication Union (ITU), e redes baseadas em IP como a Internet. ENUM alcança esta convergência usando uma técnica baseada no Sistema de Nome de Domínio (DNS) da Internet. Como

conhecido, o DNS é um componente essencial da Internet contemporânea, que associa vários tipos de informação com os assim chamados "nomes de domínio", e serve como o "livro de telefone" para a Internet, traduzindo nomes hospedeiros de computador legíveis para o ser humano, e.g. endereços de sítios da Web, em correspondentes endereços de IP que os equipamentos de rede necessitam para entregar informação. O DNS permite aos computadores de usuários encontrar servidores de sítio da web através da Internet usando endereços de sítio de web fáceis de lembrar em vez de endereços de Internet numéricos e complicados.

[007] Os detalhes de ENUM são descritos no documento RFC 3761 da Engineering Task Force (IETF), que é o documento de protocolo aprovado da IETF discutindo o uso de DNS para o armazenamento de número de telefones e os serviços disponíveis conectados a um número de telefone.

[008] Usar números de telefones condizentes com E. 164 e o DNS para implementar o ENUM é apropriado, porque por um lado E.164 é um padrão para números de telefones que é aceito e usado em todo o mundo, e, no outro lado, o DNS inclui a habilidade de correlacionar informação alfanumérico com endereços de IP. Números de E.164, como nomes de sítio de web, permanecem relativamente estáticos no tempo, requerendo atualizações relativamente não frequentes (que são limitados aos casos onde por exemplo assinantes de serviço individual mudam seu número de telefone).

[009] Um número de telefone condizente com o E.164 tipicamente inclui um código de país, um código de área ou cidade, e um número de telefone. O ITU atribui código de país unívocos para nações soberanas, e.g., os Estados Unidos da América têm o código de país "1", Itália tem o código de país "39". Códigos de área ou cidade e número de telefones são administrados pelas nações soberanas através de agências reguladoras de telecomunicações.

[0010] Por exemplo, um número de E. 164 totalmente qualificado

para o número de telefone 555-1234 hipotético em Washington, D.C. (código de área 202) nos Estados Unidos seria +1-202-555-1234. O símbolo "+" indica que o número é um número de E. 164 totalmente qualificado.

[0011] ENUM endereça os desafios de endereços discutidos acima considerando VoIP e outros serviços, enquanto fornecendo clientes de telefone com vários benefícios. ENUM permite operadores de rede de telecomunicações convergentes, móveis, com fio, ISPs (Provedores de Serviço de Internet), OLOs (Outros Operadores Licenciados), operadores de telefonia fixa ou móvel para oferecer uma ampla gama de serviços baseados em IP para se comunicar com uma outra pessoa quando um usuário conhece somente um número de telefone ou tem somente acesso a um teclado de telefone simples. O usuário pode, por exemplo, ter acesso a esses serviços baseados em IP e recursos usando telefones habilitados à Internet (VoIP), que são por exemplo telefones simples conectados à portões de passagem da Internet ou servidores de preparação, e / ou outro dispositivos acoplados à Internet onde a capacidades de entrada são limitadas para dígitos numéricos. Por exemplo, usuários, se inscrevendo a um serviço específico oferecido por, e.g., um ISP ou operador de telecomunicação, pode especificar no sistema de ENUM (particularmente, em uma implementação dele chamado "ENUM Global", como discutido no descrito a seguir) preferências para receber comunicações entrantes; isto concede ao usuário grande controle sobre as comunicações. Por exemplo, um usuário pode configurar preferências de correio de voz ou pode entrar um número de telefone de destinação em um serviço de passar chamada.

[0012] Há muitas aplicações potenciais de ENUM. Contudo, as aplicações principais para ENUM têm até agora se centrado em duas áreas: VoIP e protocolo de voz para correio de Internet (VPIM). Um objetivo da indústria de VoIP é fazer uma chamada telefônica através da Internet tão fácil de fazer como um plano de chamada telefônica da antiga PSTN e com o

mesmo nível de qualidade. Se um cliente de telefone médio foi fazer chamada telefônica usando, e.g., um telefone habilitado para Internet para um outro telefone habilitado para Internet, todos os passos entre eles devem permanecer transparente para o usuário. Para a parte de quem chama e a parte chamada, esta chamada telefônica deve parecer a mesma que uma chamada feita através da PSTN.

[0013] Já que ENUM pode oferecer muitos diferentes tipos de serviços, ENUM tem uma ampla gama de clientes potenciais, incluindo assinantes de telefone residencial individual, corporações, agências do governo, militar, e hospedeiros de outros usuários não individuais. Uma lista dos serviços que um assinante usuário tem direito é armazenada no banco de dados do ENUM e pode ser acessada em resposta a entrada de um código através do teclado de telefone. Quando assinantes desejam usar um serviço específico, eles podem identificar o serviço de ENUM que eles desejam usar, e.g., entrando o código associado no teclado de telefone. Essencialmente, o protocolo ENUM como definido no documento RFC 3761 do IETF trabalha na seguinte maneira. Uma vez que um número de telefone é entrado, é traduzido em um nome de domínio; a tradução do número de telefone entrado em um nome de domínio envolve primeiro traduzir o número entrado em um número de E. 164 totalmente qualificado, adicionando a cidade - ou área - e código de país; então, a ordem dos dígitos do número E. 164 totalmente qualificado é reversa, e pontos são colocados entre cada dígito; o domínio "e164.arpa" é finalmente anexado ao final.

[0014] ENUM então emite uma indagação de DNS no nome de domínio resultante. Uma vez que o servidor de nome de domínio oficial é encontrado, ENUM recupera os recursos relevantes de NAPTR (Naming Authority PoinTeR) gravados a partir de um banco de dados de ENUM, e efetua de acordo com os serviços registrados do usuário para aquele número de telefone.

[0015] ENUM pode ter várias implementações; duas possíveis implementações de ENUM são referidos como "ENUM Público " ou "ENUM Global" e "ENUM de Transporte" ou "ENUM de infra-estrutura".

[0016] ENUM Global é um banco de dados como diretoria pública e global, com capacidades opção do assinante e delegação no nível de código de país no domínio e164.arpa. ENUM Global fornece informação de encaminhamento (endereços de IP relacionados aos números de E. 164 gerenciados por um dado operador) para outros operadores e provedores de serviço. No ENUM Global, um usuário final é habilitado a fornecendo e lendo a informação de encaminhamento. Em particular, o ENUM Global define o domínio "e164.arpa" que pode ser usado como as bases para armazenar números de E.164 no DNS (de acordo com o documento de RFC 3761 do IETF). A administração de ENUM Global é uma questão nacional ou regional, e é gerenciado por agências reguladoras de telecomunicação dos diferentes países. Sendo publico e aberto para todos, o ENUM Global pode ser afetado problemas de spam e outras formas de comportamento fraudulento, como discutido mais tarde.

[0017] Ao contrário, o ENUM de infra-estrutura é uma implementação de ENUM que pode ser usado somente dentro de um número restrito de operadores confiáveis selecionados. Um ENUM de infra-estrutura não é acessível para usuários finais, é pretendido para uso interno somente dentro do círculo de operadores confiáveis. Isto assegura segurança de serviço e privacidade de assinante. Infra-estrutura ENUM facilita achar usuários e seus serviços relacionados para propósitos de encaminhamento dentro das redes de operador, para encontrar os elementos de fronteira conectados a outros operadores ou portões de passagem para a rede de PSTN, para esconder os usuários e a infra-estrutura atrás dos elementos de fronteira e para dar acesso aos operadores externos para somente esses elementos de fronteira. Um ENUM de infra-estrutura é pretendido para ser usado pelos operadores

para atingir os elementos de fronteira de redes confiáveis; não é pretendida para ser usada diretamente por assinantes ou usuários finais de redes não confiáveis. Por esta razão, o espaço de nome de domínio "e164.arpa" não é apropriado para os serviços do ENUM de infra-estrutura, e nomes de domínio privado devem ser adotados.

[0018] Apesar de suas vantagens indubitáveis, os riscos potenciais de ENUM já foram reconhecidos. Por exemplo, no documento TS 102 051 do ETSI com o título de "*ENUM Administration in Europe*" é previsto que ENUM fornece um risco significativo para uso sem escrúpulos da informação contida em seus registros de NAPTR. Qualquer tentativa de comunicação para um número de E.164 para o qual registros de ENUM existem, vai permitir a uma aplicação de cliente de ENUM de solicitação ter acesso a informação sobre todos os identificadores de comunicação específico de serviço (número de telefones, endereços de correio eletrônico, endereços de tratamento de mensagem instantânea, etc.) contida no registro de NAPTR de um certo assinante. Esta informação poderia ser usada para determinar a identidade da pessoa associada com um número de E. 164 entrado aleatoriamente (e.g. olhando no nome em seu endereço de correio eletrônico, ou olhando em qualquer outra entrada em seu registro de NAPTR que dá uma pista do nome do assinante). Este abuso potencial de ENUM poderia ser usado para auxiliar "furtos de identidade" ou para ajudar organizações que desejam construir listas de identidades para a propagação de comunicações de "spam" através de uma ampla gama de diferentes serviços de comunicações (e.g. pessoa que nos dias de hoje contata outra pessoa trabalhando através de listas de número de telefones poderiam, abusando do ENUM, também gerar listas de endereços de correio eletrônico e identificadores de tratamento de mensagem instantânea associados com aqueles números). Informação contida nos registros de NAPTR pode revelar os tipos de aplicação e serviços de comunicações que são usado por um usuário final do ENUM, e

potencialmente também os provedores dessas aplicações e serviços. Esta informação poderia ser usada pelas terceiras partes para propósitos comerciais, por exemplo, para fazer ofertas para o usuário final do ENUM considerando aplicações e serviços que competem com aqueles usados pelo assinante, ou para desenvolver e vender perfis de mercado mostrando as aplicações e serviços de comunicações usados pelos usuários finais do ENUM.

[0019] ENUM, como qualquer sistema que mapeia múltiplos serviços para um identificador único (o número de E. 164 do assinante), pode ser vulneráveis à ataques de Negação de Serviço (DoS) de múltiplos serviços. Por exemplo, qualquer um montando um "ataque de inundação" sobre os registros de NAPTR de DNS poderia prevenir a recuperação de quaisquer endereços de comunicação a partir do registro de NAPTR atacado. Tal um ataque tornaria impossível para alguém indagando o registro de NAPTR, pegar uma resposta a sua indagação. O resultado de tal um ataque poderia ser que ninguém seria capaz de se comunicar com aquele usuário final de ENUM usando quaisquer dos serviços de comunicação possíveis associados com ele, assim sendo completamente desabilitando as comunicações entrantes do assinante (possivelmente, com a única exceção de chamadas de telefone sobre a PSTN).

[0020] Riscos adicionais podem surgir de implementações privadas de ENUM que sofrem de controles e supervisão pobres.

[0021] Para os aspectos de segurança e integridade, duas das ameaças principais são passar despercebido e sequestro.

[0022] Passar despercebido é onde uma entidade representa a si próprio como alguém ou alguma coisa que não é usual, para alcançar uma vantagem comercial ou para propósitos criminais. No contexto de ENUM, passar despercebido poderia ocorrer quando uma entidade aprovisiona no DNS o número de E.164 de alguém mais (uma outra pessoa ou empresa),

inserindo seus próprios detalhes no registro de NAPTR correspondendo ao outro numero de pessoa ou empresa. Passar despercebido é considerado como prejudicial porque mina a confiança que indivíduos e organizações devem ter umas comunicações usando capacidades de ENUM.

[0023] Sequestro é onde um provedor de aplicações e serviços de comunicações é inserido em um caminho de comunicação sem uma permissão do usuário final. No contexto de ENUM, sequestro poderia ocorrer quando um provedor de aplicações ou serviços de comunicações arruma números de E. 164 dos usuários finais a serem provisionados no DNS sem o seu consentimento e quando comunicações usando capacidades de ENUM para esses números são re-direcionados através de uma rede, aplicação ou serviço que os usuários finais não escolheram.

[0024] Sequestro é considerado como prejudicial porque ele poderia permitir a um provedor de comunicações, aplicações ou serviços coletar trânsito ou outras receitas indevidamente, e contradizer uma decisão do usuário final considerando o transporte de suas comunicações de entrada.

[0025] Devido à possibilidade de configurar vários, possivelmente sistemas de ENUM privados competindo, distintos do e164.arpa ENUM (como por exemplo e164.com, e164.org ou o similar), problemas de consistência dentre os dados armazenados nos registros de NAPTR dos diferentes bancos de dados do sistema de ENUM existem.

[0026] Ambos esses pontos de risco para a necessidade de mecanismos adequados para assegurar que a solicitação para provisionar um número no DNS que se origina a partir do legítimo cessionário do assinante do número.

[0027] Um possível método poderia envolver autenticação através de uma entidade de validação. Qualquer que seja a solução desenvolvida, qualquer método efetivo é provável de envolver algum grau de validação. Enquanto este método supera o problema de "passar despercebido, ele pode

não completamente solucionar o problema de "sequestro", já que a entidade de validação poderia tentar sequestrar o número. Questões similares ocorrem no caso de alteração e rescisão de um número. O desafio é assegurar que os processos encontram requisitos de modo a manter consistência entre nomes de domínio de ENUM e números de E.164, enquanto não impondo uma explosão administrativa excessiva em quaisquer entidades envolvidas.

[0028] Riscos adicionais surgem devido ao potencial que modelos de administração ruins poderiam permitir as entidades fazer mau uso de posições de poder de mercado significativo. O banco de dados de ENUM tem uma estrutura hierarquia de três níveis: o nível hierárquico mais alto é chamado "Registro de Camada 0" ou, simplesmente, "Camada 0", e é alcançável por meio de um nome de DNS de domínio de nível alto (TLD) (como "e164.arpa"); o nível hierárquico abaixo da Camada 0 é chamada "Registro de Camada 1" ou "Camada 1"; várias Camadas 1 existem, cada um associado com um respectivo código de país; o nível hierárquico inferior é chamado "Registro de Camada 2" ou "Camada 2", e corresponde a um respectivo número de telefone. Um mau uso de posição de poder de mercado principalmente aumenta em torno da Camada 1. Normalmente, o gerenciamento da Camada 1 está sob a responsabilidade do país para o qual o código de país da Camada 1 corresponde. Contudo, deve uma responsabilidade delegada do país para gerenciar sua Camada 1 sem controles adequados, o gerenciador da Camada 1 apontado poderia potencialmente fazer mau uso de sua posição única, por exemplo cobrando uma taxa desproporcional para entrar números de E.164 em seus bancos de dados; no outro lado, apontando dois ou mais itens de gerenciar a Camada 1 de um certo país conduz a muitas complicações adicionais, incluindo requisitos de interfuncionamento difícil e complexo.

[0029] Também é possível que controle do domínio no qual o ENUM está hospedado por gerenciadores de um único país ou região fornece aquele

país ou região com influência indevida sobre as operações de redes de telefonia convergidas na Internet. De forma similar, se a localização de servidores de DNS na qual o mecanismo de ENUM depende, se encontra predominantemente em um único país ou região, isto pode resultar em comunicações dentro da Europa ou entre a Europa e outras regiões sendo indevidamente dependente das infra-estruturas fora da Europa.

[0030] Há também a possibilidade de se registrar blocos inteiros de números no ENUM. Por esta razão, é importante assegurar que aqueles números estão sob o controle do proprietário com a possibilidade de mudar a política sobre quando a resolução deve ser feita e por quem está autorizado ou não.

[0031] US 6,968,050 divulga um sistema que segurança de ENUM para autenticar e autorizar pessoas a registrar informação correspondendo a um número de telefone no contexto de métodos e aparelhos baseados em AIN (Advanced Intelligent Network), e.g., em um banco de dados do ENUM. Os métodos podem ser usados para autenticar um parte procurando registrar a informação de número de telefone relacionada com ENUM. Um acionador é configurado em uma linha de registro de ENUM. Chamadas para a linha de registro de ENUM ativa o acionador forçando informação de LIDB (Banco de dados de Informação de Linha) correspondendo ao número da parte de quem chama a ser recuperado. A informação recuperada, e.g., nome, endereço e / ou número de telefone, é fornecido a um serviço de registro de ENUM que retorna uma senha a ser usada quando atualizando ou provendo registro de ENUM correspondendo ao número de telefone a partir do qual a chamada de registro é colocada em algum tempo futuro, e.g., através da Internet. Senhas de ENUM atribuídas podem ser obtidas quando esquecidas, colocando uma chamada para o serviço de registro a partir do número de telefone associado ou registrado.

[0032] O documento RFC 4033 do IETF com o título de "*DNS*

Security Introduction e Requirements" estabelece uma extensão para o DNS que fornece integridade e autenticação de dados para solucionadores e aplicações de conhecimento de segurança através do uso de assinaturas digitais criptográficas. Essas assinaturas digitais estão incluídas em zonas seguras com registros de recursos. Segurança também pode ser fornecida através de servidores de DNS de conhecimento de não segurança em alguns casos. As extensões fornecem para o armazenamento de chaves públicas autenticadas no DNS. Este depósito de chaves pode suportar serviços de distribuição de chave pública assim como segurança de DNS. As chaves armazenadas permitem aos solucionadores de conhecimento de segurança instruírem-se da chave de autenticação das zonas em adição para aqueles aos quais eles são inicialmente configurados. Chaves associadas com nomes de DNS podem ser recuperadas para suportar outros protocolos. Em adição, as extensões de segurança fornecem a autenticação opcional das transações e solicitações do protocolo de DNS.

[0033] O documento por G. Kambourakis et al com o título de "*Security e privacy issues towards ENUM protocol*", publicado nos procedimentos do 2005 IEEE International Symposium sobre processamento de sinal e Tecnologia de Informação mantido no 18-21 de Dezembro de 2005 em Samos (Greece) (páginas 478- 483), descreve as questões de segurança relacionando o uso da tecnologia de ENUM tecnologia e fornece uma lista de potenciais para assegurar aquelas questões.

[0034] O documento por Richard Shockey Neustar *et al.* "*Privacy and Security Considerations in ENUM*", *draft-ietf-enum-privacy-security-01.txt_IETF_Standard-Working-Draft_IETF_CH._vol._Enum._no._1.1_July_2003*, propõe o uso de "pseudônimos" para o SIP URI em substituição à indicação pública dos nomes reais (nome e sobrenome) de um dono de telefone.

[0035] O documento US2004/230792 revela métodos e sistemas para criptografia de dados transparentes e descriptografia.

Sumário da invenção

[0036] A partir da discussão acima, parece que o sistema de ENUM, como correntemente implementado, pode ser exposto à ameaças de segurança potencial. De fato o sistema de ENUM, quando a informação é globalmente disponível ou não propriamente controlada, pode ser submetida à difusão em massa (que gera comunicação não solicitada reusando a informação sobre a habilidade de alcance do alvo do ataque), à hackers (que usa a informação contida no sistema de ENUM para realizar ataque de VoIP específico) ou à uso incorreto por operadores não confiáveis (que podem por exemplo usar a informação para conduzir análises de marketing sem qualquer controle forma de onda proprietário da informação). A informação relacionada ao encaminhamento e habilidade de alcance dos clientes / serviços que foram protegidos por uma rede de PSTN / ISDN parece ser perdida ou não facilmente gerenciada com uma perda de potencial de negócios para operador e segurança para cliente.

[0037] Muitos dos problemas derivam do fato que o ENUM é um serviço de rede de pacote (i.e., baseado na Internet e o conjunto de protocolo TCP / IP), baseado no protocolo e infra-estrutura de DNS, que foi atribuído sem qualquer necessidade de controle da informação processada.

[0038] Em relação à solução divulgada no US 6,968,050, o Requerente acredita que ela tem os seguintes inconvenientes:

- é orientada para autenticar e autorizar a modificação da informação armazenada no sistema de ENUM (i.e. a associação entre o número de telefone e o URI - Identificador de Recursos Uniforme);
- ela é vinculada ao antigo sistema de PSTN e IN (Rede Inteligente) sistema, e é baseada no mecanismo de autenticação de PSTN CLI (Identidade da Linha que Chama, o número de telefone do chamador) de PSTN.

[0039] A solução divulgada em US 6,968,050 propõe um mecanismo

de auto provisionamento de informação para um servidor de ENUM, iniciando diretamente a partir dos dados gerados pelo assinante de PSTN que deseja ser alcançável pelas chamadas de VoIP. A solução não é adequada para proteger a informação já publicada no sistema de ENUM, e não endereça os vários problemas surgindo da Internet e as conexões de redes de pacote.

[0040] Considerando o documento RFC 4033 da IETF, o Requerente acredita que a solução de DNSsec tem os seguintes inconvenientes:

- é focada na integridade e autenticidade dos dados contidos no banco de dados de modo a confrontar algum ataque específico (i.e., envenenamento de DNS);
- não pode ser usada / adaptada para proteger a privacidade dos dados de usuário e a mudança da confidencialidade da informação dentro de comunicações de ENUM;
- quando ENUM é baseado no mecanismo de DNSsec, ele ainda não protege o negócio do operador (por exemplo, alguma informação protegida, uma vez disponível no sistema de ENUM, é também disponível para outras partes que não podem ser controlados pelo proprietário).

[0041] Por outro lado, o documento por G. Kambourakis et al fornece uma visão geral útil para a identificação das deficiências da infra-estrutura de ENUM, mas não fornece qualquer solução concreta para questões identificadas além do DNSec.

[0042] O Requerente abordou o problema de fazer serviços de ENUM mais seguros e capazes de garantir a privacidade dos usuários.

[0043] O Requerente achou que a solução para este problema pode ser obtida escondendo a informação de contato que está normalmente no sistema de banco de dados de ENUM (i.e., o URI de SIP) usando uma informação de contato de usuário fictícia, que é adaptada para ser armazenada em um banco de dados de ENUM mas por si só não pode ser usada para contatar o usuário, e adicionar uma plataforma de gerenciamento de política de segurança para o

sistema de ENUM de modo a condicionar a resolução da informação de contato fictícia, revelar a informação de contato do usuário confiável, a satisfação das regras pré-determinadas.

[0044] Um aspecto da presente invenção se refere à um método para prover serviços de telecomunicações, compreendendo:

- gerar uma informação de contato fictícia, de modo unívoco, associada com um número de telefone atribuído a um assinante;
- armazenar a informação de contato fictícia em um banco de dados;
- responsivo a uma solicitação, recebida de um solicitante, de uma informação de contato correspondendo ao número de telefone mencionado e adaptada para permitir contato através da Internet o assinante cessionário do número de telefone mencionado, tendo o banco de dados fornecendo a informação de contacto fictícia mencionada;
- condicionar uma resolução da informação de contato fictícia para o aprovisionamento da informação de contato para a satisfação de pelo menos, um regra de segurança adaptada para avaliar propriedades de pelo menos, um dentre o solicitante e a solicitação mencionada, e
- no caso que a solicitação a partir do solicitante satisfaz a pelo menos mencionada, uma regra de segurança, resolvendo a informação de contato fictícia e fornecendo ao solicitante a informação de contato.

[0045] Em particular, o banco de dados mencionado pode ser um banco de dados de ENUM.

[0046] A informação de contato mencionada pode incluir um URI de SIP, de modo unívoco, identificando o assinante mencionado.

[0047] A informação de contacto fictícia mencionada pode incluir um URI fictício, de modo unívoco, associado com o URI de SIP do assinante mencionado. Em particular, o URI fictício pode incluir uma informação gerada aleatoriamente. Mesmo mais particularmente, o URI fictício pode

incluir um nome de domínio de modo unívoco identificando um sistema de resolução adaptado para resolver a informação de contato fictícia condicionada para a satisfação da pelo menos, uma regra de segurança.

[0048] A pelo menos mencionada, uma regra de segurança pode definir um ou mais dentre: operadores de rede de telefonia com a condição para resolver a informação de contato fictícia, solicitantes com a condição de resolver a informação de contato fictícia, tipos de serviços de conectividade que o solicitante tem condição de explorar contatar através da Internet o cessionário do assinante do número de telefone, indicações sobre data e horas quando solicitantes são permitidos contatar o cessionário do assinante do número de telefone mencionado.

[0049] O método pode ainda compreender possibilitar ou cessionário do assinante do número de telefone ou um operador de telefonia para o qual o assinante se inscreveu, define a pelo menos mencionada, uma regra de segurança.

[0050] A geração mencionada de uma informação de contato fictícia, de modo unívoco, associada com o número de telefone atribuído para o assinante pode preferencialmente incluir gerar uma nova informação fictícia após a informação de contato fictícia resolvida mencionada.

[0051] Um outro aspecto da presente invenção se refere a um sistema para prover serviços de telecomunicações, compreendendo:

- um gerador adaptado para gerar informação de contato fictícia, de modo unívoco, associada com um número de telefone atribuído a um assinante, e para forçar a informação de contato fictícia a ser armazenada em um banco de dados como a informação de contato do assinante mencionado;

- um aplicador de regras de política de segurança adaptada para:

- receber de um solicitante, uma solicitação de resolução da

informação de contacto fictícia mencionada para obter a informação de contato correspondendo ao número de telefone mencionado, a informação de contato mencionada sendo adaptada para permitir o contato através da Internet de um assinante tendo o número de telefone mencionado; e para

- condicionar a resolução da informação de contato fictícia e o aprovisionamento para o solicitante da informação de contato para pelo menos, uma regra de segurança adaptada para avaliar propriedades de pelo menos um dentre o solicitante mencionado e a solicitação mencionada.

[0052] O banco de dados pode em particular ser um banco de dados de ENUM.

[0053] A informação de contato mencionada pode incluir um URI de SIP, de modo unívoco, identificando o assinante mencionado.

[0054] A informação de contacto fictícia mencionada pode incluir um URI fictício, de modo unívoco, associado com o URI de SIP do assinante mencionado. Em particular, o URI fictício pode incluir informação gerada aleatoriamente. Mesmo mais particularmente, o URI fictício pode incluir um nome de domínio, de modo unívoco, identificando o aplicador de regras de política de segurança.

[0055] A pelo menos mencionada, uma regra de segurança pode definir um ou mais dentre: operadores de rede de telefonia com a condição para resolver a informação de contato fictícia, solicitantes com a condição de resolver a informação de contato fictícia, tipos de serviços de conectividade que o solicitante tem condição de explorar contatar através da Internet o cessionário do assinante do número de telefone, indicações sobre data e horas quando solicitantes são permitidos contatar o cessionário do assinante do número de telefone mencionado.

[0056] A pelo menos mencionada, uma regra de segurança pode ser na linguagem XML.

[0057] O sistema pode adicionalmente compreender um gerenciador

de regra de segurança adaptado para permitir ou cessionário do assinante do número de telefone ou um operador de telefonia para o qual o assinante se subscreveu, define a pelo menos mencionada, uma regra de segurança.

[0058] Preferencialmente, uma nova informação de contato fictícia, de modo unívoco, associada com o número de telefone atribuído para o assinante, pode ser gerada após a resolução da informação de contato fictícia.

Descrição Breve dos Desenhos

[0059] As características e vantagens da presente invenção serão melhor entendido lendo a seguinte descrição detalhada de algumas modalidades dele, fornecida meramente através de exemplos não limitativos, descrição que será realizada fazendo referência aos desenhos anexos, onde:

Figura 1, de forma esquemática, mostra um cenário de aplicação de uma modalidade da presente invenção;

Figura 2 descreve, ainda, de forma esquemática, mas em maiores detalhes, uma plataforma de segurança para assegurar serviços de ENUM, de acordo com uma modalidade da presente invenção;

Figura 3 é um fluxograma esquemático de uma fase de subscrição de um número de telefone para a plataforma de segurança, incluindo uma fase de definição de política de segurança, de acordo com uma modalidade da presente invenção;

Figuras 4A e 4B mostram um fluxograma esquemático de uma fase de imposição da política de segurança, de acordo com uma modalidade da presente invenção;

Figura 5, de forma esquemática, mostra um outro cenário de aplicação de uma modalidade da presente invenção; e

Figuras 6A e 6B mostram um fluxograma esquemático de uma fase de imposição de política de segurança, de acordo com uma outra modalidade da presente invenção.

Descrição Detalhada das Modalidades da invenção

[0060] Referindo à Figura 1, um cenário de aplicação de uma modalidade da presente invenção é, de forma esquemática, mostrado.

[0061] No desenho, referência numeral de referência 100 denota a rede de um primeiro genérico operador de telefonia A ("Rede A", como indicado no desenho); o operador de telefonia A é por exemplo um dos operadores de telefonia fornecendo serviços de telefonia em um certo país do mundo, e.g. Itália.

[0062] O operador de telefonia A tem respectivos assinantes, um genérico um dos quais é denotado com o numeral de referência numeral 105. o assinante genérico do operador de telefonia A atribui a ele um respectivo número de telefone.

[0063] Numeral de referência **110** denota a rede de um outro genérico segundo operador de telefonia B ("Rede B", como indicado no desenho); o operador de telefonia B é, no exemplo aqui considerado, um dos operadores de telefonia fornecendo serviços de telefonia em um determinado país do mundo, diferente do país do operador de telefonia A, e.g. os Estados Unidos da América. O país de numeral de referência **115** denota um assinante genérico do operador de telefonia B; o assinante **115** atribuiu a ele um respectivo número de telefone, por exemplo o número de telefone hipotético 202-555-1234, que identifica um assinante tendo o número de telefone 555-1234 na área de Washington, D. C. (código de área 202). Isto é assinalado que a presente invenção também se aplica aos casos em que dois operadores de telefonia A e B operam em um mesmo país, ou até mesmo coincidem, é também assinalado que a presente invenção não é limitada ao caso de dois operadores de telefonia, e se aplica independente do número de operadores de telefonia.

[0064] Numeral de referência **120** no desenho denota aparelhos de rede núcleo do operador de telefonia A, incluindo, por exemplo, centrais de

comutação e aparelhos de servidor de chamada; de forma similar, o numeral de referência **125** denota aparelhos de rede núcleo do operador de telefonia B.

[0065] As redes **100** e **110** dos operadores de telefonia A e B são conectados à Internet 130.

[0066] Os aparelhos de rede núcleo **120** do operador de telefonia A implementam uma funcionalidade de cliente de ENUM **135** adaptada para a interface de rede **100** do operador de telefonia A para o sistema de ENUM.

[0067] O sistema de ENUM compreende uma estrutura de hierárquica de bancos de dados, também referidos como a "árvore dourada", que compreende um banco de dados de ENUM **140** de nível alto, referidos como Camada 0, localizado no topo da estrutura hierárquica, vários bancos de dados localizados em um primeiro sub-nível abaixo da Camada 0, referidas como Camada 1, como os dois bancos de dados **145-1** e **145-2** mostrado no desenho, e, abaixo de cada bancos de dados Camada 1, vários bancos de dados de nível inferior referidos como Camada 2, como os dois bancos de dados **150-1** e **150-2** mostrados no desenho.

[0068] O banco de dados de Camada 0 **140** é atribuído e é alcançável por meio de um nome de domínio de ENUM de nível alto, como "e164.arpa" de acordo com as prescrições do documento RFC 3761 do IETF, e armazena endereços de servidores da Internet hospedando os bancos de dados do Camada 1. Cada um dos bancos de dados de Camada 1 é associado com um respectivo código de país, i.e. com um respectivo país do mundo, no exemplo aqui considerado, o banco de dados de Camada 1 **145-1** é associado com o código de país "+39", correspondendo à Itália, e o banco de dados de Camada 1 **145-2** é associada com o código de país "+1", correspondendo aos Estados Unidos de América. Cada banco de dados de Camada 1 armazena endereços de Internet dos servidores de Internet hospedando os bancos de dados de Camada 2 de número de telefones do respectivo país. Cada banco de dados de Camada 2 normalmente armazena registros de NAPTR (Naming Authority

PoinTeR) para número de telefones individuais. No exemplo aqui considerado, o banco de dados de Camada 2 **150-1** é pretendido para armazenar registros de NAPTR para número de telefones de assinantes para o operador de telefonia A, e o banco de dados de Camada 2 **150-2** é pretendido para armazenar registros de NAPTR para números de telefones de assinantes para o operador de telefonia B; um registro de NAPTR genérico para um certo número de telefone armazena informação para o encaminhamento de chamadas colocadas para aquele número de telefone, e as preferências de encaminhamento e terminação de chamada de assinante.

[0069] É assinalado que a aplicabilidade da presente invenção não é limitada para o "e164.arpa" de ENUM público e global sendo bem como aplicável para sistema de ENUMs privados.

[0070] Na implementação convencional do sistema de ENUM, o registro genérico de NAPTR em um banco de dados de Camada 2 contém o URI (Identificador de Recursos de Uniforme) atribuídos para um determinado assinante de uma rede de telefonia; o URI é uma sequência de caracteres, tendo a sintaxe definida pelo documento RFC 3866 de IETF, que identifica recursos em uma rede como a Internet. O URI permite localizar o assinante usando os serviços de um DNS (Servidor de Nome de Domínio) ou sistemas de DNS 155. Em particular, os URIs armazenados nos registros de NAPTR do sistema de ENUM são "URIs de TEL", cujo formato é especificado no documento RFC 3966 do IETF (com o título de "*The tel URI for Telephone Numbers*"); um URI de TEL genérica descreve recursos identificados pelos números de telefone.

[0071] Como discutido na introdução da presente descrição, o sistema convencional de implementação de ENUM é exposta a vários riscos. O Requerente observou que muitos dos riscos para os quais o sistema de ENUM é exposto deriva do fato que os URIs de TEL são livremente acessíveis.

[0072] De acordo com uma modalidade da presente invenção, de

modo a superar esse problema e feito o sistema de ENUM mais seguro, uma plataforma de política de segurança é fornecida em conjunto com o sistema de ENUM.

[0073] Em particular, de acordo com uma modalidade da presente invenção, a plataforma de política de segurança, que na figura 1 é globalmente identificado pelo numeral de referência **160** e é representado em maior detalhe na figura 2, essencialmente compreende um Sistema de Perfil de Política (PPS) de segurança que permite a definição e gerenciamento de regras de política de segurança.

[0074] As regras de política de segurança são regras que definem o comportamento esperado do sistema quando acesso à informação armazenada no sistema de ENUM é tentado, e em particular eles definem que solicitações devem ser permitidas e que em seu lugar devem ser negadas em termos de informação que podem ser acessados (por exemplo discriminar dentre quem pode recuperar a informação e quando a informação pode ser recuperada).

[0075] O PPS de acordo com uma modalidade da presente invenção compreende um subsistema de gerenciamento de política (gerenciador de política) **165** adaptado para permitir a definição e registro de regras de política de segurança, e um subsistema de imposição de política (aplicador de política) **170** adaptado para aplicar as regras de política de segurança definidas através do registrado no gerenciador de política **165**.

[0076] As regras de política de segurança podem ser definidas e registradas diretamente por um usuário da plataforma de política de segurança, que pode ser um usuário final, sendo um assinante de um operador de telefonia e tendo atribuído um número de telefone, ou um operador de telefonia desejando estabelecer, com relação a um ou mais, possivelmente todos de seus assinantes, regras de política de segurança para condicionar o acesso aos serviços de ENUM; por exemplo, referindo à **Figura 1**, as regras de política de segurança podem ser definidos e registrados no gerenciador de

política **165** pelo assinante **115**, ou pelo operador de telefonia B do assinante **115**, ou por ambos deles.

[0077] O gerenciador de política **165** interage com o aplicador de política **170**.

[0078] Em particular, o gerenciador de política **165** fornece para o aplicador de política **170** as regras de política de segurança a serem impostas com relação aos assinantes específicos, ou / e com relação aos grupos de assinantes (possivelmente todos os assinantes) de um operador de telefonia; no exemplo mostrado na figura **1**, as regras de política de segurança são regras a serem impostas com relação ao assinante **115**, ou / e com relação aos grupos de assinantes (possivelmente todos os assinantes) do operador de telefonia B.

[0079] O gerenciador de política **165** também interage, através de interfaces de comunicação adequadas **205** e **210**, com o sistema de ENUM e possivelmente com o sistema de DNS, que na figura **2** são denotados de modo global como **215** e **220**, respectivamente; a interação do gerenciador de política **165** com o sistema de ENUM **215** e com o sistema de DNS **220** é descrita em detalhes mais tarde, quando a operação da plataforma de política de segurança **160** é descrita.

[0080] A plataforma de política de segurança **160** pode ser acessada por assinantes / operadores de telefonia através de uma extremidade frontal **230**, como por exemplo um servidor de HTTP (Protocolo de Transferência de Hiper Texto) ou um servidor de Web, permitindo aos clientes de software de PPS **235** fazer interface com o gerenciador de política **165** de modo a permitir a inserção / modificação / revogação de regras de política de segurança.

[0081] O gerenciador de política **165** pode ser baseado em um sistema de registro de VoIP padrão, i.e., ele pode ser um registro de SIP - Protocolo de Iniciação de Sessão - que é um elemento padrão elemento da arquitetura baseada no SIP, como definido no documento RFC 3261 do IETF, gerenciar o

registro de usuários. Como conhecido para aqueles com qualificação na arte, o SIP é um protocolo de controle de camada de aplicação (sinalização) que roda sobre o topo de vários diferentes protocolos de transporte e é com base no conjunto de protocolo de TCP / IP, e que pode ser usado para criar, modificar, e terminar sessões com um ou mais participantes. Essas sessões incluem chamadas de telefone de Internet (VoIP), distribuição de multimídia, conferências em multimídia. O SIP faz uso de elementos chamados servidores de preparação para ajudar a encaminhar solicitações para a localização corrente do usuário, autenticar e autorizar usuários para serviços, implementar provedor de políticas de encaminhamento de chamada, e fornecer recursos aos usuários. O SIP fornece uma função de registro que permite usuários para carregar suas localizações correntes para uso pelos servidores de preparação.

[0082] O gerenciador de política **165** inclui um banco de dados **240** onde as regras de política de segurança definidas pelos clientes são armazenadas.

[0083] O gerenciador de política **165** também compreende um gerador de mudo-URI, operável para gerar mudo, URIs fictícios que são, de modo unívoco, associados com URIs de SIP confiáveis, para o propósito de esconder os URIs de SIP confiáveis, como discutido em maior detalhe mais tarde.

[0084] A operação da plataforma de política de segurança de acordo com uma modalidade da presente invenção é descrita em detalhe daqui em diante.

[0085] De modo a um usuário, como por exemplo, o assinante **115** do operador de telefonia B, ou diretamente o próprio operador de telefonia B, em benefício dos serviços da plataforma de política de segurança **160**, uma subscrição preliminar para a plataforma de política de segurança é solicitada. Os passos principais de um procedimento de subscrição de usuário para a plataforma de política de segurança são representados no fluxograma

esquemático da **Figura 3**.

[0086] O usuário (como por exemplo, o assinante **115**, ou o operador de telefonia B) acessa (por exemplo, através de uma página da Web de um sítio da Web da plataforma de política de segurança) a plataforma de política de segurança **160**, particularmente o gerenciador de política **165** (ação **305**).

[0087] O usuário (o assinante **115**, ou o operador de telefonia B) fornece para o gerenciador de política **165** o respectivo número de telefone (por exemplo, o número de telefone +1-202-555-1234 do assinante **115** na figura **1**), junto com o correspondente URI de SIP (por exemplo, o URI de SIP de assinante **115** pode ser assinante-X@domain-B.com) e URI de TEL. Por exemplo, o usuário pode submeter esses dados usando o protocolo SIP, particularmente a mensagem SIP REGISTER, através da qual, como definido no documento RFC 3261 de IETF, informação de registro é transportado. O número de telefone pode ser fornecido já no formato de E.164, ou pode ser traduzido no formato E.164 através do gerenciador de política **165**. No fluxograma, essas ações são globalmente indicadas como a ação **310**.

[0088] O gerenciador de política **165** recebe e armazena a data de registro de usuário, por exemplo, no banco de dados de política **240**; então, o gerenciador de política **165** invoca o gerador de mudo-URI **245** pedindo a geração de um mudo-URI unívoco para ser associado com o URI de SIP recebido proveniente do usuário (ação **315**).

[0089] Um possível mudo-URI é uma sequência de ASCII mudo intrinsecamente sem sentido, i.e. uma sequência de caracteres, dígitos e símbolos em código ASCII; qualquer caráter pode ser usado, exceção feita para o símbolo "@", que é reservado sendo normalmente usado como um separador entre um nome de usuário e um nome de domínio da Internet. A sequência de ASCII mudo pode ser gerada pela concatenação de caracteres ASCII gerados aleatoriamente (por exemplo gerados por um algoritmo ou hardware gerador adaptado para gerar sequências aleatórias de números /

caracteres). Um exemplo de mudo-URI pode ser o seguinte: *asfjwegoSJDHASDOksdaoq12313asdaqe*.

[0090] Um outro possível mudo-URI é a concatenação de uma sequência ASCII mudo intrinsecamente sem sentido, com no exemplo acima, seguido pelo símbolo "@" seguido por um nome de domínio da Internet, i.e. pode ter o formato <mudo-ASCII-string>@<domain>. Um exemplo de mudo-URI pode neste caso se refere o seguinte: *fthftydftrtyer456drftddJHJI@domain-C.com*. O "domain", de modo unívoco, identifica uma plataforma de política de segurança, por exemplo o "domain" "domain-C" pode identificar a plataforma de política de segurança **160**. Nesta maneira, um sistema de plataformas de política de segurança pode ser configurado, cada um identificado por um correspondente nome de domínio, com a vantagem de realizar uma distribuição da carga mais do que uma plataforma de política de segurança.

[0091] O usuário então define as regras de política de segurança preferidas (ação **320**). Para este propósito, o usuário pode usar uma linguagem formal, tal como a XML (eXtensible Markup Language), por exemplo a linguagem define by OASIS (*Organization for the Advancement of Structured Information Standards*, sítio da Internet <http://www.oasis-open.org>), particularmente a linguagem XACML (*eXtensible Access Control Markup Language*) (detalhes nesta linguagem podem ser encontrados no endereço de Internet http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml).

[0092] Uma regra de política de segurança exemplar que o usuário pode definir é a seguinte:

<Rule>

<NAME> "Time Policy XYZ" </NAME>

<From>

<NUMBER> 202-555-1234 </NUMBER>

```

<INCOMING> Operator-A"< / INCOMING>
< / From>
<To> * < / To>
<Service> VoIP, MMS < / Service>
<RANGE DATE> MON-FRI < / RANGE DATE>
<ACTION> Disclose-URI < / ACTION>

< / Rule>

```

[0093] No exemplo acima, a sequência "Time Policy XYZ" entre as marcas <NAME>, < / NAME> define o nome da regra (o nome pode ser atribuído pelo usuário); as marcas <From>, < / From> e < TO >, < / TO> delimitam uma parte da regra onde o número de telefone do assinante para aquela regra de segurança é pretendida ser aplicada, e número de telefones ou intervalos de número de telefones ou identificadores de operadores de telefonia podem ser especificados; as marcas <Service>, < / Service> delimitam uma parte da regra onde serviços para os quais a regra é pretendida ser aplicada pode ser especificada; as marcas <RANGE DATE>, < / RANGE DATE> delimitam uma parte da regra onde intervalos de tempo podem ser especificados; as marcas <ACTION>, < / ACTION> delimitam uma parte da regra onde uma ou mais ações condicionadas para a satisfação da regra podem ser especificadas.

[0094] A regra exemplar acima, com o nome "Time Policy XYZ", estabelece que o URI associado com o número de E.164 202-555-1234 pode ser inquirido por (divulgados pára) todos os clientes de ENUM que são assinantes do "Operator-A" (o operador de telefonia A no exemplo da **Figura 1**) e quem deseja configurar uma chamada de VoIP ou enviar uma mensagem de MMS (Serviço de Tratamento de Mensagem de Multimídia) somente de Segunda a Sexta.

[0095] Outras regras de política de segurança exemplares podem definir (usando uma linguagem similar àquela usada para definir a regra

exemplar anterior) as seguintes condições: "Assinante A é sempre permitido resolver o número de telefone do Assinante B", "Assinante A é permitido resolver o número de telefone de Assinante B somente para serviços de MMS", "Assinantes não na comunidade do Assinante B não são permitidos resolver o número de telefones do Assinante B", onde a "comunidade" pode ser definida como um livro de endereço de números de telefones confiáveis definidos pelo assinante B (e.g., o assinante **115** na figura **1**), ou um intervalo de número de telefones que o operador de telefonia B considera confiável. Nos exemplos acima, por "resolver o número de telefone" é pretendido as ações para derivar, com base no serviço de ENUM e no DNS, a partir do número de telefone da parte chamada o respectivo endereço de IP para alcançar a parte chamada através da Internet.

[0096] O usuário pode definir uma ou mais regras de política de segurança; o usuário pode compilar as regras de política de segurança em tempo real, através do sítio de Web da plataforma de política de segurança **160**, ou off-line, em suas premissas, e então carregar as regra(s) compiladas anteriormente para a plataforma de política de segurança **160**.

[0097] O gerenciador de política **165** recebe as regras de política de segurança provenientes do usuário e as armazena nos banco de dados de política de segurança **240** (ação **325**). As regras de política de segurança são, de modo unívoco, associadas com o mudo-URI que foi anteriormente gerado e atribuído ao usuário.

[0098] Uma vez que o usuário completou a definição das regras de política de segurança desejada, o usuário fecha a sessão com o gerenciador de política **165** (ação **330**).

[0099] O gerenciador de política **165** então comunica as regras de política de segurança definida pelo usuário para o aplicador de política **170**. O gerenciador de política **165** também comunica o número de telefone recebido pelo usuário e o mudo-URI associado, de modo unívoco,, gerado para aquele

número de telefone para o sistema de ENUM **215** (ação **335**); o número de telefone e o mudo-URI intrinsecamente sem sentido associado (não o SIP URI de SIP real, como na usual ENUM serviço implementação de serviço de ENUM) é assim sendo armazenado nos bancos de dados de ENUM. Em particular, considerando o exemplo da **Figura 1**, esses dados são armazenados no banco de dados Camada 2 **150-2**.

[00100] Opcionalmente, o gerenciador de política **165** pode comunicar para o sistema de DNS **220**, o domínio e endereço de IP do usuário que o terminal de comunicação do usuário ou os aparelhos de rede núcleo do operador comunicou para o gerenciador de política de segurança **165** (ação **340**). Isto pode ser útil naqueles casos onde ao usuário que se inscreveu para a plataforma de política de segurança foi atribuído um endereço IP estático, que dinamicamente não muda de uma sessão de Internet para outra.

[00101] O usuário pode acessar a plataforma de política de segurança **160** mesmo após ter sido preliminarmente subscrito a ela, por exemplo para modificar as regras de política de segurança anteriormente definidas, adicionar novas regras, eliminar regras. Cada vez que uma mudança nas regras de política de segurança ocorre, as novas regras de política de segurança são comunicadas ao aplicador de política **170**.

[00102] Cada vez que o usuário **110** liga seu terminal (com um telefone habilitado em IP, e.g. um telefone de VOIP) e se conecta aos aparelhos da rede núcleo **110** do operador de telefonia B, para conectar à Internet **130**, ao terminal de usuário é atribuído um endereço de IP (por exemplo, no caso de **115** o endereço de IP hipotético 11.22.33.44). Uma fase de registro do SIP ocorre (conforme especificado no documento de RFC 3261 do IETF), através do qual o terminal de usuário se registra em um servidor SIP de registro (não mostrado nos desenhos porque é conhecido por si só). O terminal de usuário comunica o endereço de IP atribuído a ele e o respectivo URI de SIP para o servidor de SIP de registro. Na conclusão bem sucedida do registro do

terminal de usuário, o usuário é considerado como "presente" e capaz de receber chamadas entrantes (sendo passível de ser alcançado no endereço de IP atribuído). O servidor de SIP de registro comunica a informação de "presença" do usuário para a plataforma de política de segurança **160**. No caso o usuário **110** não tem um terminal habilitado na Internet, com um antigo plano telefônico, o registro de SIP do usuário é efetuado pelos aparelhos da rede núcleo do operador de telefonia B.

[00103] O fluxograma esquemático das **Figuras 4A e 4B** mostra as principais ações efetuadas pela plataforma de política de segurança de acordo com uma modalidade da presente invenção, quando alguém, como por exemplo, o assinante **105** do operador de telefonia A na figura **1**, tenta alcançar o assinante **115** do operador de telefonia B através da Internet.

[00104] Em particular, no cenário agora considerado, é assumido que o assinante **105** deseja colocar uma chamada telefônica para o assinante **115** usando um plano telefônico, i.e. não um telefone habilitado na Internet como um telefone de VoIP.

[00105] O assinante **105** disca como de costume em seu telefone o número de telefone do assinante **115**, completado com o código de país e código de área.

[00106] Quando os aparelhos de rede **120** do operador de telefonia A recebem do assinante **105** uma solicitação para estabelecer uma conexão com o assinante **115**, os aparelhos de rede **120**, particularmente a funcionalidade de cliente de ENUM **135**, contatam o sistema de ENUM **215**, fornecer a ele o número de E.164 do telefone do assinante chamado (ação **405**).

[00107] O sistema de ENUM **215** olha através de seus bancos de dados pesquisando pelo número de E. 164 especificado (ação **410**). Em particular, no exemplo da **Figura 1**, a árvore dourada do ENUM, i.e. a estrutura hierárquica dos bancos de dados é galgada a partir do banco de dados Camada 2 **150-1** para o banco de dados Camada O **140**, e então descida para o banco

de dados Camada 2 **150-2**.

[00108] O banco de dados de ENUM **150-2** que armazena o registro de NAPTR para o número de E. 164 pesquisado fornece o registro de NAPTR encontrado para funcionalidade de cliente de ENUM **135** do operador de telefonia A (ação **415**). O registro de NAPTR retornado para a funcionalidade de cliente de ENUM **135** contém o mudo-URI associado com o número de telefone especificado.

[00109] A funcionalidade de cliente de ENUM **135**, que é assumido ser capaz de reconhecer que um URI é um mudo-URI e não um SIP URI de SIP real, indaga a plataforma de política de segurança **160**, particularmente o aplicador de política **170**, perguntando pelo URI de SIP real da parte chamada correspondente ao mudo-URI (ação **420**). Quando contatando o aplicador de política **170**, a funcionalidade de cliente de ENUM **135** fornece para o aplicador de política **170** suas credenciais, por exemplo usando um mecanismo de autenticação mútua do tipo fornecido pelo protocolo de TLS (Segurança de Camada de Transporte) baseado em certificados digitais definidos no documento RFC 2246 do IETF (ou outro mecanismo de segurança similar, como por exemplo o mecanismo de IPsec definido no documento RFC 2401 do IETF). As credenciais que a funcionalidade de cliente de ENUM **135** fornece para o aplicador de política **170** pode incluir informação sobre a identidade da parte de quem chama (e.g., o número de telefone dele), i.e. do assinante **105**; esta informação pode ser necessária para o processamento da solicitação pelo aplicador de política **170**.

[00110] O aplicador de política **170** processa solicitação proveniente da funcionalidade de cliente de ENUM **135** e, usando o mudo-URI recebido a partir da funcionalidade de cliente de ENUM **135** como uma chave para pesquisar entre as políticas de segurança que ele armazena, pega as regras de política de segurança associadas com aquele mudo-URI (ação **425**).

[00111] Então, o aplicador de política **170** processa as regras de

política de segurança associadas com o mudo-URI especificado (ação **430**). Dependendo nos resultados do processamento das regras de política de segurança, o aplicador de política **170** retorna uma resposta para a funcionalidade de cliente de ENUM **135**. Se, como no exemplo aqui considerado, o aplicador de política **170** confirma que a parte de quem chama, i.e. o assinante **105**, tem condição de **resolver** o mudo-URI a fim de recuperar o endereço de IP da parte chamada, i.e. o assinante **115**, o aplicador de política **170** retorna para a funcionalidade de cliente de ENUM **135** o URI de SIP da parte chamada (ação **435**); se, ao contrário, o processamento das regras de política de segurança fornece como um resultado que a parte de quem chama não tem condição de recuperar o URI de SIP real (através do que ele poderia resolver o endereço de IP) da parte chamada, o mudo-URI não é resolvido, e uma resposta negativa é enviada de volta para a funcionalidade de cliente de ENUM **135**. As regras de política de segurança podem também definir comportamentos específicos naqueles casos onde o usuário chamado não está "presente", i.e. seu terminal de comunicações não se registrou no servidor SIP de registro; por exemplo, as regras de política de segurança pode prescrever que no caso que o usuário chamado não esteja "presente", i.e. ele não pode ser contatado no momento, a solicitação do chamador é simplesmente descartada, ou ela pode prescrever que se o chamador tem condição de resolver o mudo-URI, mas o usuário chamado não está "presente", i.e. ele não pode ser contatado no momento, uma mensagem de informação de cortesia é enviada para o chamador.

[00112] Para uma segurança aumentada, o gerenciador de política **165** pode gerar um novo mudo-URI para aquele número de telefone, e armazena o novo mudo-URI no banco de dados de ENUM apropriado em substituição ao anterior.

[00113] A funcionalidade de cliente de ENUM **135** recebe o URI de SIP da parte chamada (ação **440**), então ela usa o URI de SIP recuperado para

indagar o sistema de DNS **215** para achar o endereço de IP da parte chamada, i.e. do assinante **115**, ou da rede **110** (e.g., de um servidor de chamada) do operador de telefonia B do assinante chamado **115** (ação **445**).

[00114] O sistema de DNS **215** localiza o endereço de IP pesquisado, usando o URI de SIP (ação **450**) e retorna o endereço de IP da (servidor de chamada da) rede **110** do operador de telefonia B do assinante chamado **115** para um servidor de chamada nos aparelhos de rede **120** do operador de telefonia A (ação **455**).

[00115] O servidor de chamada nos aparelhos de rede **120** do operador de telefonia A usa o endereço de IP recuperado para tentar estabelecer a chamada com a parte chamada (assinante **115**). Em particular, assumindo que SIP é usado como protocolo de sinalização entre as redes de telefonia **100** e **110**, o servidor de chamada nos aparelhos de rede **120** do operador de telefonia A pode enviar uma mensagem de INVITE de SIP (uma mensagem padrão permitindo configurar uma chamada telefônica) que contém o URI de SIP para o cliente "B"; o servidor de chamada nos aparelhos de rede **125** do operador de telefonia B resolve o URI de SIP do assinante chamado **115** em um endereço de IP local (i.e., interno à rede **110**) do assinante chamado **115** (e.g., um endereço de IP dinâmico atribuído pelo operador de telefonia B para um terminal de comunicação, e.g. um telefone de VOIP, ou um computador pessoal, do assinante chamado **115**) e a conversação entre os assinantes **105** e **115** pode acontecer por meios da rede infra-estruturas de rede dos operadores de telefonia A e B.

[00116] É assinalado que o procedimento descrito acima se da mesma forma no caso que os assinantes **105** e **115** pertencem à mesma rede (e.g. Rede A, no qual caso os aparelhos de rede **120** e **125** e os bancos de dados Camada 2 **150-1** e **150-2** coincidem); em tal um caso, a resolução do URI de TEL do assinante chamado **115** é simplificado, já que somente o banco de dados Camada 2 de ENUM **150-1** está envolvido.

[00117] Na **Figura 5**, um outro possível cenário de aplicação de uma modalidade da presente invenção é, de forma esquemática, mostrado. Os mesmos numerais de referência são usados para denotar elementos que são idênticos ou similares àqueles mostrados na **figura 1**.

[00118] Neste outro cenário, é assumido que o assinante **105**, sendo a parte de quem chama no exemplo considerado, tem um telefone habilitado na Internet, como um telefone de VoIP, com uma funcionalidade de cliente de ENUM **535** adaptada para efetuar as ações que, no cenário da **Figura 1**, foi por sua vez efetuado pela funcionalidade de cliente de ENUM **135** dos aparelhos de rede **120** do operador de telefonia A.

[00119] O fluxograma esquemático das **Figuras 6A e 6B** mostra as ações principais efetuadas através da plataforma de política de segurança de acordo com uma modalidade da presente invenção, quando alguém, como por exemplo o assinante **105** do operador de telefonia A na **figura 5**, tenta alcançar o assinante **115** do operador de telefonia B através da Internet. É assumido que o assinante **115** (ou seu operador de telefonia B) se registrou na plataforma de política de segurança **160** e definiu suas regras de política.

[00120] O assinante **105** disca como de costume o número de telefone do assinante chamado **115**, complementado com o código de país e código de área.

[00121] A funcionalidade de cliente de ENUM **535** do telefone do assinante **105** contata o sistema de ENUM **215**, fornecendo a ele o número de E.164 do telefone do assinante chamado (ação **605**).

[00122] O sistema de ENUM **215** olha através de seus bancos de dados pesquisando pelo número de E. 164 especificado (ação **610**). Em particular, no exemplo da **Figura 1**, a árvore dourada do ENUM, i.e. a estrutura hierárquica dos bancos de dados é galgada dos banco de dados Camada 2 **150-1** para o banco de dados Camada 0 **140**, e então descida para o banco de dados Camada 2 **150-2**.

[00123] O banco de dados de ENUM **150-2** que armazena o registro de NAPTR para o número de E. 164 pesquisado fornece o registro de NAPTR encontrado para a funcionalidade de cliente de ENUM **535** do telefone do assinante **105** (ação **615**). O registro de NAPTR retornado para a funcionalidade de cliente de ENUM **535** contém o mudo-URI associado com o número de telefone especificado.

[00124] A funcionalidade de cliente de ENUM **535**, que é assumida ser capaz de reconhecer que um URI é um mudo-URI, indaga a plataforma de política de segurança **160**, particularmente o aplicador de política **170**, perguntando pelo o URI de SIP real da parte chamada correspondente ao mudo-URI (ação **620**). Quando contatando o aplicador de política **170**, a funcionalidade de cliente de ENUM **535** fornece para o aplicador de política **170** suas credenciais, por exemplo usando um mecanismo de autenticação mútua do tipo fornecido pelo protocolo de TLS (Transport Layer Security) com base nos certificados digitais definidos no documento RFC 2246 do IETF (ou outro mecanismo de segurança similar, como por exemplo mecanismo de IPsec definido no documento de RFC 2401 do IETF). As credenciais que a funcionalidade de cliente de ENUM **535** fornece para o aplicador de política **170** pode incluir informação sobre a identidade da parte de quem chama (e.g., o número de telefone dele), i.e. do assinante **105**; esta informação pode ser necessária para o processamento da solicitação pelo aplicador de política **170**.

[00125] O aplicador de política **170** processa a solicitação a partir da funcionalidade de cliente de ENUM **535** e, usando o mudo-URI como uma chave, pega as regras de política de segurança associadas com ela (ação **625**).

[00126] Então, o aplicador de política **170** processa as regras de política de segurança associadas com o mudo-URI (ação **630**) especificado. Dependendo dos resultados do processamento das regras de política de segurança, o aplicador de política **170** envia uma resposta para a

funcionalidade de cliente de ENUM **535**. Se, como no exemplo aqui considerado, o aplicador de política 170 confirma que a parte de quem chama, i.e. o assinante **105**, tem condição de resolver o mudo-URI a fim de recuperar o URI de SIP (através do qual ela poderia resolver o endereço de IP) da parte chamada, i.e. o assinante **115**, o aplicador de política 170 retorna para a funcionalidade de cliente de ENUM **535**, o URI de SIP da parte chamada (ação **635**); se, ao contrário, o processamento das regras de política de segurança fornece como um resultado que a parte de quem chama não tem condição de recuperar o URI de SIP da parte chamada, o mudo-URI não é resolvido, e uma resposta negativa é enviada de volta para a funcionalidade de cliente de ENUM **535**.

[00127] A funcionalidade de cliente de ENUM **535** recebe o URI de SIP da parte chamada (ação **640**), então ela indaga o sistema de DNS **215** para achar o endereço de IP da parte chamada, i.e. do assinante **115**, ou da rede **110** do operador de telefonia B do assinante chamado **115** (ação **645**).

[00128] O sistema de DNS **215** localiza o endereço de IP pesquisado, usando o URI de SPI (ação **650**) e retorna o endereço de IP da parte chamada, i.e. do assinante **115**, ou da rede **110** do operador de telefonia B do assinante chamado **115** para o telefone do assinante **105** (ação **655**).

[00129] O telefone do assinante **105** usa o endereço de IP recuperado para tentar estabelecer uma chamada com a parte chamada (assinante **115**). Em particular, o telefone do assinante **105** pode enviar uma mensagem de INVITE de SIP que contém o URI de SIP para o cliente "B", para o telefone do assinante **115**, ou para um servidor de chamada nos aparelhos de rede **125** do operador de telefonia B; o servidor de chamada nos aparelhos de rede **125** do operador B de telefonia resolve o URI de SIP do assinante chamado **115** em um endereço de IP local (i.e., interno para a rede **110**) IP do assinante chamado **115** (e.g., um endereço de IP dinâmico atribuído pelo operador B de telefonia para um terminal de comunicação, e.g. um telefone de VoIP, ou um

computador pessoal, do assinante chamado **115**) e a conversação entre os assinantes **105** e **115** pode acontecer.

[00130] Como no cenário anteriormente descrito, o procedimento apenas descrito se aplica da mesma forma no caso que os assinantes **105** e **115** pertencem à mesma rede (e.g. Rede A, em qual caso os aparelhos de rede **120** e **125** e os banco de dados Camada 2 **150-1** e **150-2** coincidem); em tal um caso, a resolução do URI de TEL do assinante chamado **115** é simplificado, já que somente o banco de dados Camada 2 banco de dados **150-1** do ENUM está envolvido.

[00131] De modo aumentar o grau de segurança, a plataforma de política de segurança **160** pode gerar um novo mudo-URI (e comunicá-lo as outras entidades) cada vez que um mudo-URI é resolvido e o correspondente URI de SIP recuperado; nesta maneira, é assegurado que a informação sobre um URI de SIP obtido uma vez resolvendo um correspondente mudo-URI pode ser re-usado mais tarde, possivelmente por sujeitos indesejados.

[00132] A partir da descrição acima de algumas modalidades exemplares dela, pode ser apreciado que a presente invenção permite fazer os serviços de ENUM mais seguros mantendo escondida a informação para contatar usuários finais, e submeter a recuperação da informação de contato mencionada à satisfação das regras de segurança que podem ser definidas pelos usuários finais ou através de seus operadores de telefonia. A recuperação da informação de contato necessária para contatar alguém através da internet iniciando a partir de seu número de telefone usual pode assim sendo ser permitido somente para usuários / classes de usuários selecionadas, que são considerados "confiáveis", e isto permite por exemplo evitar formação de spam e, em geral, chamadas de pessoas / entidades indesejadas.

[00133] A plataforma de política de segurança pode ser implementada por meio de um ou mais servidores conectados à Internet, e oferecer serviços para operadores de telefonia.

[00134] A presente invenção foi aqui divulgada fazendo referência a algumas modalidades exemplares dela, contudo aqueles com qualificação na arte prontamente vão reconhecer que modificações para as modalidades descritas são possíveis, assim como outras modalidades, sem se afastar do escopo das reivindicações anexas. Por exemplo, as ações para gerar um mudo-URI a ser associado com um número de telefone e comunicar para o sistema de ENUM o número de telefone e o mudo-URI pode ser efetuado somente a primeira vez que um usuário se inscreve à plataforma de política de segurança, conforme descrito no descrito anteriormente, ou periodicamente, ou qualquer hora que alguém tenta contatar o cessionário do assinante daquele número de telefone.

[00135] Mais geralmente, a presente invenção pode aplicar aos sistemas outros do que ENUM, onde, contudo um banco de dados pretendido para armazenar informação de contato de usuários é fornecido.

REIVINDICAÇÕES

1. Método para prover serviços de telecomunicação, caracterizado pelo fato de que compreende:

- gerar (315) por uma plataforma de política de segurança (160) uma informação de contato fictícia univocamente associada com um número de telefone atribuído a um assinante, em que a informação de contato fictícia é uma informação que *per se* não pode ser usada para contatar o assinante;

- armazenar (335) a informação de contato fictícia em uma base de dados (150-2);

- em resposta a uma solicitação (405, 605), recebida de um solicitante (105, 135, 105, 535) de uma informação de contato real correspondendo ao número de telefone e adaptada para permitir contato através da Internet com o cessionário do assinante do número de telefone, ter a base de dados provendo (415, 615) a informação de contato fictícia;

- reconhecer (420, 620) o caractere fictício da informação de contato fictícia pelo solicitante;

- solicitar (420; 620), pelo solicitante, uma resolução da informação de contato fictícia;

- condicionar (425, 430, 625, 630) a resolução da informação de contato fictícia para o provisionamento da informação de contato real para a satisfação de pelo menos uma regra de segurança adaptada para avaliar propriedades de pelo menos um dentre o solicitante e a solicitação, e

- no caso de a solicitação do solicitante satisfazer dita pelo menos uma regra de segurança, resolver a informação de contato fictícia e prover (435, 635) ao solicitante a informação de contato real.

2. Método, de acordo com a reivindicação 1, caracterizado pelo fato de que a base de dados é uma base de dados ENUM.

3. Método, de acordo com a reivindicação 1 ou 2,

caracterizado pelo fato de que a informação de contato inclui um SIP URI identificando univocamente o assinante; e

a informação de contato fictícia inclui um URI fictício univocamente associado com o SIP URI do assinante.

4. Método, de acordo com a reivindicação 3, caracterizado pelo fato de que o URI fictício inclui informação aleatoriamente gerada.

5. Método, de acordo com a reivindicação 4, caracterizado pelo fato de que o URI fictício inclui um nome de domínio identificando univocamente um sistema resolvidor adaptado para resolver a informação de contato fictícia condicionada à satisfação da pelo menos uma regra de segurança.

6. Método, de acordo com qualquer uma das reivindicações 1 a 5, caracterizado pelo fato de que a pelo menos uma regra de segurança define um ou mais entre: operadoras de rede de telefonia habilitadas para resolver a informação de contato fictícia, solicitantes habilitados para resolver a informação de contato fictícia, tipos de serviços de conectividade que o solicitante é habilitado a explorar para contatar através da Internet o cessionário de assinante do número de telefone, indicações sobre datas e vezes quando os solicitantes são permitidos contatar o cessionário de assinante do número de telefone.

7. Método, de acordo com qualquer uma das reivindicações 1 a 6, caracterizado pelo fato de que compreende:

habilitar (230) ou o cessionário de assinante do número de telefone ou uma operadora de telefonia ao qual o assinante subscreveu, para definir a pelo menos uma regra de segurança.

8. Sistema para prover serviços de telecomunicação, caracterizado pelo fato de que compreende:

- um gerador (245) compreendendo uma plataforma de política de segurança (160) adaptada para gerar informação de contato fictícia

univocamente associada com um número de telefone atribuído a um assinante, e para fazer a informação de contato fictícia ser armazenada em uma base de dados (150-2) como uma informação de contato do assinante, em que a informação de contato fictícia é uma informação a qual *per se* não pode ser usada para contatar o assinante;

- um executor de regras de política de segurança (170) adaptado para:

- receber, de um solicitante (105, 135, 105, 535) capaz de reconhecer o caractere fictício da informação de contato fictícia, uma solicitação de resolução da informação de contato fictícia para obter uma informação de contato real correspondendo ao número de telefone, a informação de contato real sendo adaptada para permitir contatar através da Internet um assinante tendo o número de telefone; e

- condicionar uma resolução da informação de contato fictícia e a provisão para o solicitante da informação de contato para pelo menos uma regra de segurança adaptada para avaliar propriedades de pelo menos um dentre o solicitante e a solicitação.

9. Sistema, de acordo com a reivindicação 8, caracterizado pelo fato de que dita base de dados é uma base de dados ENUM.

10. Sistema de acordo com a reivindicação 8 ou 9, caracterizado pelo fato de que dita informação de contato inclui um SIP URI identificando univocamente o assinante; e

a informação de contato fictícia inclui um URI fictício univocamente associado com o SIP URI do assinante.

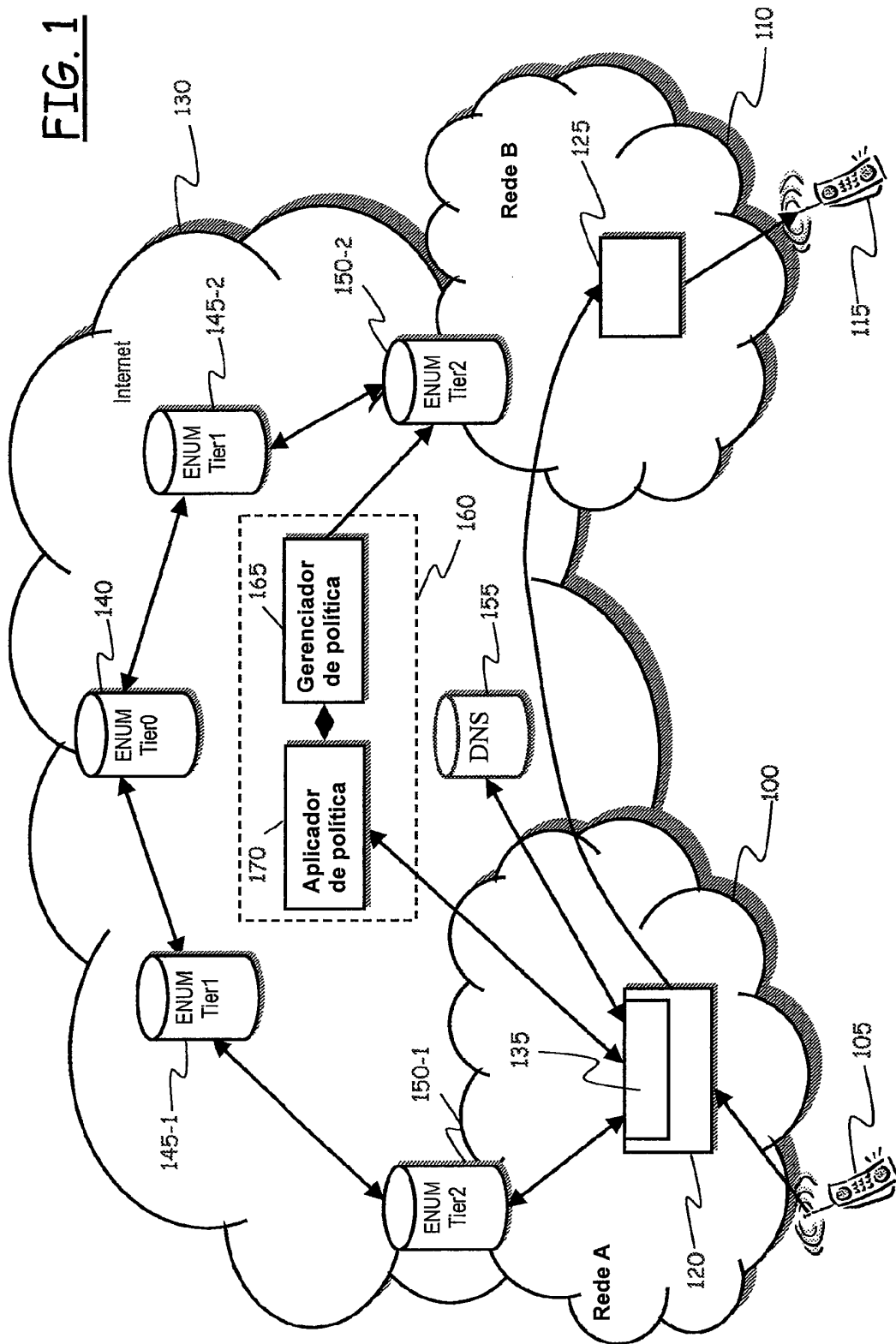
11. Sistema, de acordo com a reivindicação 10, caracterizado pelo fato de que o URI fictício inclui informação aleatoriamente gerada.

12. Sistema, de acordo com a reivindicação 11, caracterizado pelo fato de que o URI fictício inclui um nome de domínio univocamente identificando o executor de regras de política de segurança.

13. Sistema, de acordo com qualquer uma das reivindicações 8 a 12, caracterizado pelo fato de que a pelo menos uma regra de segurança define um ou mais dentre: operadoras de rede de telefonia habilitadas para resolver a informação de contato fictícia, solicitantes habilitados para resolver a informação de contato fictícia, tipos de serviços de conectividade que o solicitante é habilitado a explorar para contatar através da Internet o cessionário de assinante do número de telefone, indicações sobre datas e vezes quando os solicitantes são permitidos contatar o cessionário de assinante do número de telefone.

14. Sistema, de acordo com qualquer uma das reivindicações 8 a 13, caracterizado pelo fato de que compreende um gerente de regra de segurança (230) adaptado para ou permitir o cessionário de assinante do número de telefone ou uma operadora de telefonia ao qual o assinante subscreveu, definir a pelo menos uma regra de segurança.

15. Sistema, de acordo com qualquer uma das reivindicações 8 a 14, caracterizado pelo fato de que o gerador é adaptado para gerar uma informação de contato fictício nova univocamente associada com o número de telefone atribuído ao assinante depois de resolver a informação de contato fictícia.

FIG. 1

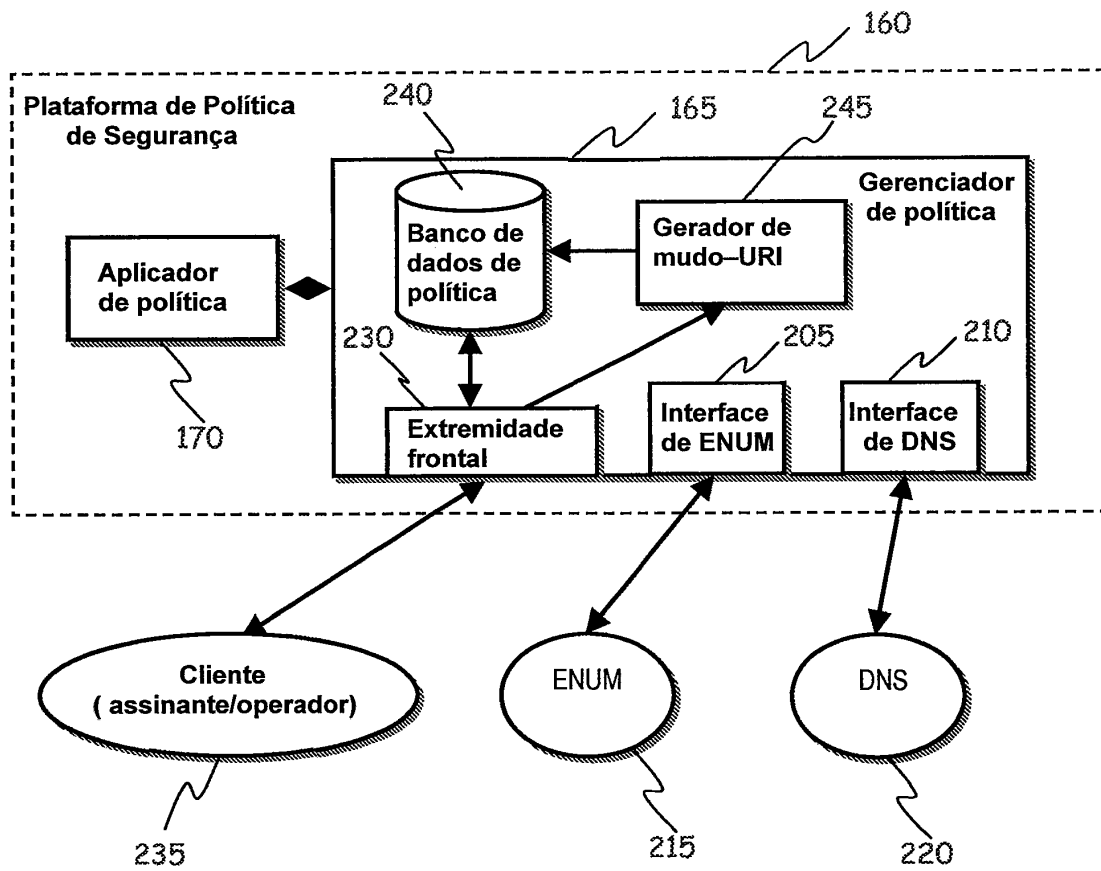
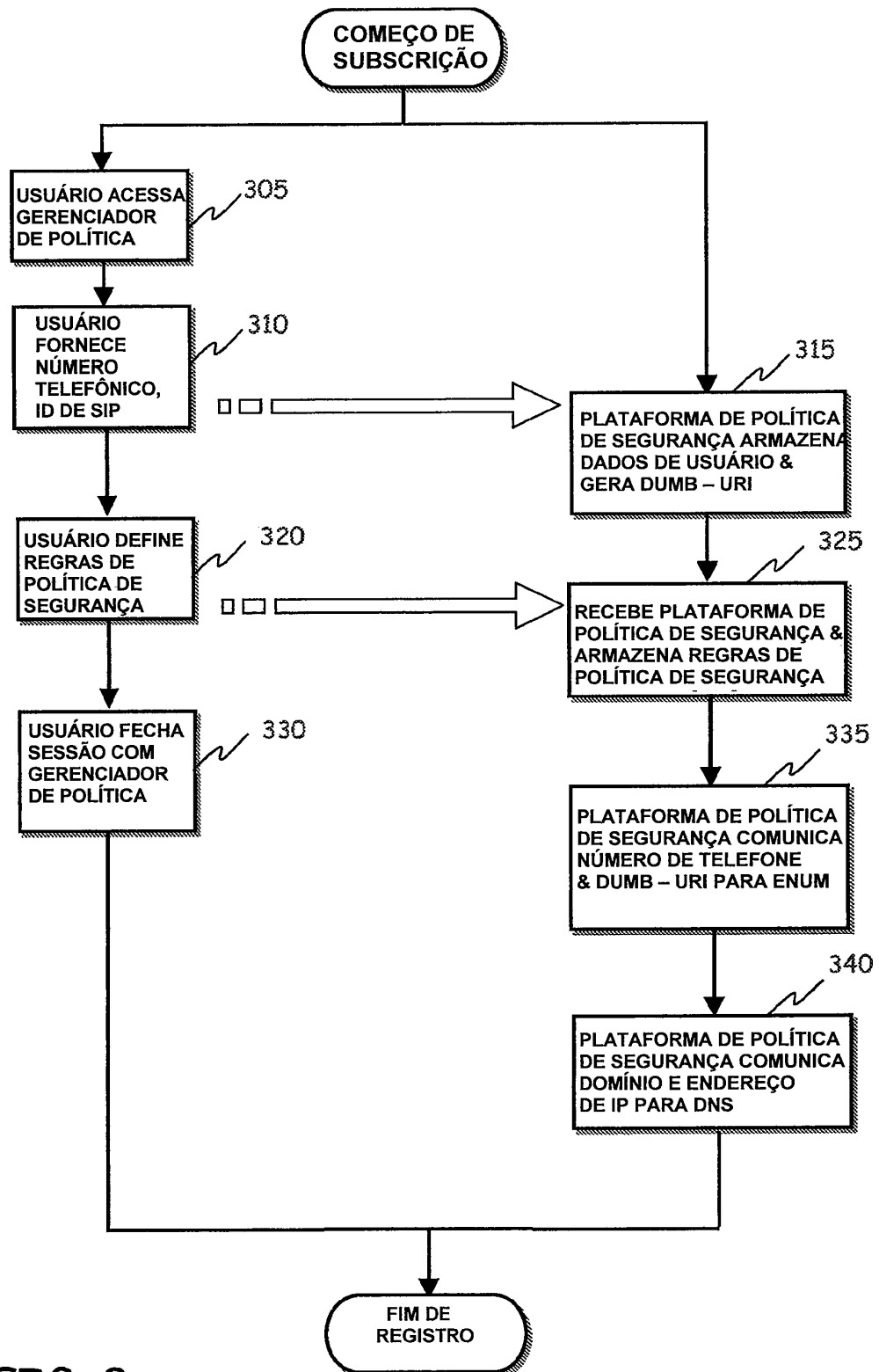


FIG. 2

FIG. 3

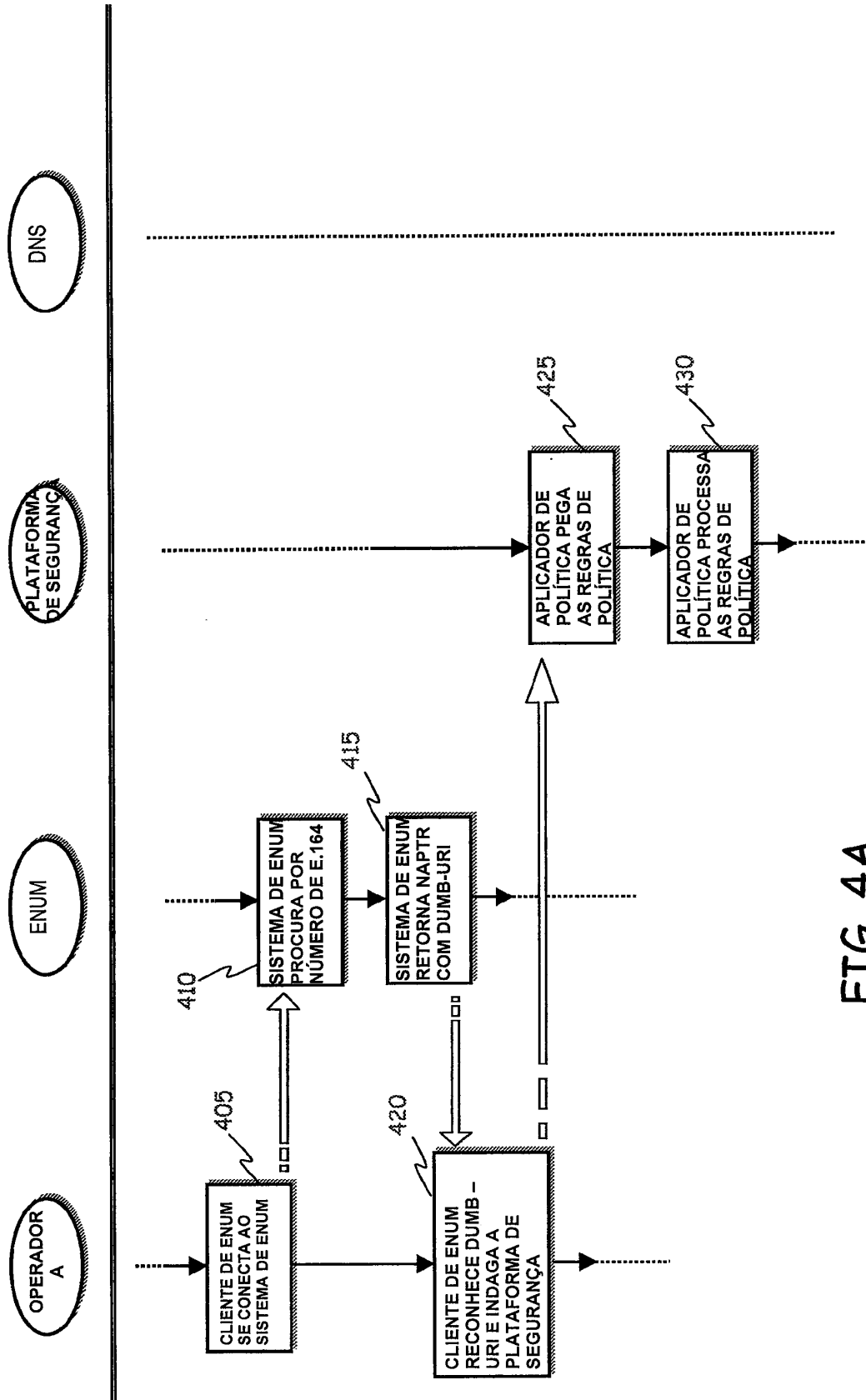


FIG. 4A

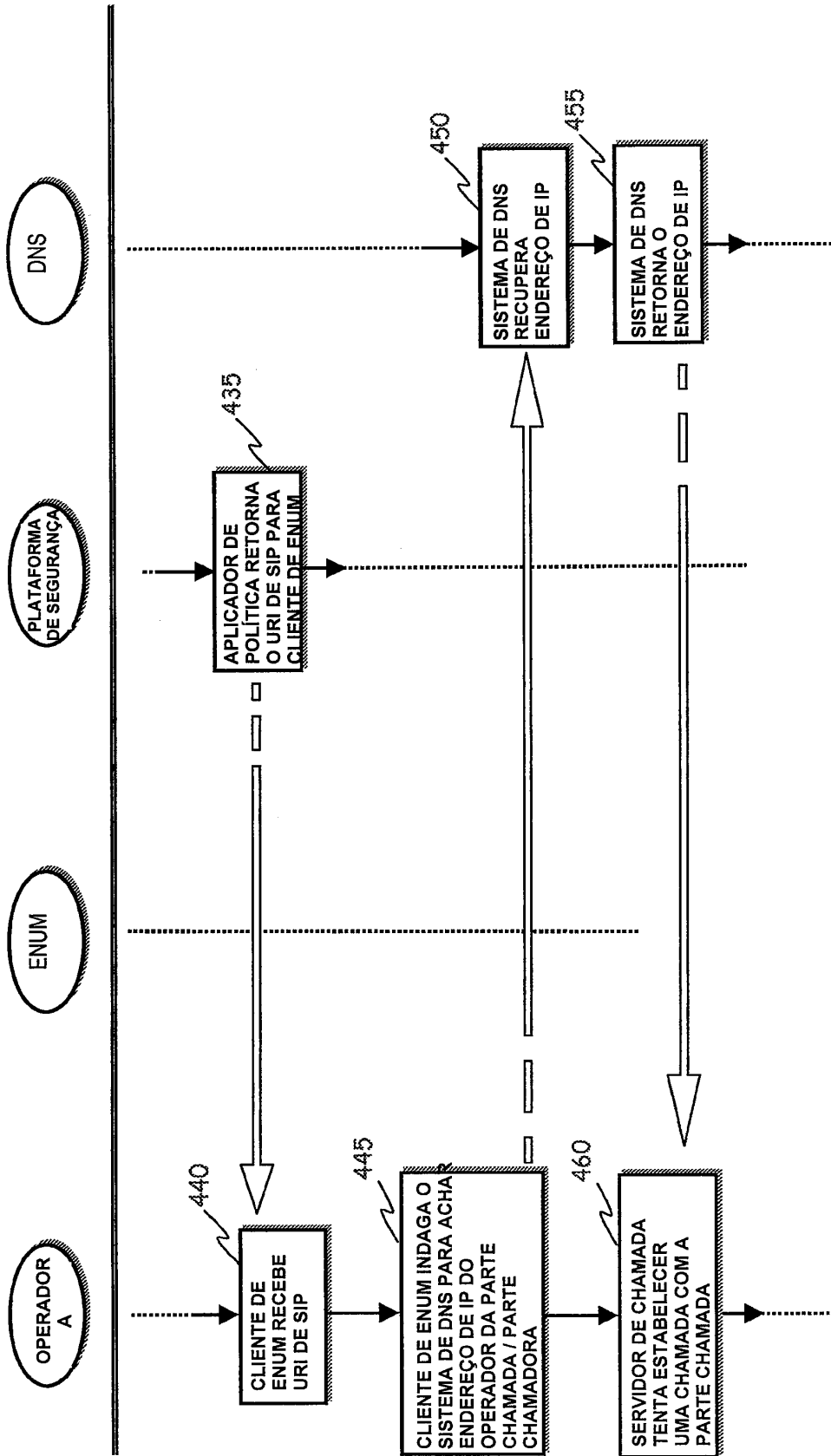
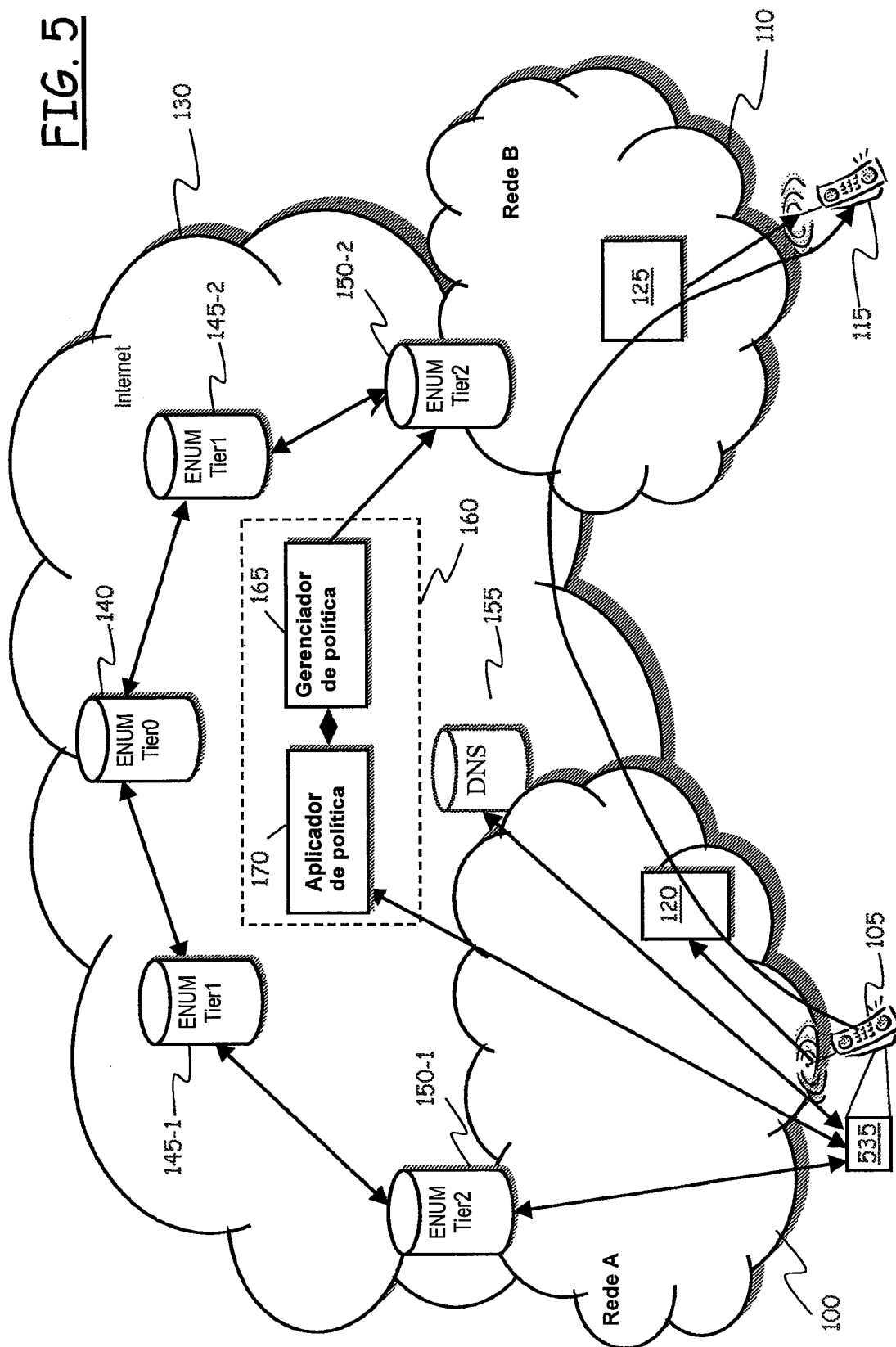


FIG. 4B

FIG. 5

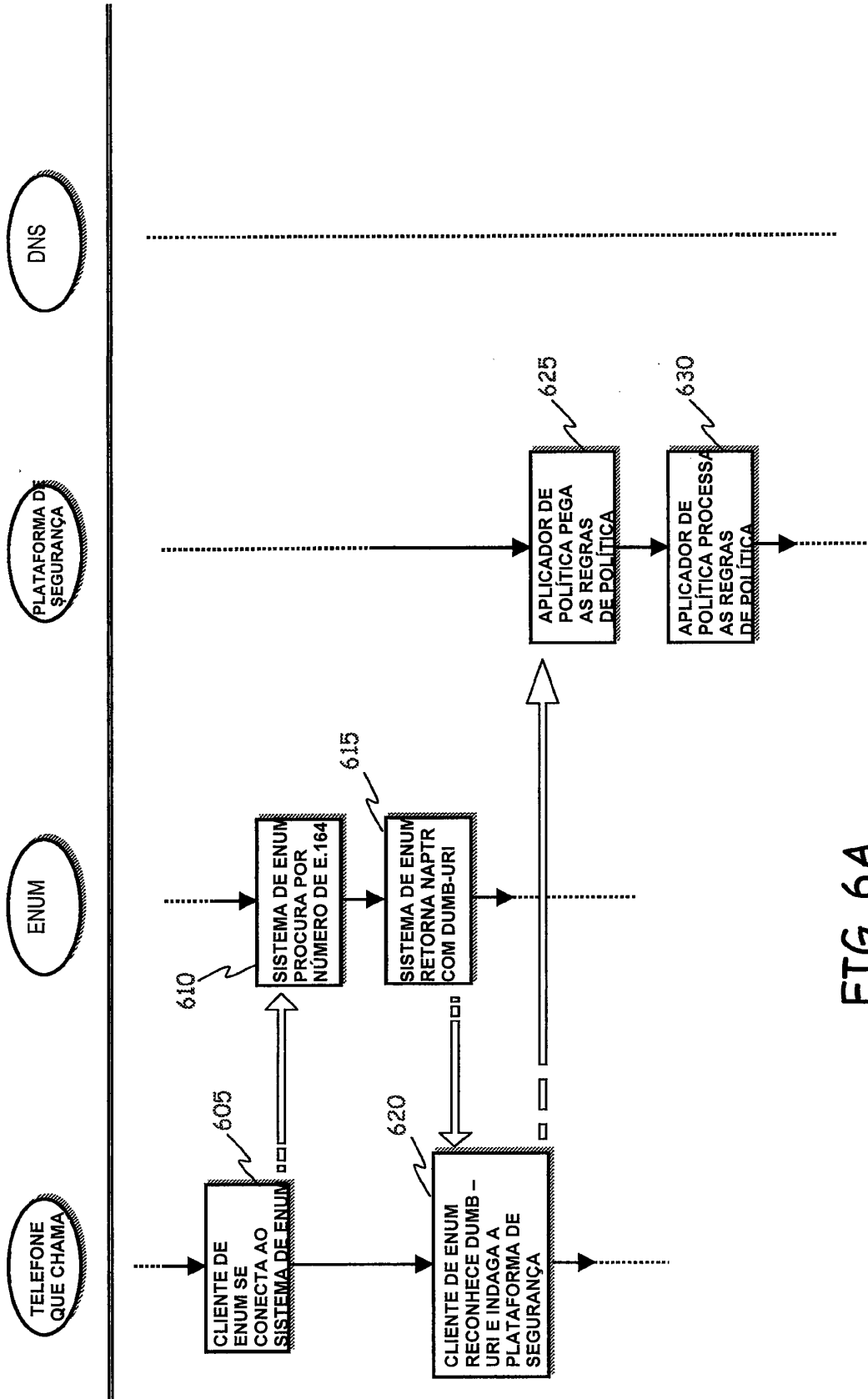


FIG. 6A

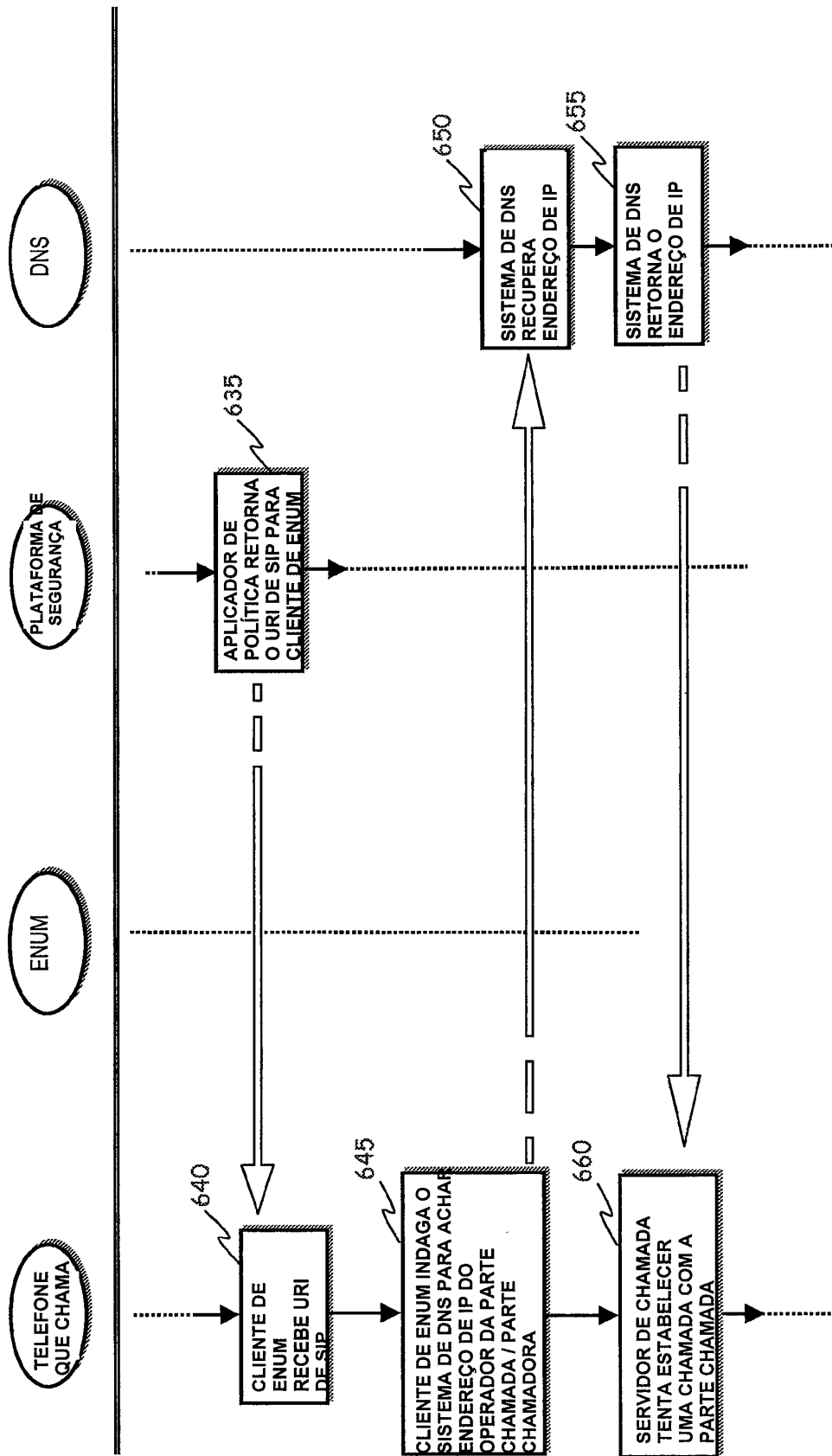


FIG. 6B