República Federativa do Brasil
Ministério da Indústria, Comércio Exterior e Serviços
Instituto Nacional da Propriedade Industrial

(11) PI 0112960-0 B1

(22) Data do Depósito: 25/07/2001

(45) Data de Concessão: 06/12/2016

(54) Título: MÉTODO PARA A VERIFICAÇÃO DE ENVIO E INTEGRIDADE DE MENSAGENS ELETRÔNICAS

(51) Int.Cl.: H04L 12/58; H04L 29/06

(30) Prioridade Unionista: 27/07/2000 US 09/626,577

(73) Titular(es): RPOST INTERNATIONAL LIMITED

(72) Inventor(es): TERRANCE A. TOMKOW

Relatório Descritivo da Patente de Invenção para **"MÉTODO PARA A VERIFICAÇÃO DE ENVIO E INTEGRIDADE DE MENSAGENS ELETRÔNICAS".**

Antecedentes da Invenção

I. Campo da Invenção

[001] Esta invenção refere-se, geralmente, a um sistema e a um método para a verificação do envio e do conteúdo de uma mensagem eletrônica e, mais particularmente, a um sistema e a um método de provisão posterior de provas referentes ao envio e ao conteúdo de uma mensagem de e-mail.

II. Descrição da Técnica Relacionada

[002] Nos últimos anos, o e-mail se tornou uma ferramenta comercial indispensável. O e-mail substituiu a "correio tartaruga" para muitas práticas comerciais, porque é mais rápido, mais econômico e, geralmente, mais confiável. Mas ainda permanecem algumas aplicações de correio onde uma cópia física ainda é dominante, tal como correio registrado e certificado. Por exemplo, quando uma carta é enviada por um correio certificado, ao remetente é provido um recibo, para provar que a carta foi postada. Um recibo de correio registrado com aviso de recebimento acrescenta ao Serviço Postal a confirmação que a carta foi enviada com sucesso para o destinatário ou para um agente autorizado do destinatário. Adicionalmente, empresas privadas de envio de correspondência, tais como a Federal Express® e a United Parcel Service® (UPS) proveem algum tipo de confirmação de envio. Uma vez que cada peça do correio por empresa de envio de correspondência, com efeito, é registrada, é natural que os consumidores se voltem para esses serviços, quando eles desejam uma prova do envio.

[003] Muitos dos sistemas de e-mail existentes e dos programas de e-mail já proveem alguma forma de prova de envio. Por exemplo,

alguns sistemas de e-mail hoje em dia permitem que um remetente marque uma mensagem com um rótulo "requisição de notificações". Esses rótulos permitem que o remetente requisite uma notificação de que a mensagem foi enviada e/ou quando a mensagem foi aberta. Quando um remetente requisita uma notificação de envio, o sistema de e-mail da Internet pode prover ao remetente um recibo de e-mail de que a mensagem foi enviada para o servidor de correio ou para a caixa de entrada eletrônica do destinatário. A mensagem de recibo pode incluir o título da mensagem, o endereço de destino e a hora de envio. Ela também pode incluir (dependendo dos tipos de "indicadores" que forem providos e ativados no software de envio de correspondência) uma lista de todas as "estações" da Internet por onde a mensagem passou em rota até o sem destino. Esta forma de relatório está embutida em algumas das regras e protocolos os quais implementam o e-mail. Mais ainda, quando uma mensagem é enviada com uma requisição de "notificação de leitura", o programa de e-mail do destinatário pode enviar para o remetente uma notificação de e-mail que o destinatário abriu aquela mensagem para leitura. Muitos clientes de correio eletrônico podem e realmente suportam este tipo de relatório; contudo, os protocolos da Internet não tornam isso mandatário.

[004] Entretanto, isso não significa que um e-mail enviado com uma requisição de notificação é tão efetivo em todos os aspectos quanto uma correspondência registrada. As pessoas certificam e registram cartas porque elas desejam uma prova de envio, por exemplo, uma prova que pode ser usada em um processo civil ou criminal, ou uma prova que satisfará a um supervisor ou a um cliente ou a uma agência governamental quanto a uma mensagem ter sido enviada, um serviço ter sido feito, um pedido feito, ou uma exigência de contrato satisfeita.

[005] Um recibo de registro do Serviço Postal Americano (USPS)

constitui uma prova de envio, porque a USPS o suporta. O recibo representa a confirmação do Serviço Postal que a carta ou a embalagem em questão foi realmente enviada para o endereçado ou por seu representante autorizado. Por outro lado, com o recibo de e-mail existem vários obstáculos para que um recibo de e-mail seja admitido e confiado como uma evidência persuasiva em um tribunal como prova de que a mensagem foi enviada. Ao final, o recibo pode ser apenas uma outra mensagem de e-mail que poderia ter sido alterada ou criada por qualquer um, em qualquer momento.

[006] Existe uma necessidade de um sistema de e-mail e/ou um método que possa prover uma prova confiável do conteúdo e do envio de uma mensagem de e-mail, de modo a tirar vantagem mais plena da conveniência e do baixo custo de uma comunicação via e-mail.

[007] Para se adequar a esta necessidade, alguns sistemas foram estabelecidos, por meio dos quais os remetentes podem receber uma prova de terceiros do envio pelo engajamento em serviços, por meio dos quais:

[008] o remetente transmite uma mensagem eletrônica a terceiros juntamente com uma lista dos remetentes pretendidos do documento;

[009] os terceiros enviam uma notificação para cada um dos remetentes pretendidos da mensagem, convidando-os a visitar o website dos terceiros, onde uma mensagem pode ser vista.

[0010] se o destinatário pretendido visitar o website dos terceiros, para ver a mensagem, os terceiros registram sua visita, de modo que o remetente pode saber que sua mensagem foi lida pelo destinatário.

[0011] Os inconvenientes desses sistemas são múltiplos. Em primeiro lugar, eles se baseiam essencialmente na cooperação do destinatário do e-mail para coletar suas mensagens a partir do serviço de terceiros. Mas as circunstâncias nas quais o remetente pode desejar

uma prova de envio de uma mensagem, frequentemente, são aquelas nas quais não pode ser assumido que o destinatário pretendido cooperará no recebimento da mensagem. Nesses casos, por exemplo, quando o reconhecimento do recibo da mensagem imporia um encargo financeiro ou legal no destinatário, o destinatário, simplesmente, pode ignorar a notificação de que a correspondência está disponível para ele receber. Note que não há nada nesse sistema que garanta que o destinatário pretendido recebeu a notificação de correspondência esperando. Em segundo lugar, sistemas como esses são trabalhosos e lentos de se usar, se comparados com o e-mail regular, à medida que eles podem requerer que o remetente e/ou o destinatário se conecte a um sítio da Rede Mundial para enviar, coletar e verificar o envio de cada mensagem. Mais ainda, a transmissão de documentos por métodos como esse pode requerer que o remetente e o destinatário transfiram e baixem arquivos para um website. Finalmente, devido ao fato de esses métodos requererem que os terceiros retenham uma cópia do todo de cada mensagem, até o momento em que elas forem coletadas ou expiradas, os métodos podem requerer que seu provedor devote recursos computacionais substanciais ao armazenamento de dados e à trilhagem de dados, por um período de tempo extenso. Como um método alternativo de provisão de prova de envio, alguns sistemas proveem plug-ins de clientes de e-mail proprietários ou de navegador da web, que notificarão aos remetentes quando uma mensagem tiver sido recebida, desde que um destinatário use o mesmo cliente de e-mail. A desvantagem óbvia desses sistemas é que eles requerem que o remetente e o destinatário usem o mesmo cliente de e-mail.

[0012] Portanto, existe uma necessidade de um sistema / método de e-mail que possa prover uma prova confiável do conteúdo e do envio de mensagens eletrônicas, o qual não requeira a cumplicidade ou a

cooperação do destinatário, o qual não requeira um software de e-mail especial da parte do remetente ou de destinatário, o qual opere com a mesma ou com aproximadamente a mesma conveniência e a velocidade de uso que o e-mail convencional, e o qual possa ser operado economicamente por um provedor de serviços.

Sumário da Invenção

[0013] Um objetivo geral da presente invenção é prover um sistema e um método para a verificação confiável, através de uma documentação segura e à prova de violação, do conteúdo e do envio de uma mensagem eletrônica, tal como um e-mail. De modo ideal, a invenção proporcionará a um e-mail e a outras mensagens eletrônicas um status legal emparelhado, se não superior, àquele do correio registrado americano. Entretanto, não é necessário para a invenção que qualquer status legal seja acordado às mensagens enviadas de acordo com os métodos ensinados aqui, uma vez que a invenção provê informação útil e verificação independentemente disso.

[0014] A presente invenção inclui um sistema de mensagem eletrônica que cria e registra uma assinatura digital de cada mensagem eletrônica enviada através do sistema. Um originador pode enviar uma cópia da mensagem eletrônica para o sistema ou gerar a mensagem eletrônica no sistema em si. O sistema, então, faz seguir e envia a mensagem eletrônica para todos os destinatários (ou para os manipuladores de mensagem designados associados aos destinatários), incluindo endereçados "para" e endereçados "com cópia". Após isso, o sistema retorna um recibo de envio para o originador da mensagem eletrônica. O recibo inclui, dentre outras coisas: a mensagem original, a assinatura digital da mensagem e um histórico de intercâmbio de indicativos e sinais de controle e de envio, incluindo os horários de envio para os destinatários. Para se verificar e autenticar, mais tarde, uma informação contida no recibo, o originador ou o usuário envia uma có-

pia do recibo para o sistema. O sistema, então, verifica se a assinatura digital combina com a mensagem original e o resto do recibo. Se os dois combinarem, então, o sistema envia uma carta ou provê uma outra confirmação de autenticidade, verificando se a mensagem eletrônica não foi alterada.

[0015] O sistema pode ser uma forma de servidor de e-mail conectado à Internet, o qual pode ser utilizado de muitas formas. Por exemplo, os usuários individuais podem registrar as suas mensagens eletrônicas, tais como e-mails, enviando uma "cópia carbono" (cc:) para o sistema ou compondo a mensagem no sistema em si. Para usuários corporativos ou de comércio eletrônico, estes usuários podem mudar seu servidor para um servidor que incorpore a presente invenção e tenha todas as suas mensagens eletrônicas externas registradas, com a opção de ter o sistema retendo e arquivando os destinatários. O sistema pode aceitar e verificar as mensagens eletrônicas encriptadas e gerenciar as mensagens eletrônicas em e/ou fora de uma "barreira de proteção". Para usuários baseados na web, isto é, indivíduos ou corporações que usam e-mails baseados na web, tais como MSN Hotmail® ou do Yahoo Mail®, tais usuários poderiam marcar uma caixa ou, de outra forma, regular um indicador nos seus programas de e-mail para seleção em uma base caso a caso quanto a registrar os e-mails e/ou arquivar as mensagens usando o presente sistema.

[0016] A assinatura digital pode ser criada usando-se técnicas de assinatura digital conhecidas, tal como pela execução de uma função de comprovação na mensagem, para a produção de um sumário de mensagem e, então, encriptando-se o sumário de mensagem. Assinaturas digitais separadas podem ser criadas para o corpo da mensagem, quaisquer anexos, e para a mensagem geral, incluindo o corpo, os anexos e os sumários de mensagem individuais. O sumário de mensagem encriptado provê um tipo de código de autenticação ou de

validação de mensagem, ou uma documentação segura. Outros códigos de autenticação e/ou de validação de mensagem também podem ser gerados e usados.

[0017] Em um aspecto, a invenção é um método de provisão de prova referente ao envio e ao conteúdo de uma mensagem eletrônica, compreendendo: o recebimento de um remetente através de uma rede de computadores de uma mensagem eletrônica, a mensagem tendo um endereço de envio associado a ela; a computação de um sumário de mensagem de acordo com a mensagem; a encriptação do sumário de mensagem; o envio da mensagem eletronicamente para um destino correspondente ao endereço de envio; a gravação do diálogo de Protocolo Simples de Transporte de Correio (SMTP) ou de SMTP Estendido (ESMTP), o qual efetua o envio da mensagem; o recebimento de uma informação de Notificação de Status de Envio associada à mensagem e ao endereço de envio; a provisão para o remetente de um recibo eletrônico, o recibo compreendendo: uma cópia da mensagem, o sumário de mensagem encriptado, as transcrições de (E)SMTP, e pelo menos um subconjunto da informação de notificação de Status de Envio, e, em uma data futura, o recebimento eletrônico do recibo eletrônico do remetente, verificar se o sumário de mensagem encriptado corresponde à mensagem, e verificar se a mensagem foi recebida por um manipulador de mensagem eletrônica associado ao endereço de envio.

[0018] Em um outro aspecto, a invenção é um método de verificação do envio de uma mensagem eletrônica, compreendendo: em um sistema de computador de rede de área ampla, o recebimento de uma mensagem eletrônica de um remetente de mensagem, para direcionamento para um endereço de destino; o estabelecimento de comunicações com um servidor de mensagem eletrônica associado ao endereço de destino, o servidor definindo um servidor de destino; a consul-

ta ao servidor de destino, para determinar se o servidor de destino suporta a funcionalidade de Notificação de Status de Envio (DSN); o recebimento de uma resposta à consulta, a consulta e a resposta em conjunto definindo um diálogo de SMTP; a requisição da informação de notificação de Status de Envio do servidor de destino, de acordo com os resultados do diálogo de SMTP; o recebimento da informação de DSN do servidor de destino em relação ao envio da mensagem eletrônica; e a provisão para o remetente da mensagem de pelo menos uma porção do diálogo de SMTP e de pelo menos uma porção da informação de DSN.

[0019] Ainda em um outro aspecto, a invenção é um método de verificação de conteúdo de uma mensagem eletrônica recebida, compreendendo: o recebimento da mensagem eletrônica; a geração de uma assinatura digital correspondente ao conteúdo da mensagem recebida; a provisão da mensagem e da assinatura digital para um endereçado designado; e, em um tempo posterior, verificar se a assinatura digital corresponde à mensagem.

[0020] De acordo ainda com um outro aspecto da presente invenção, o método inclui estabelecer se uma mensagem foi eletronicamente recebida por um destinatário, compreendendo: prover uma mensagem para ser despachada eletronicamente juntamente com um endereço de destinatário a partir de um remetente; a criação de uma assinatura em associação com a mensagem; o despacho da mensagem eletronicamente para o endereço de destinatário; a trilhagem da mensagem, para determinar o Status de Envio final da mensagem despachada para o endereço do destinatário; ao receber o Status de Envio final da mensagem, a geração de um recibo, o recibo incluindo uma cópia da mensagem, a assinatura e o de Envio final para a mensagem; e a provisão do recibo para o remetente, para posterior estabelecimento de que a mensagem foi eletronicamente recebida pelo destinatário.

[0021] De acordo ainda com um outro aspecto da presente invenção, é provido um método para prover que uma mensagem eletrônica enviada para um destinatário tenha sido lida, compreendendo: a provisão de uma mensagem eletrônica juntamente com um endereço de destinatário; o cálculo de uma assinatura digital correspondente à mensagem eletrônica; o despacho da mensagem eletrônica eletronicamente para o endereço do destinatário; a requisição de uma notificação de Agente de Usuário de Correio ("leitura" de cliente de e-mail) do destinatário; ao receber a notificação de leitura, a geração de um recibo de leitura, o recibo de leitura incluindo uma cópia da mensagem, a assinatura digital para a mensagem eletrônica correspondente, e uma segunda assinatura digital para o recibo de leitura a partir do destinatário; e a provisão do recibo de leitura para posterior verificação de que a referida mensagem foi recebida pelo destinatário.

[0022] De acordo com um outro aspecto da presente invenção, é provido um método para validação da integridade de uma cópia com significado de uma mensagem eletrônica, compreendendo: o recebimento da cópia de mensagem eletrônica com significado, a referida cópia com significado incluindo um sumário de mensagem encriptado associado a ela; a desencriptação do sumário de mensagem; a geração de um segundo sumário de mensagem baseado no conteúdo da cópia com significado; e validação da cópia com significado por uma comparação do sumário de mensagem desencriptado e do segundo sumário de mensagem, para se determinar se os dois sumários de mensagem combinam.

[0023] De acordo ainda com um outro aspecto da presente invenção, é provido um método para a validação de um e-mail registrado recebido, compreendendo: o recebimento de um recibo eletrônico, o referido recibo incluindo uma mensagem de base e um sumário de mensagem encriptado; a desencriptação do sumário de mensagem

encriptado; a geração de um segundo sumário de mensagem a partir da mensagem de base; e validação do e-mail, se o sumário de mensagem desencriptado combinar com o segundo sumário de mensagem.

[0024] Ainda em um outro aspecto, a invenção é de um website, para o qual os usuários podem ir para o envio e o recebimento de mensagens seguras, com a central do website atuando como um terceiro independente, o qual enviará e receberá as mensagens e proverá uma documentação segura referente ao conteúdo e ao envio das mensagens.

[0025] Os objetivos descritos acima da presente invenção e outros aspectos e benefícios da presente invenção se tornarão claros para aqueles versados na técnica quando lidos em conjunto com a descrição detalhada a seguir de uma modalidade preferida ilustrativa e vistos em conjunto com os desenhos em anexo, nos quais números iguais se referem a partes iguais, e com as reivindicações em apenso.

Breve Descrição dos Desenhos

[0026] A descrição detalhada da modalidade preferida da invenção será feita com referência aos desenhos em anexo.

[0027] A figura 1 é um diagrama de sistema de uma primeira modalidade da presente invenção, na qual as mensagens de saída são registradas ao serem transmitidas por um Agente de Transporte de Correspondência especial (MTA).

[0028] As figuras 2A a 2F constituem um fluxograma representativo, para registro de um e-mail de saída, de acordo com a modalidade da figura 1.

[0029] A figura 3 é um diagrama de sistema de uma segunda modalidade da presente invenção, na qual os remetentes podem se dirigir a um Agente de Transporte de Correspondência, para a transmissão de mensagens selecionadas através de um MTA de registro separado.

[0030] A figura 4 é um diagrama de sistema de uma terceira modalidade da presente invenção, no qual cópias carbono (cc's) de mensagens de saída são enviadas para um servidor especial para serem registradas.

[0031] A figura 5 é um diagrama de sistema de uma quarta modalidade da presente invenção, na qual os usuários compõem mensagens de saída para serem registradas em um website designado.

[0032] A figura 6 é um diagrama de sistema de uma quinta modalidade da presente invenção, na qual os usuários podem enviar e-mails registrados e armazenar recibos a partir de dentro de um Agente de Usuário de Correio baseado na Web (MUA).

[0033] A figura 7 é um fluxograma para a validação de um recibo de e-mail registrado.

[0034] A figura 8 é um diagrama de sistema de uma modalidade da presente invenção, para registro de mensagens de entrada.

[0035] A figura 9 é um fluxograma para o registro de mensagens de entrada.

[0036] A figura 10 é um fluxograma para a validação das mensagens registradas recebidas.

[0037] A figura 11 é um diagrama de sistema que mostra um uso de exemplo da presente invenção por um negócio eletrônico para registrar e reconhecer comunicações de entrada e de saída.

Descrição Detalhada da Invenção

[0038] Esta descrição não deve ser tomada em um sentido limitativo, mas é feita meramente com a finalidade de ilustração dos princípios gerais da invenção. Os títulos da seção e a organização geral da presente descrição detalhada são para fins de conveniência apenas e não são pretendidos para limitarem a presente invenção. Assim sendo, a invenção será descrita em relação a sistemas de envio de mensagem de e-mail, que usam a arquitetura e a infraestrutura de rede da

Internet. Deve ser compreendido que o tipo de mensagem em particular e a arquitetura de rede descritos aqui são para ilustração apenas; a invenção também se aplica a outros protocolos de mensagem eletrônica e tipos de mensagem, usando outras arquiteturas de rede de computadores, incluindo redes com fio e sem fio. Por conveniência de discussão, as mensagens que são processadas de acordo com a presente invenção podem ser referidas aqui como sendo mensagens "registradas". Na discussão que se segue, o termo "RPost" se referirá, em termos gerais, a uma entidade de terceiros, a qual cria e/ou opera um software e/ou um hardware que implementa a presente invenção, e/ou atua como um verificador de mensagem de um terceiro desinteressado. O termo é usado para conveniência de discussão apenas, e não deve ser compreendido como limitando a invenção.

Modalidade de RPOST como Servidor de Correio de Saída

[0039] A figura 1 é um diagrama de sistema de uma primeira modalidade da presente invenção, onde e-mails de saída são registrados de acordo com a presente invenção. Nesta modalidade, o servidor de registro RPost 14 serve como um Agente de Transporte de Correspondência especial (MTA) para um Agente de Usuário de Correio (MUA) 13 de um remetente de mensagem. Embora o destinatário de mensagem 18 seja, tecnicamente, o endereçado e, portanto, é meramente o destinatário pretendido ou o destino pretendido neste ponto no tempo, por simplicidade de discussão, esta entidade será referida aqui como o destinatário, o endereçado ou o destino. Note que uma mensagem única pode ter muitos destinos diferentes e que cada um desses pode ser atingido através de um MTA diferente.

[0040] O método de envio de mensagens registradas pode ser dividido em três partes:

[0041] *Pré-processamento*: etapas as serem realizadas antes de uma mensagem ser transmitida;

[0042] *Transmissão*: o método de envio de mensagens para os endereçados;

[0043] *Pós-processamento*: partículas para a acumulação de informação sobre as mensagens, após o seu envio, a criação de recibos e a validação de recibos.

I.1 Pré-processamento

[0044] Ao receber uma mensagem para transmissão, o servidor RPost criará registros em um banco de dados para cada mensagem que será usada para armazenamento de tal informação tal como:

[0045] o horário no qual a mensagem foi recebida;

[0046] os nomes dos anexos da mensagem;

[0047] o número de endereços da mensagem;

[0048] Para cada destino da mensagem, o banco de dados registrará:

[0049] o nome do destino (se disponível);

[0050] o endereço na Internet do destino;

[0051] o horário no qual a mensagem foi enviada para o Servidor de Correio de destino;

[0052] O *Status de Envio* deste destino.

[0053] Os Status de Envio de Destinatário usados pelo sistema incluirão:

NÃO ENVIADA

[0054] Este status indica que a mensagem não foi enviada.

ENVIADA E ESPERANDO POR DSN

[0055] Este status indica que a mensagem foi enviada para um ESMTP conforme com MTA, que suporta uma Notificação de Status de Envio (DSN), de modo que uma notificação de sucesso/falha possa ser esperada.

ENVIADA

[0056] Este status significa que a cópia da mensagem enviada pa-

ra este destinatário foi enviada de forma bem sucedida para um servidor que não suporta uma DSN de ESMTP.

ENVIADA PARA CAIXA DE CORREIO

[0057] Este status significa que uma mensagem de DSN foi recebida, a qual indica que a cópia da mensagem enviada para este destinatário foi enviada para a caixa de correio do destinatário.

RETRANSMITIDA

[0058] Este status significa que uma DSN de MTA foi recebida, a qual indica que a cópia da mensagem enviada para este destinatário foi retransmitida para frente para um outro servidor.

NÃO ENVIÁVEL

[0059] Este status indica que depois de repetidas tentativas RPost foi incapaz de se conectar a um MTA para enviar as mensagens para este destinatário.

FALHOU

[0060] Este status significa que uma DSN de MTA foi recebida, a qual indica uma falha no envio de uma cópia da mensagem para este destinatário.

[0061] Neste momento, o sistema também executará funções de comprovação no conteúdo da mensagem.

[0062] O servidor RPost 14 emprega uma função de comprovação e um algoritmo de encriptação. A função de comprovação pode ser qualquer uma das funções de comprovação bem conhecidas, incluindo MD2, MD5, o Algoritmo de Comprovação Segura (SHA), ou outras funções de comprovação, as quais possam ser desenvolvidas no futuro. Os algoritmos de comprovação e os métodos são descritos por Bruce Schneider, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, John Wiley & Sons, Inc. (Nova York) 1993; *Federal Information Processing Standard Publication 180-1 (FIPS PUB 180-1) Secure Hash Standard*, National Institute of Standards and Techno-

logy; e na Patente U.S. Nº 5.530.757, emitida para Krawczyk, intitulada "Distributed Fingerprints for Information Integrity Verification", os quais, desse modo, são incorporados aqui como referência por seus ensinamentos de funções de comprovação, encriptação, e métodos e sistemas para a implementação daquelas funções. Outros métodos conhecidos e novos de detectar se o conteúdo da mensagem foi alterado ou não podem ser usados.

[0063] Uma boa função de comprovação H é de uma via; isto é, é difícil de inverter, onde "difícil de inverter" significa que dado um valor de comprovação h, é computacionalmente impossível encontrar alguma entrada x de modo que H(x) = h. Mais ainda, a função de comprovação deve ser pelo menos fracamente sem colisão, o que significa que, dada uma mensagem x, é computacionalmente impossível encontrar alguma entrada y de modo que H(x) = H(y). A consequência disto é que um possível falsificador que conhecesse o algoritmo usado e o valor de comprovação resultante ou o sumário de mensagem, não obstante, não seria capaz de criar uma mensagem falsificada que se comprovasse com o mesmo número. O valor de comprovação h retornado por uma função de comprovação, geralmente, é referido como um sumário de mensagem. O sumário de mensagem é referido, às vezes, como uma "impressão digital" da mensagem x. Atualmente, é recomendado que funções de comprovação de uma via produzam saídas que tenham pelo menos 128 bits de comprimento, de modo a garantir que os resultados sejam seguros e não falsificáveis. Conforme o estado da arte atual avança, o comprimento recomendado para funções de comprovação seguras pode aumentar.

[0064] O servidor RPost 14 computa um sumário de mensagem para o corpo da mensagem e um sumário de mensagem separado para cada um dos anexos da mensagem, e os armazena de uma manei-

ra pela qual eles possam ser incluídos, mais tarde, em um recibo para a mensagem.

[0065] Antes de a mensagem ser alterada das formas que um registro requereria, uma cópia da mensagem original e de seus anexos é armazenada de uma maneira pela qual ela possa ser recuperada, mais tarde, pelo sistema.

[0066] O servidor RPost pode alterar uma mensagem de várias formas, antes de uma transmissão para o MTA do destinatário.

[0067] Embora isso não seja necessário para a prática da invenção, a mensagem pode ser rotulada, para denotar o fato de que a mensagem foi registrada, tal como pela inserção da palavra "Registrado" ou no começo da linha de "assunto" da mensagem, pelo acréscimo de um rótulo tal como:

[0068] "Esta mensagem foi registrada com RPost. Visite nosso website em www.RPost.com para informações adicionais."

[0069] ao final da mensagem original ou uma outra rotulagem. Adicionalmente, o rótulo pode conter instruções, os endereços da Rede Mundial, ou links que convidem e permitam que o destinatário envie uma resposta registrada para a mensagem por meio de um link com a página da web a partir da qual mensagens registradas podem ser compostas e enviadas.

[0070] Embora a rotulagem seja opcional, a mensagem enviada, geralmente, será referida aqui como a mensagem rotulada.

[0071] Os protocolos de Internet proveem duas formas de recibo para mensagens de e-mail:

NOTIFICAÇÕES DE MTA

[0072] Estas são e-mails que são enviados por um MTA de destinatário notificando o remetente nominal da mensagem que vários eventos ocorreram. Os MTAs que se conformam ao protocolo SMTP, tipicamente, apenas enviarão uma notificação no evento de o encarre-

gado do envio de correspondência não possa enviar uma mensagem para a caixa de correio do endereçado (como poderia acontecer se o endereço não fosse válido ou se a caixa de correio do endereçado tivesse excedido sua quota de armazenamento alocada).

[0073] Com a introdução do padrão SMTP Estendido, se tornou possível o envio de MTAs para requisição de notas de sucesso e falha no envio de mensagens. Essas Notificações de Status de Envio (DSNs) são e-mails, os quais são enviados por um MTA de recebimento para o remetente nominal da mensagem, quando certos eventos ocorrerem: por exemplo, a mensagem foi depositada com sucesso na caixa de correio do destinatário; a mensagem não pode ser enviada para a caixa de correio do destinatário por alguma razão; a mensagem do destinatário foi retransmitida para um outro servidor, o qual não dá recibos de DSN.

[0074] Note que apenas quando servidores que suportam o protocolo SMTP Estendido (ESMTP) suportam esta forma de DSN e que um suporte para esta função é opcional para servidores de ESMTP e depende da configuração selecionada pelos administradores do servidor.

[0075] Embora a DSN seja um termo que apenas veio a uso com o advento de ESMTP, usaremos, no que se segue, 'DSN' para se referir a qualquer mensagem gerada por MTA referente ao status de uma mensagem recebida, independentemente de estar ou não em conformidade com o protocolo ESMTP.

NOTIFICAÇÕES DE MUA (NOTIFICAÇÕES DE LEITURA)

[0076] Estes são e-mails que são enviados para o autor (nominal) de uma mensagem pelo Agente de Usuário de Correio (MUA) do destinatário (programa de e-mail), quando certos eventos ocorrerem: por exemplo, a mensagem é aberta para leitura, ou apagada do sistema sem ter sido lida. Pela convenção da Internet (RFC 1891), nenhum

programa de MUA pode ser forçado a gerar essas notificações. Se um MUA gerará esses recibos dependerá da configuração escolhida por seu usuário.

[0077] O servidor RPost 14 configurará e transmitirá mensagens em uma forma que tenta eliciar as DSNs de MTA e as notas de MUA a partir de MTAs e MUAs conformes. De modo a eliciar um Recibo de Leitura de MUAs conformes, certos cabeçalhos devem ser incluídos na seção de cabeçalho de uma mensagem de e-mail. MUAs diferentes respondem a cabeçalhos diferentes; assim, o Servidor 14 adicionará vários cabeçalhos diferentes a cada mensagem requisitando uma notificação de leitura em uma forma reconhecida por vários MUAs. Todos esses cabeçalhos tomam a forma:

[0078] Header label: user name <user address>

[0079] Por exemplo:

[0080] Disposition-notification-to: john smith jsmith@adomain.com>

[0081] read-notification-to: john smith <jsmith@adomain.com>

[0082] onde 'john smith' é o nome do usuário a quem uma notificação de MUA deve ser enviada e '<jsmith@adomain.com>' é o endereço na Internet daquele usuário. Normalmente, esses cabeçalhos se referirão ao autor da mensagem, mas no caso do presente método, é requerido que a notificação seja retornada para o RPost, de modo que a notificação possa ser processada por RPost. Para assegurar que isso seja assim, o Servidor 14 inserirá cabeçalhos que requisitem que recibos de MUA sejam enviados para um endereço, onde eles podem ser processados pelo servidor Rpost, por exemplo, "readreceipt@RPost.com". Isso dirigirá quaisquer MUAs de destinatário conforme para enviarem suas notificações para um endereço de RPost para processamento.

[0083] A tarefa de processamento de notificações de MUA retor-

nadas cria um outro problema, que deve ser considerado neste estágio. Não há normas que governem o formato ou o conteúdo de notificações de MUA. Frequentemente, eles citarão o assunto da mensagem original e o horário do evento (por exemplo, "aberto para leitura") que eles estiverem reportando. Mas, mesmo se esta informação for incluída na notificação, raramente é suficiente para identificar de forma única a mensagem que o orienta ou identificar o autor daquela mensagem. Quando o sistema recebe uma notificação de MUA, ele deve ser capaz de identificar a mensagem que o orienta, de modo a incluir a informação de notificação no recibo que o RPost gerará para o remetente. Alternativamente, o sistema deve pelo menos ser capaz de identificar de forma confiável o remetente da mensagem à qual a notificação de MUA se refere, de modo que a informação de notificação possa ser passada para o remetente na forma de um recibo de leitura de RPost (veja abaixo).

[0084] Para realizar a última meta, o sistema pode tirar vantagem do fato de os endereços internos terem dois componentes: um campo de nome e um campo de endereço, onde o campo de endereço é limitado pelos sinais de citação de canto "<>". A maioria dos MUAs incluirá ambos os campos no endereço de destino de suas notificações de MUA. Na composição de suas requisições por recibos de MUA, o sistema RPost incluirá o Servidor 14 ler o endereço de manipulação de recibo como o endereço para a notificação, mas usar o *endereço* do remetente original no nome do campo do cabeçalho. Por exemplo, quando o remetente original da mensagem é o usuário John Smith com endereço da internet jsmith@adomain.com, o servidor RPost incluirá cabeçalhos da forma:

[0085] Disposition-notification-to: jsmith@adomain.com <readreceipts@Rpost.com>

[0086] Isso resultará, tipicamente, no MUA conforme enviar uma

notificação para readreceipts@RPost.com, endereçada como: jsmith@adomain.com <readreceipts@Rpost.com>

[0087] Ao receber uma notificação como essa no endereço "readreceipts@RPost.com", o servidor apenas pode, ao analisar gramaticalmente o campo do endereçado, determinar que a notificação concerne a uma mensagem originalmente enviada por *jsmith@adomain.com*, mesmo se isto não pudesse ser determinado por qualquer exame do conteúdo da notificação. Com esta informação a mão, o servidor, então, pode empacotar o conteúdo da notificação em um recibo de Leitura de RPost assinado digitalmente e enviar o recibo para o endereço jsmith@adomain.com.

[0088] O sistema RPost também se empenhará para eliciar e coletar notas de DSN de MTA geradas pelos MTAs de destinatário. Uma vez que essas notificações sempre são enviadas para o endereço listado no campo "DE:" do cabeçalho da mensagem, o servidor 14 deve alterar cada cabeçalho de mensagem de modo que seja recebido como "DE:" de um endereço RPost no qual as DSNs possam ser processadas.

[0089] Entretanto, o problema de processamento de DSNs levanta uma outra questão, a qual deve ser considerada neste estágio. As DSNs não têm um conteúdo ou um formato padrão; frequentemente, é impossível determinar, meramente pelo exame do conteúdo desses e-mails, de que mensagem seus conteúdos estão dando notificação. Este problema foi supostamente endereçado por DSNs geradas em conformidade com o protocolo ESMTP, pelo uso de números de ID de envoltória de DSN (veja a RFC 1869). De acordo com o protocolo, um MTA de transmissão pode incluir um número de referência juntamente com sua requisição por uma DSN. Este número seria citado em qualquer DSN de retorno, permitindo ao remetente identificar a mensagem em questão da DSN. Entretanto, de fato, muitos MTAs que reportam a

si mesmos como suportando DSN de ESMTP não retornam uma ID de envoltória de DSN ou qualquer outra informação suficiente para identificar, de forma confiável a mensagem em questão. Finalmente, mesmo quando uma DSN não retorna informação suficiente para identificar a mensagem de que está dando notificação, frequentemente, ela não conterá informação suficiente para identificar o endereçado específico da mensagem que orientou a notificação. Assim, uma mensagem única poderia ser enviada para dois endereçados em um domínio; uma poderia ser enviada com sucesso para a caixa de correio do endereçado; a outra não. O MTA para o domínio pode reportar esses eventos em uma DSN em formas que não proveem um caminho para o destinatário da DSN determinar para qual endereçado foi enviada com sucesso e para qual não foi (como, por exemplo, pode ocorrer se a DSN reportar os endereços do remetente como seus nomes alternativos locais ao invés de por seus endereços contidos na mensagem original).

[0090] A presente invenção resolve este problema em quatro etapas:

[0091] Um número de identificação único é gerado para cada mensagem de saída (por exemplo, baseado em um selo de tempo). Este número é armazenado em um banco de dados.

[0092] Os destinatários de cada mensagem são enumerados e os números de identificação são armazenados em um banco de dados.

[0093] A mensagem é enviada separadamente para cada MTA de destinatário pretendido (mesmo quando dois destinatários têm um nome de domínio comum e um MTA, o servidor 14 transmitirá a mensagem para aquele MTA em duas sessões de telnet de SMTP separadas).

[0094] Quando o Servidor 14 transmite a mensagem para um MTA de destinatário, ele aumenta o campo "DE" da mensagem, para mos-

trar a mensagem como tendo sido enviada a partir de um endereço o qual incorpora a ID única da mensagem e o número de identificação do remetente. O endereço também contém uma subsérie (por exemplo, "rcpt"), que permite que o Servidor identifique mensagens de retorno como DSNs.

[0095] Assim, uma mensagem única denominada "mmyyddss" pelo Servidor 14, a partir do remetente denominado John Smith, poderia ser enviada para seu primeiro destinatário (denominado "a" pelo sistema) com uma leitura de cabeçalho:

[0096] From: John Smith <rcptmmddyyssa@RPost.com>

[0097] A mesma mensagem seria enviada para o segundo destinatário com uma leitura de cabeçalho:

[0098] From: John Smith <rcptmmddyyssb@RPost.com>

[0099] Muitos MUAs de e-mail apenas exibem o nome do remetente de uma mensagem e, assim, o endereço especial será invisível para a maioria dos destinatários.

[00100] O desfecho desta forma de endereçamento é que quando os MTAs do destinatário emitem DSNs (independentemente de conformes com o ESMTP ou não), eles endereçarem aquelas DSNs a endereçados de RPost diferentes. Ao receber essas DSNs, o Servidor 14 pode identificá-las como mensagens de DSN por seu prefixo "RCPT" e, pela análise gramatical dos endereçados, pode determinar qual mensagem e qual destinatário são o assunto da DSN.

[00101] O sistema 14 alterará o campo 'DE' de cada mensagem para se referir a um destinatário da mensagem a cada vez que ele tentar transmitir a mensagem para o MTA daquele destinatário.

[00102] Para garantir que as respostas do destinatário a mensagens transmitidas sejam dirigidas apropriadamente, o sistema 14 adiciona um cabeçalho de mensagem explícito "responder para:" na mensagem listando o nome do remetente original e o endereço na Internet.

No caso do presente exemplo, este seria:

[00103] Reply-to: john smith <jsmith@adomain.com>

[00104] Isso levará os MUAs de destinatário a respostas de endereço a uma mensagem recebida para o endereço do remetente real, ao invés do endereço de RPost construído.

I.2 Transmissão

[00105] Como notado acima, é parte do método que o servidor RPost transmita uma cópia separada de uma mensagem de saída para cada endereçado daquela mensagem. Mais ainda, o RPost tentará fazer um envio como esse através de uma conexão de SMTP direta com um trocador de correio (MX) de registro para cada destino.

[00106] Nota: cada endereço de e-mail válido da Internet inclui um nome de domínio da Internet ou um endereço de IP. Cada nome de domínio / endereço tem associado a ele um servidor de e-mail autorizado para receber correspondência para endereços naquele domínio. Será notado que alguns domínios têm mais de um servidor. O Servidor de Nome de Domínio responsável por cada domínio difunde a identidade de seus servidores de correio através da Internet. Esta informação está publicamente disponível e é gerenciada e transmitida em formas que se conformam às regras e convenções as quais governam o e-mail na Internet e o serviço de Nome de Domínio.

[00107] Antes de transmitir uma cópia da mensagem para qualquer destino, o servidor RPost executará uma Consulta de Servidor de Nome da Internet, para identificar um MTA associado ao domínio de destino. Tendo identificado o MTA responsável pelo recebimento da correspondência em nome do endereço de destino, o sistema tentará abrir uma conexão de telnet com o MTA local do destino.

[00108] É prática comum que os e-mails da Internet sejam retransmitidos de MTA para MTA até atingirem seu destino final. A finalidade primária de requerer uma conexão direta entre o servidor RPost e o

MTA de destino é para que o servidor RPost possa registrar o envio da mensagem (este registro tomando a forma de um diálogo de SMTP) com o servidor de e-mail, o qual tem responsabilidade proprietária quanto ao recebimento de e-mail para o nome de domínio de destinatário.

[00109] A existência deste registro provê evidência útil de que a mensagem foi enviada, muito da mesma forma que um recibo de correspondência registrada provê evidência de envio. A correspondência Registrada do USPS é tratada como enviada de forma verificada se puder ser provado que ela foi enviada para o agente autorizado do endereçado (por exemplo, uma secretária ou um funcionário atendente de sala de correspondência). No caso de qualquer desafio legal ao mérito de evidência de um recibo de envio de RPost, será reconhecido que na seleção do provedor de serviços de e-mail na Internet, o destinatário autorizou aquele provedor a coletar mensagens eletrônicas em seu nome. Por sua vez, aquele provedor de serviços tem reconhecido seu status como agente autorizado para destinatário de e-mail daquele nome de domínio pela difusão do endereço de seus MTAs como os servidores de e-mail de recepção para seu domínio.

[00110] Assim sendo, tendo as mensagens enviadas diretamente para o servidor de correio responsável pelo recebimento do e-mail do destinatário, o RPost terá enviado a mensagem para um agente que o destinatário legalmente autorizou a receber sua correspondência. Pelo registro da transação de envio (aquela transação tomando a forma de um diálogo de SMTP), o RPost pode reivindicar ter prova de envio para o agente autorizado do destinatário.

[00111] Note que, embora o método descrito aqui tente coletar outras formas de prova de envio para cada destino, se essas tentativas são bem sucedidas ou não dependendo de fatores que não estarão sob o controle do RPost (por exemplo, a forma de suporte de SMTP

empregado no servidor de correio do destinatário). Por outro lado, todo envio bem sucedido dirigido a um servidor de correio de destinatário sempre gerará um registro de SMTP. A gravação deste registro permite que o RPost proveja prova de envio para qualquer destino de Internet válido que se conforme com os protocolos mínimos (SMTP) para correio da Internet. Isso representa uma vantagem importante do método atual em relação a outros métodos que poderiam tentar provar o envio por confiança em DSN de ESMTP.

[00112] Tendo identificado o MTA para um destino de uma mensagem, o servidor RPost tentará abrir uma conexão de ESMTP com o MTA de destino, emitindo um intercâmbio de indicativos e sinais de controle "EHLO" em conformidade com a RFC 1869. Se o SERVIDOR 16 suportar ESMTP, ele responderá listando quais serviços de ESMTP ele suporta.

[00113] Se o SERVIDOR 16 suportar ESMTP, o servidor RPost, primeiramente, determinará se o SERVIDOR 16 suporta o Serviço de ESMTP "VERIFICAR". O serviço Verificar permite que um servidor de SMTP chamando determine, dentre outras coisas, se um endereço em um domínio de MTA é genuíno. Se o servidor RPost determinar por esses meios que o endereço para o qual ele está tentando enviar sua mensagem não é válido, ele terminará a conexão, caracará de tentar enviar uma mensagem para este endereçado, e gravará em seu banco de dados o status deste destino de mensagem como NÃO ENVIÁVEL.

[00114] Qualquer que seja o seu resultado, o servidor RPost gravará o diálogo VERIFICAR ESMTP em um arquivo e o armazenará, de modo que ele possa ser anexado, mais tarde ou incluído no Recibo de Envio para esta mensagem. Deve ser notado que, fora da questão da segurança, poucos servidores de ESMTP suportam a função VERIFICAR.

[00115] Se o Sistema 16 não suportar o método VERIFICAR, então, o servidor RPost, não obstante, tentará enviar a mensagem para o Sistema 16. Tipicamente, um MTA aceitará mensagens para qualquer endereço nominalmente em seu domínio e, mais tarde, enviará uma DSN, se o endereço for inválido.

[00116] O servidor RPost, então, tentará determinar se o servidor de destino suporta a DSN de serviço de ESMTP. Se o fizer, o RPost transmitirá a mensagem com uma requisição para que o SERVIDOR 16 notifique o remetente da mensagem com uma DSN de ESMTP, se o envio para o endereçado for bem sucedido ou falhar. Após a transmissão bem sucedida da mensagem para este destino, o sistema gravará o Status de Envio deste destino como ENVIADA E ESPERANDO POR DSN.

[00117] Se o Servidor 16 responder ao intercâmbio de indicativos e sinais de controle "EHLO" de uma forma que indique que ele não suporta o ESMTP, o servidor RPost emitirá uma mensagem "HELO", para iniciar uma conexão de SMTP. Se esta conexão for obtida, o servidor RPost transmitirá a mensagem em conformidade com o protocolo de SMTP e gravará o Status de Envio do destino como ENVIADA.

[00118] Independentemente de a conexão ser SMTP ou ESMTP, o servidor RPost gravará todo o diálogo de protocolo entre os dois servidores. Tipicamente, este diálogo incluirá mensagens de protocolo, nas quais, dentre outras coisas, o servidor de destino identifica a si mesmo, outorga permissão para a transmissão de uma mensagem para um destinatário denominado, e reconhece que a mensagem foi recebida. O RPost salvará o registro desta transação de forma que ele possa ser, mais tarde, recuperado e incluído ou anexado ao Recibo de Envio de RPost para esta mensagem.

[00119] Por várias razões, o RPost pode não ser capaz de obter uma conexão de SMTP com um MTA de um destinatário, ou pode ob-

ter esta conexão mas ter negada uma permissão para transmitir a mensagem pelo destinatário. Nesse caso, se a consulta de DNS da Internet revelar que o endereço de destino é servido por múltiplos MTAs, o servidor RPost tentará enviar sua mensagem para cada um deles de forma sucessiva. O RPost continuará a tentar enviar para um MTA apropriado tão frequentemente quanto os recursos do sistema permitirem. Se, após uma extensão de tempo, o RPost não puder enviar a mensagem para um endereço, ele marcará o status deste destinatário desta mensagem como "NÃO ENVIÁVEL", e parará de tentar enviar esta mensagem para seu endereço de destino.

[00120] Quando o servidor RPost é bem sucedido na transmissão de uma mensagem para um Servidor de destino que explicitamente suporta DSN de ESMTP, o RPost gravará o status deste destinatário para esta mensagem como "ENVIADA E ESPERANDO POR DSN".

[00121] Quando o servidor RPost é bem sucedido na transmissão de uma mensagem para o Servidor de destino através de uma conexão que não suporta explicitamente DSN de ESMTP, o RPost gravará o status deste destinatário para esta mensagem como "ENVIADA".

I.3 PÓS-PROCESSAMENTO

Processamento de DSN

[00122] As DSNs de MTA serão retornadas para o servidor RPost endereçado para endereços fictícios em seu domínio proprietário (por exemplo, "RPost.com"), esses endereços tendo sido construídos como descrito acima. O servidor RPost varrerá toda a correspondência originada endereçada ao domínio e detectará mensagens de DSN por sua subsérie de identificação (por exemplo, "rcpt"). Pela análise gramatical desses endereços da maneira descrita acima, o sistema pode identificar a mensagem e o destinatário que orientou a notificação DSN.

[00123] Não há um formato padrão para mensagens de DSN; nem há qualquer léxico padrão no qual elas reportam seus resultados. Para

avaliar uma DSN recebida, o sistema deve olhar a linha de assunto e o corpo das mensagens de DSN palavras e frases que expressem o significado da DSN. Por exemplo, frases tais como "envio bem sucedido" ou "enviada para caixa de correio" ou "foi enviada" normalmente sinalizam que a mensagem a que o DSN concerne foi depositada na caixa de correio do destino. Quando ele detecta essas frases, o sistema mudará o Status de Envio deste destino da mensagem para "ENVIADA PARA CAIXA DE CORREIO".

[00124] Frases tais como "não pode ser enviada", "erro fatal", "falha" e "sem sucesso", tipicamente, sinalizam uma DSN que reporta uma falha pelo MTA no envio da mensagem para o destino. Quando ele detecta frases tais como estas na DSN, o sistema mudará o registro do Status de Envio do destinatário para "FALHOU".

[00125] Embora o sistema sempre envie uma correspondência a um MTA proprietário para o domínio de destino, esses MTAs, às vezes, retransmitirão a mensagem para um servidor diferente (como pode ser o caso, por exemplo, se o MTA de recebimento enviar um correio por trás de uma barreira de proteção). Neste caso, a DSN conterá frases tais como "retransmitida" ou "retransmitida para frente". Nesses casos, o sistema mudará o Status de Envio de destinatário para "RETRANSMITIDA".

[00126] Tendo avaliado a DSN e atualizado o Status de Envio de destinatário de modo conforme, o sistema salvará a DSN e quaisquer anexos que ela possa conter, de forma tal que esta(s) mensagem(ns) possa(m) ser incluída(s) e/ou anexada(s) a um Recibo de Envio de RPost.

Gerenciamento de Mensagem

[00127] De tempos em tempos, o sistema varrerá cada mensagem enviada e examinará o status de cada destino daquela mensagem, de modo a determinar se o sistema completou um processamento daque-

le envio de destino. Os critérios para completação dependerão do Status de Envio do destino:

[00128] ENVIADA: este status indica que uma cópia da mensagem para este destinatário foi enviada para um MTA que não suporta DSN ESMTP. Um MTA como esse, não obstante, pode enviar uma forma de Notificação de Status de Envio no caso de a mensagem não poder ser enviada para a Caixa de Correio do endereçado (ou poderia ocorrer, por exemplo, de o endereço de destino não corresponder a uma conta válida no domínio). Assim sendo, o sistema não tratará o envio para um destinatário como esse como completo, até um período de tempo ter decorrido desde o envio para o MTA do destinatário. Este período de tempo – tipicamente de duas a vinte e quatro horas – representa uma estimativa do tempo máximo requerido para a maioria dos servidores retornar uma notificação de uma falha de envio e pode ser ajustado, se o domínio de destino específico for remoto ou conhecido como sendo pronto ou tardio na produção dessas notificações.

[00129] RETRANSMITIDA: este status significa que uma DSN foi recebida, a qual indica que o MTA do destinatário enviou a mensagem para um outro MTA que não suporta uma DSN de ESMTP. Neste caso, não obstante, é possível que o MTA para o qual a mensagem foi enviada envie uma notificação de falha em enviar no curso devido. Assim sendo, destinatários com este status são tratados como completos sob as mesmas condições que os destinatários com o status ENVIADA.

[00130] ENVIADA E ESPERANDO POR DSN: este status indica que o MTA do destinatário suporta uma DSN de ESMTP e que uma DSN foi solicitada, mas ainda não foi recebida. Às vezes, pode acontecer de, embora um MTA identifique a si mesmo como suportando este serviço, ele, não obstante, não prover uma DSN, mesmo no caso de um envio bem sucedido. Assim sendo, o sistema considerará envi-

os para um destino com este status como completos, mesmo se nenhuma DSN for recebida após um intervalo de tempo. Este intervalo – tipicamente de seis a vinte e quatro horas – representa uma estimativa do tempo máximo tipicamente requerido para um MTA conforme retornar uma DSN.

[00131] ENVIADA PARA CAIXA DE CORREIO: este status indica que uma DSN indicando um envio bem sucedido foi recebida por este destinatário e, assim, o envio da mensagem para este destino está completo.

[00132] FALHOU, NÃO ENVIÁVEL: envios para destinatários com este status sempre são tratados como completos.

[00133] Quando o sistema descobre que o envio para todos os destinatários de uma mensagem foi completado, o sistema constrói um Recibo de Envio para a mensagem.

Criação de Recibos de Envio

[00134] Os recibos de envio são e-mails enviados para o remetente original da mensagem Registrada. O recibo 20 pode conter:

[00135] um identificador para fins administrativos. Este identificador pode ser ou pode incluir uma referência à ID do remetente e/ou o valor da ID de Mensagem da Internet da mensagem do remetente como recebida pelo sistema;

[00136] a data e a hora em que o recibo foi gerado;

[00137] o corpo citado da mensagem original juntamente com os endereços de e-mail de seus destinatários pretendidos;

[00138] a data e a hora nas quais o servidor RPost recebeu a mensagem;

[00139] uma tabela para cada listagem de destino:

[00140] o tempo no qual o MTA do destinatário recebeu a mensagem e/ou o tempo no qual o sistema recebeu um relatório de DSN do MTA do destinatário;

[00141] um Status de Envio da mensagem para aquele destino. O Status de Envio citado em um Recibo de Envio é baseado no registro interno do sistema do Status de Envio do destino. Eles podem ser transcritos como se segue:

[00142] envios para destinos cujo status seja FALHOU ou NÃO ENVIÁVEL serão registrados no recibo como "falhou".

[00143] envios para destinos cujo status seja ENVIADA ou ENVIADA E ESPERANDO POR DSN serão registrados no recibo como "enviada para servidor de correio".

[00144] envios para destinatários cujo status é ENVIADA PARA Caixa de correio serão registrados no recibo como "enviada para caixa de correio".

[00145] A finalidade desses relatórios é informar precisamente ao leitor a forma de verificação do envio que o sistema foi capaz de obter.

[00146] 6. uma lista dos anexos originais do e-mail juntamente com os sumários de mensagem separados daqueles anexos;

[00147] . cópias dos anexos à mensagem original, cada anexo original sendo anexado como um anexo ao recibo;

[00148] 8. transcrições, sumários ou abstrações das transcrições de todos os diálogos de SMTP envolvidos no envio da mensagem para cada destino;

[00149] 9. citações dos corpos e dos anexos de todos os relatórios de DSN recebidos, incluindo quaisquer detalhes de envio ou disposição da mensagem que eles pudessem revelar; e

[00150] 10. quaisquer arquivos que fossem retornados para o sistema como anexos aos relatórios de DSN.

[00151] Todos esses elementos separados do recibo podem ter seus próprios sumários de mensagem ou as assinaturas digitais incluídos no recibo. Adicionalmente, o recibo pode incluir um único sumário de mensagem encriptado geral ou uma assinatura digital computada e

anexada como parte do recibo, desse modo provendo um único código de autenticação de mensagem, o qual poderia ser usado para a autenticação de toda a informação contida no recibo. Uma vez que o recibo em si e os diálogos de SMTP e relatórios de DSN no recibo contêm selos de tempo, o recibo inclui um registro não forjável do(s) destinatário(s) da mensagem, do conteúdo da mensagem e do(s) horário(s) e da(s) rota(s) de envio.

Processamento de Notificação de MUA

[00152] As Notificações de MUA poderiam ser coletadas e incorporadas nos recibos de Envio de RPost da mesma maneira que as DSNs de MTA. Entretanto, as notificações de MTA, tipicamente, são emitidas pelos MTAs de recebimento em umas poucas horas de envio, ao passo que as Notificações de MUA não serão geradas, se o forem, até o destinatário abrir seu cliente de e-mail de MUA e fazer alguma ação em relação à correspondência recebida. Por esta razão, nesta modalidade da invenção, as notificações de MUA são coletadas separadamente das notificações de MTA e reportadas em "Recibos de Leitura de RPost" separados dos Recibos de Envio de RPost.

[00153] As notificações de MUA eliciadas pelos cabeçalhos de mensagem construídos da maneira descrita acima serão retornadas como um endereço de RPost comum (por exemplo, "readreceipts@RPost.com") e cada notificação conterá – no campo de nome de seu endereço – o endereço do remetente original desta mensagem. Devido ao fato de esta ser a única informação requerida para a geração de um recibo de leitura de RPost da maneira descrita abaixo, o sistema pode lidar com notas de MUA sempre que essas notas possam chegar, e sem qualquer necessidade de ter armazenada qualquer informação sobre a mensagem original em seus bancos de dados.

[00154] As notas de MUA podem relatar, dentre outras coisas, que uma mensagem foi lida por um destinatário, que uma mensagem foi

exibida no terminal do destinatário (independentemente de ser lida ou não), que uma mensagem foi apagada sem ter sido aberta. Não há um padrão governado por protocolo para o conteúdo ou o formato de mensagens de MUA. O sistema poderia ser configurado de modo a examinar o texto de MUAs para interpretar seus relatórios da mesma forma que o sistema usa para DSNs de MTA. Entretanto, na modalidade atual da invenção, os MUAs não são avaliados ou interpretados pelo servidor RPost, mas são, ao invés disso, passados para o remetente para sua própria avaliação em uma forma que possa ser autenticada por RPost. Para realizar isto, o sistema criará uma mensagem de e-mail marcada como uma "Nota de Leitura de RPost", a qual pode incluir, dentre outros itens:

[00155] uma linha de assunto da nota de MUA recebida;

[00156] o corpo da nota de MUA recebida citada como o corpo da Nota de Leitura;

[00157] a nota de MUA recebida incluída como um anexo;

[00158] quaisquer anexos à nota de MUA recebida incluídos como um anexo.

[00159] sumários de mensagem da nota de MUA recebida e quaisquer anexos àquela nota;

[00160] um selo de data e horário;

[00161] uma comprovação encriptada de pelo menos 5 e 6 itens provendo uma assinatura digital de selo de tempo autenticável para o documento e todo o seu conteúdo.

Disposição de Recibo

[00162] No caso da modalidade atual da invenção, ambos os recibos de envio de RPost e as Notas de Leitura são enviados para o remetente original da mensagem registrada. Uma vez que esses recibos são digitalmente assinados com uma comprovação encriptada, o RPost pode autenticar a informação contida nessas mensagens a

qualquer momento que sejam apresentadas para o RPost para esta finalidade, da maneira descrita abaixo. Isso significa que uma vez que tenha transmitido uma cópia do recibo para o seu remetente (com instruções para o remetente reter o recibo para seu registro), o RPost não tem nenhuma necessidade adicional de reter quaisquer dados concernentes à mensagem ou ao seu envio, e pode expurgar todos esses registros do seu sistema. Assim, o RPost não precisa manter qualquer cópia da mensagem original ou do recibo. Esta economia de memória de arquivo dá à presente invenção uma vantagem em relação a vários sistemas de autenticação de mensagem da técnica anterior, que requerem grande quantidade de armazenamento de dados no lado do provedor de serviços.

[00163] Neste caso, o encargo de reter os dados do recibo recai sobre o remetente original da mensagem. De forma alternativa ou adicional, um RPost de verificador de terceiros pode, talvez, por um honorário adicional, armazenar uma cópia permanente do recibo ou de alguns ou de todos os dados de recibo. O recibo ou parte(s) do mesmo pode(m) ser mantido(s) em quaisquer dispositivos de armazenamento de arquivo adequados, incluindo fita magnética, CD ROM, ou outros tipos de dispositivo de armazenamento. De forma adicional ou alternativa, o RPost pode retornar recibos ou partes dos mesmos para um sistema de armazenamento devotado a esta finalidade no controle do remetente ou da organização do remetente.

[00164] Como descrito acima, a informação de recibo de RPost inclui todos os dados da mensagem do remetente original e seus anexos. Há circunstâncias nas quais os usuários do sistema poderiam não desejar sofrer o encargo de reter recibos nos seus registros (por exemplo, medo de perda acidental de dados), mas também poderia não desejar ter o conteúdo da sua mensagem nas mãos de terceiros de RPost. Assim sendo, o RPost poderia descartar o conteúdo de men-

sagens, mas armazenar em seu banco de dados apenas essa uma informação (por exemplo, remetente, data de composição, sumários de mensagem, destinos e Status de Envio) tal como poderia ser requerido para o RPost autenticar e verificar o envio de uma mensagem, quando apresentado a uma cópia da mensagem retida pelo remetente.

Verificação

[00165] No caso de o originador de uma mensagem requerer uma evidência em uma data posterior de que um e-mail foi enviado, remetido e/ou lido, o originador apresenta o(s) recibo(s) para a mensagem aos operadores do sistema.

[00166] Por exemplo, de modo a provar que uma mensagem em particular foi enviada a partir do remetente 10 para o destinatário 18, o remetente 10 envia ao RPost uma cópia de recibo 20 com uma requisição para verificar a informação contida no recibo. Isso poderia ser feito pelo envio do recibo para uma caixa de correio predefinida no RPost, por exemplo, verify@RPost.com. O RPost, então, determina se o recibo é ou não um recibo válido. Um recibo é um recibo válido se a assinatura digital combinar com o restante do recibo, e os sumários de mensagem combinarem com as respectivas porções da mensagem original. Especificamente, o RPost executa uma função de comprovação nas várias porções das mensagens, incluindo o corpo da mensagem, os anexos e a mensagem geral, incluindo o diálogo de SMTP e os relatórios de DSN, para a produção de um ou mais sumários de mensagem correspondentes à cópia de mensagem com significado. O RPost compara os sumários de mensagem na cópia com significado, incluindo o sumário de mensagem geral, com os sumários de mensagem os quais o RPost computou a partir da cópia de mensagem com significado. O sumário de mensagem geral pode ser comparado pela desencriptação do sumário de mensagem geral recebido como a assinatura digital no recibo com significado, ou pela encriptação do sumá-

rio de mensagem geral, o qual foi calculado a partir da cópia de mensagem com significado. Se os sumários de mensagem, incluindo a assinatura digital, combinarem, então, o recibo é um recibo gerado por RPost autêntico. Assumindo que uma boa função de comprovação tenha sido usada e que as chaves usadas na função de comprovação criptográfica e no algoritmo de encriptação de assinatura digital não tenham sido divulgadas para outros, é virtualmente impossível que o recibo tenha sido "forjado" pela pessoa apresentando o recibo. Isto é, o recibo deve ter sido um recibo que foi gerado por RPost, e, portanto, a mensagem contida no recibo, a informação para/de, a data e o horário de envio, o fato do envio bem sucedido, a rota pela qual a mensagem andou, e qualquer informação de DSN contida no recibo, devem ser uma cópia fiel daquela informação e ser acurados. O RPost, então, pode prover autenticação, verificação e confirmação da informação contida no recibo. Esta confirmação pode tomar a forma de uma confirmação de e-mail, testemunho de declaração juramentada, de empregados do RPost familiarizados com os métodos usados pelo RPost, testemunho de juramento ao vivo em depoimentos e no tribunal, e outras formas de testemunho. O RPost pode cobrar honorários do remetente 10, do destinatário 18 ou de qualquer outra entidade pelos vários respectivos serviços de confirmação. O RPost também pode prover testemunho ou uma outra confirmação com referência à não autenticidade de um recibo com significado. O testemunho pode ser provido de acordo com as Regras Federais de Evidência 901(9), 901(10), 803(6), 803(7), 1001-1104, 1006, 702-706, regras estaduais correspondentes de evidência e outras regras aplicáveis.

[00167] Em resumo, o sistema provê uma evidência confiável com base no testemunho de terceiros desinteressados de que uma mensagem em particular tendo um conteúdo em particular foi enviada, quando ela foi enviada, quem a enviou, quem a recebeu, quando ela foi a-

berta para leitura, e quando ela foi apagada. Esta evidência pode ser apresentada a qualquer momento que uma disputa surgir referente ao conteúdo e ao envio de mensagens, como, por exemplo, na formação de um contrato, na sincronização de pedidos de compra ou venda de ações, e em muitas outras aplicações. Os operadores do sistema podem atestar a acurácia da informação contida no recibo em si, sem a necessidade de os operadores preservarem qualquer registro ou cópia da informação contida no recibo.

[00168] Uma vantagem significativa do sistema é que ele pode ser usado por MUAs existentes, sem qualquer mudança neles. Devido ao fato de toda a computação, a encriptação, a interrogação e o diálogo de ESMTP, a coleta de relatório de DSN, e a compilação de recibo serem realizados por um servidor de RPost de terceiros, nenhuma dessas funções precisa ser implementada em qualquer um dos equipamentos do usuário. Assim, os usuários podem tirar vantagem do sistema de forma rápida e fácil.

[00169] Na modalidade da invenção descrita acima, o servidor RPost registra o envio de todas as mensagens que passem através dele. Alternativamente, um servidor RPost poderia registrar apenas aquelas mensagens tendo certos destinos (por exemplo, externos a uma organização) ou de certos remetentes (por exemplo, um grupo de relações de consumidor). De forma alternativa ou adicional, o servidor RPost poderia registrar apenas aquelas mensagens que tivessem caracteres distintos ou cadeias no assunto ou no corpo da mensagem. Por exemplo, o servidor poderia registrar apenas mensagens que o remetente tivesse incluído "(R)" no assunto da mensagem. Todas as outras mensagens poderiam ser enviadas pelo servidor RPost ou algum outro servidor funcionando como um MTA de Internet comum.

[00170] Nesta modalidade, o RPost pode elevar a receita de uma variedade de formas. Por exemplo: o RPost pode cobrar um honorário

de um remetente de mensagem 10 ou da sua organização em uma base por mensagem, em uma base por quilobyte, em uma base periódica de honorário fixo, tal como mensalmente, ou em uma combinação do acima. O RPost também pode cobrar honorários para a autenticação e a verificação de um recibo, com uma escala de encargos dependendo de a verificação visada ser um e-mail de retorno simples, uma declaração juramentada por escrito ou uma declaração, um testemunho de fato juramentado em depoimento ou em tribunal, ou um testemunho de especialista juramentado em depoimento ou em tribunal. Se os usuários optarem por terem o RPost retendo cópias dos recibos, o RPost pode cobrar honorários de armazenamento por item e/ou por quilobyte por mês.

II. FLUXOGRAMA PARA REGISTRO DE UMA MENSAGEM DE SAÍDA

[00171] As figuras 2A a 2G constituem um fluxograma que mostra uma operação de exemplo da primeira modalidade do sistema. A modificação deste fluxograma para aplicação a outras modalidades está na capacidade de alguém familiarizado com protocolos de software e de e-mail.

[00172] A figura 3A, Pré-processamento, ilustra as etapas seguidas com uma mensagem, antes de ela ser transmitida pelo Servidor de Registro (o Sistema).

[00173] Para registrar uma mensagem de e-mail, na etapa 201, um originador/remetente/usuário cria uma mensagem de e-mail, usando qualquer Agente de Usuário de Correio da Internet (MUA). Os MUAs possíveis incluem: (1) programas de e-mail de lado de cliente; (2) programas de e-mail baseados em servidor; (3) serviços de e-mail baseados na web; e (4) formulários em HTML submetidos através de páginas da web. A mensagem pode conter arquivos anexados, como descrito nas Requisições por Comentários (RFCs) 822, 2046 e 2047, as

quais, desse modo, são incorporadas como referência. As RFCs são uma série de notas referentes à Internet, que discutem muitos aspectos da comunicação em computador, concentrando-se em protocolos de rede, procedimentos, programas e conceitos.

[00174] Nesta modalidade, o sistema funciona como o servidor de correio de saída do remetente e, assim, a mensagem do remetente será diretamente transferida para o servidor RPost pelo MUA do remetente (etapa 202).

[00175] Na etapa 203, o sistema cria uma cópia da mensagem original para ser armazenada para um processamento posterior.

[00176] Na etapa 204, o sistema cria um registro em um banco de dados, o qual pode incluir informação tal como: o horário no qual a mensagem foi recebida pelo remetente, os nomes e o(s) tamanho(s) do(s) anexo(s) de arquivo da mensagem, o nome (se conhecido) de cada destino da mensagem; o endereço na Internet de cada destino. O horário no qual a mensagem foi enviada para o MTA de destino (inicialmente, este valor é nulo) e uma unidade a qual registra o Status de Envio de cada destino.

[00177] Na etapa 205, o Status de Envio de cada destino é regulado para "NÃO ENVIADA".

[00178] Na etapa 206, o sistema gera e armazena um sumário de mensagem ou uma impressão digital gerada a partir do corpo da mensagem.

[00179] Na etapa 207, o sistema gera e armazena uma comprovação ou um sumário de mensagem para cada anexo incluído na mensagem.

[00180] Na etapa 208, o sistema pode criar uma cópia modificada da mensagem original. Nesta segunda cópia (etapa 209), a linha de assunto original da mensagem foi emendada para indicar que esta cópia é registrada (por exemplo, por um prefixo "Registrado").

[00181] Na etapa 210, uma nota de que a mensagem é registrada pelo sistema juntamente com links para o sítio da Rede Mundial do sistema podem ser anexados ao corpo da mensagem.

[00182] Na etapa 211, os cabeçalhos de e-mail podem ser adicionados, requisitando uma notificação de leitura em uma variedade de formatos de cabeçalho reconhecidos por vários MUAs. As requisições por notificação dirigem a notificação de retorno para um endereço associado ao sistema: por exemplo, "readreceipt@RPost.com". Esses cabeçalhos também incluirão o endereço do remetente original da mensagem no campo de nome do endereço para o qual a notificação de MUA deve ser enviada.

[00183] O pré-processamento tendo sido completado, os sistema, agora, transmitirá uma cópia da mensagem para cada um de seus destinos, como ilustrado na figura 2B.

[00184] A figura 2B ilustra as etapas requeridas para a transmissão de uma mensagem registrada. Como a etapa 220 indica, o processo requer uma transmissão separada para cada destinatário da mensagem.

[00185] Na etapa 221, o sistema muda o campo de cabeçalho de sua cópia de trabalho da mensagem, para mostrar a mensagem como sendo "DE:" um remetente cujo nome é o remetente original da mensagem, mas cujo endereço é um endereço "RPost.com" construído a partir de:

[00186] uma série usada para a identificação de notificações de MTA de retorno (por exemplo, "RCPT");

[00187] uma série a qual identifica de forma única a mensagem sendo enviada;

[00188] um rótulo, o qual identifica de forma única esta cópia da mensagem que é para ser enviada.

[00189] Na etapa 222, usando-se o nome de domínio do destino

para o qual se está enviando atualmente, o sistema faz uma consulta de troca de Correio de Servidor de Nome de Domínio para encontrar o endereço do(s) MTA(s) responsáveis pela coleta de correspondência para endereços neste domínio.

[00190] Na etapa 223, o sistema tenta fazer uma conexão de telnet direta com o MTA do destino. Se a conexão falhar, o sistema tentará fazer a conexão de novo. Desde que o sistema não tenha excedido um número máximo de novas tentativas (227) para este destino, o sistema tentará refazer a conexão, talvez usando um outro servidor de MX para o domínio do destino (228).

[00191] Se, após um número máximo de tentativas, o sistema não puder se conectar a um MTA para este destino, o sistema, como na etapa 226, registra seu Status de Envio de destino como "NÃO ENVIÁVEL", e cessa de tentar enviar esta mensagem para este destino.

[00192] Ao se conectar o MTA de destino, o sistema começará a fazer um registro de seu diálogo de (E)SMTP com o MTA (225).

[00193] Na etapa 229, o sistema tenta iniciar uma troca de SMTP Estendido (ESMTP) com o MTA de destino, emitindo uma saudação "EHLO".

[00194] Se o MTS de destino suportar ESMTP, o sistema, então, (230) determinará se o MTA de destino suporta a função de SMTP VERIFICAR. Se o MTA suportar VERIFICAR, o sistema tentará determinar se o endereço de destino é um endereço válido no domínio (231).

[00195] Se o endereço não for válido, então, como na etapa 232, o sistema registrará o Status de Envio deste destino como "FALHA" e cessará de tentar enviar esta mensagem para este destino.

[00196] Se o endereço for válido ou se o servidor de ESMTP não suportar VERIFICAR, o sistema, então, (233) determinará se o MTA de recebimento suporta a DSN (Notificação de Status de Envio) do serviço de ESMTP.

[00197] Se o MTA realmente suportar a DSN de ESMTP, o sistema transmitirá a mensagem com requisições de ESMTP, para notificar ao remetente nominal da mensagem do sucesso ou da falha do envio (234). Tendo transmitido a mensagem, o sistema registrará o Status de Envio deste destino como "ENVIADA E ESPERANDO POR DSN" (235).

[00198] Se o MTA de recebimento não suportar o SMTP Estendido, o sistema transmitirá a mensagem usando o SMTP (236) e gravará o status de destino como "ENVIADA" (237).

[00199] Tendo enviado a mensagem, o sistema, então, armazenará o diálogo de (E)SMTP, gravando o envio de uma maneira a qual possa ser mais tarde recuperada (238) e tentará enviar a mensagem para um outro destino.

[00200] Tendo transmitido a mensagem para o(s) seu(s) destino(s), o sistema deve executar várias funções, de modo a acumular informação sobre a disposição da mensagem. A figura 2C ilustra o processo por meio do qual o sistema processa as Notificações de MTA retornadas pelos MTAs de destinatário.

[00201] Devido ao formato usado nos cabeçalhos de mensagens enviadas ilustrado na etapa 221 da figura 2B, as notificações de mensagem de MTA serão enviadas para um endereço local fictício no servidor. O sistema será capaz de detectar essas notificações por uma série (por exemplo, "rcpt") embutida nos seus endereços (241). Por uma análise gramatical do endereço, como ilustrado em 242, o sistema pode determinar qual mensagem para qual destino orientou a notificação recebida.

[00202] Na etapa 243, o sistema varre a linha de assunto e o corpo dos MTAs recebidos quanto a frases que indiquem se o MTA está reportando um envio bem sucedido, um envio falho, ou que a mensagem foi retransmitida para um outro servidor.

[00203] No caso de o processo na etapa 243 revelar que a notificação está reportando um envio bem sucedido, o sistema, como ilustrado na etapa 245, mudará o Status de Envio do destino relevante da mensagem relevante para "ENVIADA PARA CAIXA DE CORREIO".

[00204] Se o sistema determinar que a nota de MTA está reportando uma falha de envio, o sistema (247) mudará o Status de Envio do destino relevante da mensagem relevante para "FALHA".

[00205] No caso de o sistema determinar que a notificação de MTA indica que a mensagem foi retransmitida para um outro servidor, o sistema, como ilustrado na etapa 249, muda o Status de Envio do destino relevante da mensagem relevante para "RETRANSMITIDA".

[00206] Tendo processado a Notificação de MTA, o sistema salvará esta mensagem e todos os seus anexos de maneira tal que eles possam ser mais tarde relembrados e usados na construção de um recibo para este destino (250).

[00207] De tempos em tempos, como ilustrado na figura 2D, o sistema examinará o status de cada mensagem, para determinar se o sistema recuperou todas as notificações de MTA que ele tem probabilidade de receber para cada destino de mensagem e pode, assim, prosseguir para construir um recibo para a mensagem.

[00208] O sistema examinará o Status de Envio de cada destino da mensagem.

[00209] Se qualquer destino tiver o Status de Envio "NÃO ENVIADA", então, o processamento da mensagem não está completo (252).

[00210] Se o Status de Envio de um destino for "ENVIADA E ESPERANDO POR DSN", então, o sistema não considerará o processamento para este destino como completo, a menos, como ilustrado na etapa 254, que o tempo desde o envio da mensagem tenha excedido ao período de espera do sistema (por exemplo, 24 horas).

[00211] Se o Status de Envio de um destino for "ENVIADA" (257), então, o sistema considerará o processamento deste destino como completo, desde que (258) um período de tempo tenha decorrido, o qual os operadores do sistema tratam como suficiente para terem recebido uma nota de falha de envio do MTA de destino (por exemplo, duas horas).

[00212] Qualquer outro Status de Envio de destino (por exemplo, "FALHOU", "NÃO ENVIÁVEL", "ENVIADA PARA CAIXA DE CORREIO") é tratado como tendo um processamento completado.

[00213] Se o processamento de qualquer um dos destinos de mensagem não estiver completo, o sistema não faz nenhuma ação, mas se move para considerar outras mensagens no sistema (etapa 255).

[00214] Contudo, como ilustrado na etapa 259, se o processamento de cada destino da mensagem estiver completo, o sistema gerará um Recibo de Envio para a mensagem.

[00215] Como ilustrado a título de exemplo na figura 2E, o recibo pode incluir:

[00216] um identificador para fins administrativos, como no bloco 271. Este identificador pode ser ou pode incluir uma referência à ID do remetente e/ou ao valor da ID da Mensagem da Internet da mensagem do remetente, como recebido pelo sistema.

[00217] Como no bloco 272, o corpo citado da mensagem original 12 juntamente com os endereços de e-mail de seus destinatários pretendidos também podem ser incluídos.

[00218] Como no bloco 273, uma tabela para cada listagem de destinatário pode incluir:

[00219] o horário no qual o MTA do destinatário recebeu a mensagem e/ou o horário no qual o sistema recebeu uma DSN do MTA do destinatário;

[00220] o relatório de Status de Envio da mensagem para aquele

destino, isto é, "Enviada para o Servidor de Correio", "Enviada para Caixa de Correio", "Retransmitida", "Falha de Envio", "Não Enviável";

[00221] Como no bloco 274, uma lista dos anexos originais do e-mail juntamente com seus valores de comprovação separados ou sumários de mensagem.

[00222] Como no bloco 275, transcrições ou resumos das transcrições de todos os diálogos de SMTP envolvidos no envio da mensagem para cada destino.

[00223] Como no bloco 276, citações dos corpos e dos anexos de todas as DSNs recebidas, incluindo quaisquer detalhes de envio ou disposição da mensagem que elas possam revelar.

[00224] Como no bloco 277, o sistema pode anexar ao recibo cópias de todos os anexos da mensagem original, e, como no bloco 278, o sistema, adicionalmente, anexa arquivos retornados para o sistema como anexos para DSNs.

[00225] Na etapa 279, tendo gerado o texto do recibo até agora, o sistema, então, gera uma primeira comprovação para a mensagem de e-mail e uma(s) segunda(s) comprovação(ões) para quaisquer anexos ao corpo do recibo, e calcula uma assinatura digital para cada uma da(s) comprovação(ões), usando uma chave de encriptação conhecida apenas pelos operadores do sistema. A encriptação pode empregar, por exemplo, o Padrão de Encriptação de Dados descrito na Publicação de Norma de Processamento de Informação Federal 4-2 (FIPS PUB 46-2), o Padrão de Encriptação de Dados,, National Institute of Standards and Technology, ao qual é incorporada desse modo como referência. Alternativamente, outros métodos conhecidos ou novos de encriptação do valor de comprovação podem ser usados.

[00226] Na etapa 280, a comprovação encriptada, então, é anexada ao final da mensagem, como a "assinatura digital do documento".

[00227] Na etapa 281, o recibo 20, agora estando completo, pode

ser enviado por e-mail para o remetente com o conselho de que seja mantido para os registros do remetente. Na etapa 282, o sistema agora pode apagar todas as cópias da mensagem original, os anexos e as DSNs. Alternativamente, ao invés de enviar o recibo para o remetente, o sistema pode armazenar o recibo, ou ambos o remetente e o sistema podem armazenar o recibo.

[00228] Devido ao fato de as notificações de MUA serem retornadas apenas à escolha do destinatário e apenas quando o destinatário faz alguma ação em relação à mensagem recebida, as modalidades do sistema podem escolher tratar essas mensagens de retorno diferentemente das notificações de MTA.

[00229] A figura 2F ilustra como essas notificações de MUA podem ser tratadas pelo sistema. As notificações de MUA são solicitadas pelo sistema pela inclusão de vários cabeçalhos nas mensagens de saída, da maneira da figura 2A, etapa 211. Esses cabeçalhos direcionam MUAs conformes para o envio de notificações para um endereço do sistema (por exemplo, "readreceipt@RPost.com") posto de lado para esta finalidade. Os cabeçalhos também usam, no campo "nome" de seu endereço de retorno, o endereço de e-mail do remetente original da mensagem. Assim sendo, na etapa 286, quando as notificações de MUA são retornadas para readreceipt@RPost.com, o sistema pode, pelo exame do endereço da notificação, determinar o endereço para o qual a notificação de leitura deve ser enviada.

[00230] Mediante a chegada de um recibo de leitura de um MUA de destino, o sistema, na etapa 287, gera um recibo de leitura, que contém o assunto da notificação de MUA recebida como seu assunto, e incorpora, em seu corpo de mensagem, o corpo da Notificação de MUA recebida.

[00231] Na etapa 288, o sistema anexa ao recibo quaisquer arquivos que possam acompanhar o recibo de MUA (tipicamente, estes po-

dem incluir detalhes de envio ou disposição e referências de identificação para o e-mail original).

[00232] Na etapa 289, o sistema gera uma comprovação para quaisquer arquivos anexados ao recibo e registra esta comprovação no corpo do recibo.

[00233] Na etapa 290, o sistema gera uma comprovação para o corpo do recibo e seus anexos, encripta esta comprovação, e anexa o resultado à mensagem como uma "assinatura digital de documento".

[00234] Na etapa 291, o sistema envia o recibo resultante para o remetente da mensagem. Na etapa 292, tendo enviado este recibo, o sistema pode apagar todos os registros internos da transação.

III. **MODALIDADE** DE RPOST COMO SERVIDOR DE CORREIO SECUNDÁRIO

[00235] A figura 3 é um diagrama de sistema de uma segunda modalidade da presente invenção, onde o servidor RPost não serve ao MTA primário do usuário, mas, ao invés disso, trabalha em colaboração com um outro MTA. Nesta modalidade, o remetente pode eleger registrar uma mensagem de saída em particular ao incluir alguma forma de indicador em uma mensagem de saída, assunto de mensagem ou endereços de mensagem. Por exemplo, se e apenas se um remetente incluir o símbolo "(R)" no assunto da mensagem, o MTA do remetente dirigirá a mensagem para ser transmitida através do servidor RPost para a geração de um recibo.

[00236] Nesta modalidade, os operadores do RPost recebem receitas do operador do MTA do remetente por mensagem e/ou por quilobyte transmitido.

IV. **MODALIDADE** DE CC PARA RPOST

[00237] A figura 4 é um diagrama de sistema de uma terceira modalidade, na qual uma cópia carbono ("cc") é enviada para o servidor RPost. Nesta modalidade, o usuário ou o remetente da mensagem 10

pode usar um MUA padrão e um MTA padrão, sem modificação. O remetente da mensagem 10 compõe o e-mail tendo um corpo de mensagem e qualquer número de anexos, e o endereça para o destinatário de mensagem 18, juntamente com quaisquer cópias carbono (cc's) e cópias carbono ocultas (bcc's), como desejado. Adicionalmente, o remetente da mensagem 10 endereça um cc para RPost. O servidor RPost 14 rotula a mensagem, como antes, e envia a mensagem rotulada incluindo os anexos para o MTA de destinatário 16 e quaisquer cc's designadas. Ao receber uma cópia como essa, o servidor RPost 14 pode enviar um e-mail reconhecendo o recibo da cópia.

[00238] O destinatário 18 e outros destinos da mensagem agora receberão duas versões da mesma mensagem: uma primeira versão da mensagem recebida diretamente a partir do remetente 10, e uma segunda versão rotulada, a qual foi enviada a partir do RPost. Uma vez que o RPost receba confirmação do MTA de destinatário 16 que a versão rotulada da mensagem foi recebida de forma bem sucedida pelo MTA de destinatário 16, o servidor RPost 14 compõe um recibo de mensagem 20, como antes, e envia o recibo para o remetente 10, para seus registros.

[00239] A receita pode ser gerada pelo estabelecimento de contas para domínios originando mensagens ou remetentes de mensagens individuais, e cobrando-se as contas de usuários por mensagem, por quilobyte, por mês ou uma combinação destes. A receita também pode ser gerada pela colocação de anúncios nos recibos e a partir de serviços de autenticação e verificação, como descrito previamente.

V. **MODALIDADE** DE WEBSITE

[00240] A figura 5 é um diagrama de sistema de uma quarta modalidade. Nesta modalidade, o servidor RPost 14 está associado a um website, no qual um usuário compõe mensagens. O remetente da mensagem 10 visita o Website do RPost e compõe sua mensagem no

website, introduzindo "para", "cc", "bcc", "Assunto" e informação de texto de mensagem desejados. Anexos podem ser adicionados pelo uso de aspectos disponíveis em navegadores padronizados e servidores da web. Nesta modalidade, o remetente deve prover, adicionalmente, um endereço para o qual o recibo de registro pode ser enviado. O servidor RPost 14 envia o recibo para o remetente 10 através do MTA do remetente.

[00241] A receita pode ser gerada pelo estabelecimento de contas para domínios originando mensagens ou remetentes de mensagens individuais, e cobrando-se as contas de usuários por mensagem, por quilobyte, por mês ou uma combinação destes. A receita também pode ser gerada pela colocação de anúncios nos recibos e a partir de serviços de autenticação e verificação, como descrito previamente.

VI. **MODALIDADE** DE MUA BASEADO NA WEB

[00242] A figura 6 é um diagrama de sistema de uma quinta modalidade. Nesta modalidade, o servidor RPost 14 está associado a um Agente de Usuário de Correio baseado na web. Além de permitir que os usuários componham uma correspondência através de um navegador da web, um MUA como esse provê aos assinantes caixas de correio que podem ser vistas por navegador, que exibem mensagens armazenadas no sítio do servidor da web. Os assinantes de um serviço como esse ganham acesso a contas de correio com nomes de usuário e senhas. Nesta modalidade, o remetente da mensagem 10 visita o Website do RPost, acessa uma conta de e-mail baseada na web introduzindo um nome de usuário e uma senha, e compõe sua mensagem, a qual é transportada para envio para o servidor RPost 14. Os recibos gerados pelo servidor RPost são retornados para uma caixa de correio baseada na web associada à conta do assinante.

[00243] Além das fontes de receita disponíveis em outras modalidades, nesta modalidade os operadores podem cobrar honorários para

recibos mantidos na caixa de correio baseada na web.

[00244] Em todas essas modalidades, o recibo pode servir como uma evidência que:

o originador enviou uma mensagem de e-mail;

a mensagem foi enviada em um certo horário;

o e-mail foi endereçado para certo(s) destinatário(s);

o e-mail foi enviado para a caixa de correio de e-mail para cada um de seu(s) destinatário(s) pretendido(s);

o e-mail foi enviado em um certo horário;

o e-mail foi enviado por uma certa rota de rede; e

a mensagem de e-mail e seus anexos tiveram o conteúdo específico gravado no recibo.

[00245] Mais ainda, o sistema, sob certas circunstâncias, gera um recibo separado, o qual pode ser usado como evidência que:

o e-mail foi inspecionado através do Agente de Usuário de Correio (MUA) do destinatário; e

o destinatário fez certas ações em resposta à mensagem, por exemplo, leu ou apagou o e-mail, em um horário em particular.

[00246] Como nas outras modalidades, esta modalidade produz evidência documentada, a qual pode ser atestada e verificada pelos operadores de terceiros desinteressados do sistema do envio e da integridade de uma mensagem eletrônica. Em outras palavras, o sistema pode ser pensado como transformando o e-mail em um e-mail registrado, que pode ser usado, mais tarde, para provar que uma mensagem de e-mail em particular foi enviada, que ela foi enviada com sucesso, e quando e como.

[00247] Caso uma disputa um dia surja, a disputa pode ser resolvida através do recibo gerado pelo sistema, porque o recibo é codificado de modo que os operadores do sistema possam determinar a autenticidade do recibo como o produto do sistema. Após isso, os operadores

do sistema podem atestar a acurácia da informação contida em um recibo autêntico, confiando na informação contida no recibo em si, e sem a necessidade de os operadores preservarem qualquer registro ou cópia da informação contida no recibo.

[00248] Além desses benefícios, os recibos gerados pelo sistema também podem ser úteis como evidência da existência e da autoria de materiais tais como poderiam ser transmitidos através do sistema. Mais ainda, o sistema é fácil de usar, uma vez que o sistema pode ser usado a partir de qualquer programa cliente de e-mail da Internet / MUA, de modo que não haja um software adicional requerido.

DIAGRAMA DE FLUXO PARA VALIDAÇÃO DE UM RECIBO

[00249] A figura 7 é um fluxograma que ilustra um método de exemplo para validação de um recibo. No caso de o remetente de uma mensagem dever requerer uma evidência que um e-mail foi enviado e remetido (e/ou lido), o remetente apresenta o(s) recibo(s) correspondente(s) à mensagem para os operadores do sistema, na etapa 700. Os operadores do sistema, então, na etapa 702, destacam e desencriptam a assinatura digital de documento anexada ao recibo. Na etapa 703, os operadores geram uma comprovação do balanço do documento, incluindo os anexos.

[00250] Na etapa 704, se o valor de comprovação atual não combinar com o valor de comprovação desencriptado, então, o sistema gera um relatório declarando que o RPost não pode autenticar o recibo como um registro acurado do envio ou do conteúdo da mensagem descrita no recibo.

[00251] Se a comprovação desencriptada for equivalente à comprovação atual da mensagem, o sistema pode, como na etapa 706, garantir que a informação contida no corpo da mensagem é sem modificação desde que o recibo passou através do sistema. Se a mensagem original não continua nenhum anexo, o sistema, agora, pode gerar um

relatório que garante que o recibo é um registro acurado do conteúdo da mensagem e do seu envio pelo servidor RPost.

[00252] Se o recibo relatar que a mensagem original continha anexos, então, o recibo também registrará o nome e o valor de comprovação de cada anexo. Na geração do recibo, todos os anexos da mensagem original são anexos não modificados ao recibo. Assim sendo, o sistema, para cada arquivo anexado como esse, gerará uma comprovação do arquivo anexado (708) e a comparará com o valor de comprovação registrado no corpo do recibo (709).

[00253] Se o valor de comprovação calculado de um arquivo combinar com o valor incluído no recibo, o sistema pode garantir que o arquivo anexado ao recibo é idêntico àquele anexado à mensagem como originalmente enviado. Se as comprovações não combinarem, então, o sistema reportará que ele não pode garantir que o arquivo anexado ao recibo é idêntico ao arquivo anexado à mensagem original.

[00254] Tendo executado este cálculo para cada arquivo anexado à mensagem original, o sistema prepara um relatório, o qual reporta a autenticidade do recibo e de cada um de seus arquivos anexados (710) ou o qual reporta a falha de validação (712).

[00255] Tendo completado sua avaliação, o sistema então anexará uma cópia do recibo e de todos os seus anexos ao relatório que ele gerou e a enviará via e-mail para o endereço de retorno do usuário que submeteu o relatório para validação.

VII. Registro de E-mails que Chegam

[00256] A figura 8 é um diagrama de sistema que ilustra uma outra modalidade da invenção, na qual as mensagens que chegam são registradas. Nessa modalidade, um remetente de mensagem 60 envia uma mensagem de e-mail 70. O MTA de remetente 62 envia a mensagem 70 pela Internet, como usual. Entretanto, nesta modalidade, o RPost contrata o assinante de serviço / destinatário 68 para registrar

os e-mails que chegam. De acordo com o acordo, o RPost é designado com Network Solutions, Inc. (NSI) ou uma outra autoridade de nome de domínio como o destinatário de correio (servidor de MX) para o destinatário 68. Isso faz com que a requisição de Serviço de Nome de Domínio (DNS) executada pelo MTA do remetente 62 retorne o endereço de IP de RPost como o endereço de IP para o destinatário, o qual, por sua vez, faz com que o MTA do remetente 62 envie a mensagem de e-mail para o servidor RPost 64. O servidor RPost 64 atua como um MTA de SMTP, POP, POP3 ou IMAP (coletivamente, "servidor de correio POP") para o destinatário 68. Os mtas de SMTP, POP e IMAP são governados pela RFC 821, o protocolo SMTP, RFC 1939 Post Office Protocol – Version 3 (o qual tornou obsoleta a RFC 1725), e o RFC 2060 IMAP (Internet Message Acess Protocol) Version 4 rev 1 (a qual tornou obsoleta a RFC 1730), os quais são, desse modo, incorporados como referência.

[00257] O servidor RPost 64 prepara uma versão registrada 74 da mensagem original 70, e coloca sua versão registrada 74 na caixa de entrada do destinatário 68 ao invés de ou além da mensagem original 70. A versão registrada pode ter todos os aspectos e as opções de verificação e informação discutidas anteriormente em relação aos recibos de e-mails. Esta informação pode incluir, mas não está limitada a: sumários de mensagem individuais para cada um dentre o corpo da mensagem e o texto, a informação para/de, uma outra informação de cabeçalho, cada anexo, um sumário de mensagem geral e assinatura digital e informação de direcionamento de mensagem e rótulos. A versão registrada 74 da mensagem 70, como mostrado na figura 6, inclui o corpo de mensagem, incluindo a informação de cabeçalho, um anexo, sumários de mensagem separados para cada um, e uma assinatura digital ou um sumário de mensagem encriptado. As funções de comprovação e a encriptação são executadas usando-se frases pro-

vadas ou chaves privadas conhecidas apenas pelos operadores do sistema. A versão registrada 74 é tornada disponível para o destinatário 68, para inspeção ou transferência através do MUA de destinatário.

[00258] O servidor RPost, opcionalmente, pode enviar um e-mail de confirmação 72 para o remetente da mensagem 60. A mensagem de confirmação 72 também poderia incluir uma mensagem tal como "Sua mensagem de e-mail foi recebida em 24 de março de 2000 às 14:05. A assinatura digital da mensagem foi [assinatura digital de 128 bits]. Para maiores informações, visite nosso website em www.RPost.com." De forma alternativa ou adicional, a mensagem de confirmação 72 poderia incluir toda a informação contida na versão registrada 74.

[00259] Assim, o sistema pode prover ao destinatário da mensagem 68 um recibo 74 ou uma outra confirmação verificável que:

[00260] o destinatário recebeu uma mensagem de e-mail;

[00261] a mensagem foi recebida em um certo horário;

[00262] o e-mail foi endereçado a partir de um certo remetente;

[00263] os significados de mensagem a serem enviados através de uma certa rota de rede; e

[00264] a mensagem de e-mail e seus anexos tinham um conteúdo específico.

[00265] Assim sendo, o sistema provê evidência, a qual pode ser atestada pelos operadores do sistema, que mensagens eletrônicas particulares e documentos foram enviados para destinatários tendo um certo conteúdo e representando a si mesmas como tendo vindo de certos remetentes.

[00266] A figura 9 é um fluxograma que ilustra um exemplo de registro de correio que chega. Na etapa 901, o servidor RPost 64 recebe uma nova mensagem de e-mail. Na etapa 902, o sistema gera uma comprovação/assinatura digital do conteúdo da mensagem, incluindo os cabeçalhos e os anexos da mensagem. Adicionalmente, o sistema

pode gerar uma comprovação separada para cada anexo de mensagem. Na etapa 903, o sistema encripta a(s) comprovação(ões) usando uma chave de encriptação conhecida apenas pelos operadores do sistema. Na etapa 904, a(s) comprovação(ões) resultante(s), então, é(são) anexada(s) ao corpo da mensagem. Então, na etapa 905, a mensagem modificada pode ser tornada disponível para inspeção ou transferência através do MUA de destinatário.

[00267] A figura 10 é um fluxograma de um exemplo de validação de uma mensagem de e-mail registrada recebida. Na etapa 1000, no caso de o destinatário de uma mensagem dever requerer evidência que um e-mail com um conteúdo específico foi recebido em um horário em particular, o destinatário pode apresentar uma cópia da versão registrada 74 (Figura 8) de uma mensagem de e-mail 70 para os operadores do sistema, para verificação. Para verificar a mensagem, na etapa 1001, o sistema destaca e desencripta a assinatura digital de documento anexada à mensagem. Na etapa 1002, o sistema gera uma comprovação do balanço do documento, e uma para cada arquivo anexado à mensagem. Nas etapas 1003 e 1004, as comprovações são comparadas. Se a(s) comprovação(ões) do documento combinar(em) com a(s) comprovação(ões) desencriptada(s), então, a mensagem e seus anexos devem ter passado através do sistema e não terem sido alterados desde o seu envio para o destinatário.

[00268] Tendo determinado que o e-mail é inalterado, os operadores do sistema podem garantir que:

[00269] o e-mail foi recebido pelo sistema em um certo tempo;

[00270] o e-mail parece ter chegado ao sistema através de uma certa rota da Internet;

[00271] o e-mail parece ser de um certo remetente;

[00272] o e-mail e seus anexos foram enviados com o conteúdo específico que eles atualmente contêm.

[00273] Por outro lado, na etapa 1006, se os valores de comprovação não combinarem, então, o operador não pode garantir que o e-mail é autêntico, isto é, que o e-mail é uma versão acurada de um e-mail que foi recebido pelo sistema.

[00274] A figura 11 ilustra como a invenção pode ser usada por um negócio o qual utiliza ferramentas eletrônicas (um negócio eletrônico). O negócio eletrônico 30 pode utilizar o sistema para registrar todas as mensagens de e-mail que chegam e saem de seus consumidores 34. Neste caso, o sistema incluir o servidor de Protocolo de Correio (POP) 36 e um servidor de Protocolo Simples de Transferência de Correio (SMTP) 38. Por exemplo, o negócio eletrônico 30 pode estabelecer seu website para formas de e-mail para consumidores e para enviar consultas e reclamações 40 dos consumidores 34. As consultas registradas, as reclamações, os pedidos, ofertas de compra e outra informação 46 são enviados para o negócio eletrônico 30 pelo sistema. Os recibos, então, são providos para os consumidores 34 através do servidor de SMTP 38. Desta forma, não há questão referente a se o consumidor enviou ou não a comunicação e o que ela continua. Mais ainda, o negócio eletrônico pode configurar um website 32 através do servidor RPost, de modo que cada comunicação com os consumidores possa ser registrada. Em outras palavras, através do website os pedidos de dados de formulário do 42 e respostas automatizadas 44 podem ser registrados através do servidor do sistema; mais ainda, qualquer confirmação, notas de coleções, suporte ao consumidor, e ofertas especiais 48 enviadas pelo negócio eletrônico para os consumidores 34 podem ser registrados e a confirmação enviada para o consumidor, para eliminação de argumentos quanto ao que foi pedido, quando ou por quem. Se desejado, recibos idênticos podem ser providos para ambos os consumidores 34 e o negócio eletrônico 30. Alternativamente, as funções do servidor de POP 36 e do servidor de SMTP 38 po-

dem ser combinadas em um servidor de sistema único.

[00275] O POP é um protocolo usado para a recuperação de um e-mail a partir de um servidor de e-mail. Muitas aplicações de e-mail (às vezes denominados clientes de e-mail) usam o protocolo de POP, embora alguns possam usar o Protocolo de Acesso de Mensagem da Internet (IMAP) mais novo. Uma versão de POP, denominada POP2, requer um SMTP para o envio de mensagens. Uma versão mais nova, POP3, pode ser usada com ou sem SMTP. O SMTP é um protocolo para o envio de mensagens de e-mail entre servidores. Muitos sistemas de e-mail que enviam e-mail pela Internet usam SMTP para o envio de mensagens de um servidor para o outro; as mensagens, então, podem ser recuperadas com um cliente de e-mail, usando-se POP ou IMAP. Além disso, o SMTP, geralmente, é usado para o envio de mensagens de um cliente de correio para um servidor de correio. Os servidores de e-mail podem usar uma variedade de protocolos para se comunicarem com a Internet. Os protocolos comumente usados incluem SMTP, POP3 e IMAP4. Os leitores de correio estão na extremidade oposta do servidor. Uma vez que os servidores de correio recebam as mensagens através de SMTP, os leitores de e-mail enviam o e-mail para um servidor de correio, usando o SMTP. Da mesma forma, uma vez que os servidores de correio enviem mensagens usando POP3 e, opcionalmente, IMAP4, os leitores de correio recebem mensagens de servidores de correio usando o protocolo POP3 ou IMAP4.

[00276] Embora o dito acima descreva geralmente um sistema e um método de verificação que um e-mail foi enviado e/ou recebido, a presente invenção pode se aplicar a qualquer mensagem eletrônica que possa ser transmitida através de uma rede de mensagem eletrônica ou através de qualquer porta eletrônica. As mensagens eletrônicas podem incluir texto, áudio, vídeo, gráficos, dados e anexos de vários tipos de arquivo. Os métodos e as técnicas ensinadas aqui podem ser

programados em servidores e outros computadores, e programas de computador implementando a invenção podem ser escritos em mídias que podem ser lidas em computadores, incluindo, mas não limitando CD ROMs, RAM, discos rígidos e fita magnética. Os serviços de registro de e-mail de acordo com a presente invenção podem ser ligados a serviços de provedor de serviços da Internet (ISP), para a provisão de uma solução única de ISP de provedor, para clientes corporativos e outros institucionais. A implementação da invenção acima está bem na habilidade do praticamente comum das técnicas de software.

[00277] Embora a presente invenção tenha sido descrita, assim, em detalhes, com referência às modalidades preferidas e aos desenhos das mesmas, deve ser evidente para aqueles versados na técnica que várias adaptações e modificações da presente invenção podem ser realizadas sem se desviar do espírito e do escopo da invenção. Assim sendo, deve ser compreendido que a descrição detalhada e os desenhos em anexo, como estabelecido aqui acima não são pretendidos para limitarem o escopo da presente invenção, o qual deve ser inferido apenas a partir das reivindicações a seguir e de seus equivalentes legais construídos apropriadamente. Nas reivindicações a seguir, pretende-se que aquelas reivindicações as quais contêm as palavras "meios para" sejam interpretadas de acordo com o 35 U.S.C. § 112, parágrafo 6; pretende-se que aquelas reivindicações as quais não contêm as palavras "meios para" não sejam interpretadas de acordo com o 35 U.S.C. § 112, parágrafo 6.

REIVINDICAÇÕES

1. Método de documentar o envio e o conteúdo de uma mensagem eletrônica que compreende as etapas de:

receber uma mensagem eletrônica de um remetente de mensagem (10), a mensagem eletrônica tendo pelo menos um endereço de destino eletrônico designado, associado com a ela;

transmitir a mensagem eletrônica ao dito endereço designado;

receber informação de notificação do estado de envio eletrônico referente ao envio da mensagem eletrônica ao endereço designado;

montar uma cópia de pelo menos uma porção da mensagem, e a informação de notificação de estado de envio, a dita montagem definindo um recibo eletrônico (20);

transmitir o recibo a um meio de armazenamento;

caracterizado pelo fato de que compreende ainda:

computar um código de autenticação de mensagem correspondente a pelo menos a mensagem, e em que a etapa de montar compreende ainda montar o código de autenticação de mensagem.

2. Método de acordo com a reivindicação 1, caracterizado pelo fato de que a transmissão do recibo (20) a um meio de armazenamento compreende transmitir o recibo (20) ao remetente de mensagem (10), e sendo que a mensagem original (12) é descartada após a transmissão do recibo eletrônico (20) ao remetente (10);

um recibo com significado e uma mensagem com significado e um código de autenticação de mensagem associado a ele são recebidos, e sendo que uma determinação é feita para saber se o código de autenticação de mensagem com sentido refere-se à mensagem.

3. Método de acordo com a reivindicação 1, caracterizado

pelo fato de que a etapa de computar um código de autenticação compreende:

computar um primeiro sumário de mensagem correspondente a pelo menos um corpo da mensagem;

computar um segundo sumário de mensagem correspondente a um anexo à mensagem;

computar um sumário de mensagem geral correspondente ao dito primeiro e ao dito segundo sumários de mensagem; e

criptografar o dito sumário de mensagem geral para criar uma impressão digital.

4. Método de acordo com qualquer uma das reivindicações 1 a 3, caracterizado pelo fato de que a computação de um código de autenticação de mensagem compreende:

computar um sumário de mensagem, que é um algoritmo de cabeçalho, correspondente a pelo menos a mensagem e a informação de notificação do estado de envio eletrônico.

5. Método de fornecer prova referente ao envio e ao conteúdo de uma mensagem eletrônica que compreende as etapas de:

receber de um remetente (10), através de uma rede de computadores, uma mensagem eletrônica, a dita mensagem tendo um endereço de envio associado a ela;

enviar a dita mensagem eletronicamente a um destino correspondente ao dito endereço de envio;

receber informação de notificação do estado de envio associada à dita mensagem e ao dito endereço de envio;

fornecer ao dito remetente (10) um recibo eletrônico (20) incluindo: uma parte de uma cópia da mensagem, e a dita informação de notificação do estado de envio;

receber eletronicamente, em uma data futura, o dito recibo eletrônico (20) do dito remetente (10);

verificar se a dita mensagem foi recebida por um manipulador de mensagem eletrônica associado ao dito endereço de envio;

enviar a dita mensagem a uma pluralidade de destinos adicionais correspondentes aos endereços de envio adicionais associados à mensagem;

caracterizado pelo fato de que o recibo eletrônico (20) compreende ainda um sumário de mensagem computado substancialmente a partir da dita cópia de mensagem e da dita informação de notificação do estado de envio; e

o método compreendendo ainda a etapa de verificar se o dito sumário de mensagem corresponde à dita mensagem.

6. Método de acordo com a reivindicação 5, caracterizado pelo fato de que compreende as etapas de:

receber informação adicional de notificação do estado de envio, associada à dita mensagem e aos ditos endereços de envio adicionais;

enviar uma mensagem de verificação de envio ao remetente, a mensagem de verificação de envio incluindo:

uma lista de todos os endereços; e

a dita informação de notificação do estado de envio respectivamente correspondente a todos os ditos endereços, a dita informação de notificação do estado de envio incluindo, para cada destinatário, uma listagem indicando se o envio foi bem-sucedido ou não e, se o envio foi bem-sucedido, a data e a hora em que o envio ocorreu.

7. Método de verificar se uma mensagem eletrônica foi enviada que compreende as etapas de:

gerar uma mensagem eletrônica para um destinatário (18) de informação recebida de um originador de mensagem;

enviar a mensagem eletrônica ao destinatário (18);

enviar a mensagem eletrônica ao originador de mensagem;

caracterizado pelo fato de que compreende ainda as etapas de:

gerar um sumário de mensagem correspondente ao conteúdo da mensagem eletrônica;

criptografar o sumário de mensagem; e

enviar o sumário criptografado ao originador de mensagem.

8. Método de informar posteriormente que uma mensagem eletrônica foi enviada anteriormente a um destinatário (18) que compreende as etapas de:

receber de uma parte independente uma mensagem eletrônica, e ainda receber um endereço correspondente a um determinado destinatário (18) da mensagem;

enviar a mensagem ao destinatário (18);

caracterizado pelo fato de que compreende ainda:

criar um código de validação correspondente à mensagem;

transmitir o código de validação a um meio de armazenamento para armazenagem no mesmo.

9. Método de informar que uma mensagem eletrônica enviada a um destinatário foi lida que compreende as etapas de:

receber uma mensagem eletrônica e um endereço de destinatário;

despachar a mensagem eletrônica eletronicamente para o endereço do destinatário;

solicitar uma notificação de leitura;

ao receber a notificação de leitura, gerar pelo menos um recibo de leitura (20), o dito pelo menos um recibo de leitura (20) incluindo uma cópia da mensagem;

fornecer o recibo de leitura (20) para verificação posterior de que a dita mensagem foi recebida pelo destinatário (18);

caracterizado pelo fato de que compreende ainda:

calcular um sumário de mensagem correspondente à mensagem eletrônica;

em que o dito pelo menos um recibo de leitura (20) inclui ainda:

um primeiro sumário de mensagem para a mensagem eletrônica correspondente; e

um segundo sumário de mensagem para a notificação de leitura do destinatário (18).

10. Método de validar a integridade de uma cópia com significado de uma mensagem eletrônica caracterizado pelo fato de que compreende as etapas de:

receber a dita cópia de mensagem eletrônica com significado, a dita cópia com significado incluindo uma assinatura digital e um histórico de transmissão associado a ele;

descriptografar a dita assinatura digital;

gerar um sumário de mensagem baseado na cópia com significado; e

validar a cópia com significado comparando a assinatura descriptografada e o sumário de mensagem para determinar se os dois coincidem.

11. Método de documentar o envio de uma mensagem de e-mail que compreende as etapas de:

receber uma mensagem de e-mail (70) de um remetente (60);

remeter a mensagem (70) a pelo menos um destinatário designado (68);

gravar informação de envio associada à remessa da mensagem (70) ao dito pelo menos um destinatário designado (68);

caracterizado pelo fato de que compreende ainda as etapas

de:

computar um sumário de mensagem correspondente à dita mensagem (70) e informação de envio;

transmitir o sumário de mensagem ao remetente (60);

descartar a mensagem (70); e

examinar posteriormente a dita mensagem (70), a dita informação de envio e o dito sumário de mensagem (70); e

proporcionar serviços de verificação de terceiros atestando que a dita mensagem (70) foi enviada ao destinatário designado (80) na hora indicada dentro da informação de envio.

12. Método de acordo com a reivindicação 11, caracterizado pelo fato de que compreende ainda as etapas de:

programar um agente de transporte de mensagem associado ao dito remetente (60) para redirecionar mensagem de e-mail (70) que sai, originalmente endereçada ao dito receptor designado, para um terceiro designado, e alterar a dita mensagem (70) para incluir o endereço de e-mail do dito destinatário designado;

e sendo que o dito terceiro realiza as etapas de remessa, gravação, computação e transmissão; e

fazer com que o remetente (60) de mensagem designe uma determinada mensagem de saída como mensagem a ser gravada.

13. Método de documentar o envio e conteúdo de uma mensagem eletrônica que compreende as etapas de:

gravar trocas de protocolo de mensagem eletrônica que efetuam envio da mensagem a uma autoridade de transporte de correspondência de destino (MTA);

montar uma cópia de pelo menos uma primeira porção da mensagem, e as trocas de protocolo, a dita montagem definindo um recibo eletrônico (20); e

transmitir o recibo (20) a um meio de armazenamento;

caracterizado pelo fato de que a etapa de montagem compreende ainda montar um código de autenticação correspondente a pelo menos uma segunda porção da mensagem.

14. Método de acordo com a reivindicação 13, caracterizado pelo fato de que compreende ainda as etapas de: montar e enviar um relatório de envio que, para cada envio bem-sucedido da mensagem, indica se o sistema é capaz de verificar, com base nas ditas trocas de protocolo gravadas, envio da dita mensagem a um servidor de correspondência de um destino ou, alternativamente, se o sistema é capaz de verificar, com base em uma notificação MTA, envio da mensagem a uma caixa postal eletrônica correspondente ao destino.

15. Método de transmitir uma mensagem de um remetente a um destinatário via um servidor afastado do destinatário, que inclui as etapas de:

receber a mensagem no servidor a partir do remetente (10),

transmitir do servidor para destinatário (18) a mensagem e o endereço do servidor e uma indicação representando a identidade do remetente (10),

receber, no servidor, do destinatário (18) um cumprimento e histórico de envio da mensagem do servidor para o destinatário (18), e

transmitir do servidor para o remetente (10) a mensagem e o cumprimento e histórico de envio da mensagem;

caracterizado pelo fato de que compreende ainda:

transmitir do servidor para o remetente (10) uma impressão digital criptografada da mensagem.

16. Método de acordo com a reivindicação 15, caracterizado pelo fato de que:

o servidor recebe do remetente (10) uma cópia da informa-

ção enviada anteriormente pelo servidor ao remetente (10), esta informação incluindo a impressão digital criptografada e a mensagem e o cumprimento e histórico de envio da mensagem, quando o remetente (10) deseja ter a mensagem autenticada pelo servidor, e sendo que:

o servidor não retém uma cópia de informação transmitida do servidor para o remetente (10), depois que o servidor transmite ao remetente a mensagem, a impressão digital criptografada da mensagem e do cumprimento e histórico de envio da mensagem.

17. Método de acordo com a reivindicação 15 ou 16, caracterizado pelo fato de que o servidor utiliza a informação recebida pelo servidor do remetente (10) para criar uma impressão digital da mensagem e uma impressão digital da impressão digital criptografada e compara estas impressões digitais para autenticar a mensagem recebida pelo servidor do remetente (10).

18. Método de transmitir uma mensagem de um remetente (10) para um destinatário (18) via um servidor afastado do destinatário (18), que inclui as etapas no servidor de:

receber a mensagem no servidor a partir do remetente (18);

gerar um “hash” constituindo uma sinopse da mensagem em forma codificada,

transmitir a mensagem ao remetente;

caracterizado pelo fato de que compreende ainda:

criptografar o “hash” como um determinado código de criptografia para gerar uma impressão digital criptografada da mensagem, e

transmitir a impressão digital criptografada da mensagem ao remetente (10).

19. Método de acordo com a reivindicação 18, caracterizado pelo fato de que inclui as etapas no servidor de:

gerar, para qualquer anexo da mensagem, um "hash" cons-

tituindo uma sinopse do anexo em forma codificada,

criptografar o hash com um determinado código de criptografia para gerar uma impressão digital criptografada do anexo; e

transmitir o anexo e a impressão digital criptografada do anexo ao remetente ao mesmo tempo que a mensagem e a impressão digital criptografada da mensagem são transmitidas do servidor ao remetente.

20. Método de acordo com a reivindicação 19, caracterizado pelo fato de que inclui as etapas no servidor de:

remover a mensagem e a impressão digital criptografada da mensagem a partir do servidor após a transmissão da mensagem e da impressão digital criptografada da mensagem do servidor para o remetente (10), e

remover o anexo, e a impressão digital criptografada do anexo, a partir do servidor após a transmissão do anexo e da impressão digital criptografada do anexo do servidor ao remetente (10).

21. Método de acordo com qualquer uma das reivindicações 18 a 20, caracterizado pelo fato de que inclui a etapa de autenticar a mensagem, com base na mensagem, e a impressão digital criptografada da mensagem, transmitida do remetente (10) ao servidor.

22. Método de acordo com qualquer uma das reivindicações 18 a 21, caracterizado pelo fato de que inclui a etapa de autenticar no servidor a mensagem recebida pelo servidor a partir do remetente (10), com base na mensagem, e na impressão digital criptografada da mensagem, transmitida do remetente (10) ao servidor, a autenticação sendo provida gerando-se a impressão digital da mensagem recebida pelo servidor a partir do remetente (10) e da impressão digital da impressão digital criptografada e comparando a impressão digital, e indicando a autenticação quando as impressões digitais são as mesmas.

23. Método de acordo com qualquer uma das reivindicações 18 a 22, caracterizado pelo fato de que inclui as etapas no servidor de:

receber um anexo do destinatário (18);

prover no servidor uma impressão digital criptografada do anexo;

transmitir ao remetente (10), ao mesmo tempo que a transmissão da mensagem e da impressão digital criptografada da mensagem, o anexo e a impressão digital criptografada do anexo;

receber do remetente (10) cópias da mensagem e do anexo da mensagem e das impressões digitais criptografadas da mensagem e do anexo;

respectivamente comparar o que foi recebido do remetente (10) em relação à mensagem, e o que foi recebido do remetente (10) em relação ao anexo, para autenticar a mensagem e o anexo com base nestas comparações.

24. Método de verificar em um primeiro servidor o envio de uma mensagem eletrônica do primeiro servidor para um servidor de destino a um endereço de destino, que inclui as etapas de:

receber no primeiro servidor uma mensagem eletrônica de um remetente (10) de mensagem para encaminhar ao servidor de destino;

transmitir do primeiro servidor ao servidor de destino a mensagem eletrônica e as transações entre o primeiro servidor e o servidor de destino em relação à mensagem eletrônica via um protocolo selecionado de um grupo que inclui um protocolo SMTP e um protocolo ESMTP,

gravar no primeiro servidor as transações entre o primeiro servidor e o servidor de destino via o protocolo selecionado do grupo que inclui o protocolo SMTP e o protocolo ESMTP,

transmitir do primeiro servidor ao remetente (10) a mensagem e as transações entre o primeiro servidor e o servidor de destino via um protocolo selecionado,

receber no primeiro servidor do remetente (10) a mensagem e as transações entre o primeiro servidor e o servidor de destino via um protocolo selecionado, e

caracterizado pelo fato de que compreende ainda a etapa de autenticar a mensagem no primeiro servidor com base na mensagem recebida pelo primeiro servidor a partir do remetente (10) e as transações recebidas pelo primeiro servidor a partir do remetente (10).

25. Método de autenticar uma mensagem transmitida de um remetente via um servidor para um destinatário, caracterizado pelo fato de que inclui as etapas de:

proporcionar uma impressão digital criptografada da mensagem,

transmitir a mensagem e a impressão digital criptografada ao remetente (10),

receber a mensagem e a impressão digital criptografada do remetente (10), e

autenticar a mensagem com base na mensagem e na impressão digital criptografada recebidas pelo servidor do remetente (10).

26. Método de acordo com a reivindicação 25, caracterizado pelo fato de que:

o servidor recebe do remetente (10) um anexo incluindo uma identificação do remetente (10) e um endereço do servidor e uma identificação e endereço do destinatário (18) e uma impressão digital criptografada do anexo e da mensagem, e sendo que:

o servidor transmite ao remetente (10) a mensagem e uma impressão digital criptografada da mensagem e o anexo e a impressão

digital criptografada do anexo, e sendo que:

o servidor recebe a mensagem e o anexo e as impressões digitais criptografadas da mensagem e do anexo, e sendo que:

o servidor autentica a mensagem com base na mensagem e na impressão digital criptografada da mensagem e no anexo e na impressão digital criptografada, todos como recebidos pelo servidor a partir do remetente (10).

27. Método de acordo com qualquer uma das reivindicações 23 a 25, caracterizado pelo fato de que o servidor autentica a mensagem preparando as impressões digitais da mensagem e do anexo e as impressões digitais procedentes das impressões digitais criptografadas da mensagem e do anexo, e comparando as impressões digitais relativas à mensagem e confirmando se elas são idênticas e comparando as impressões digitais relativas ao anexo e confirmando se as impressões digitais comparadas são idênticas.

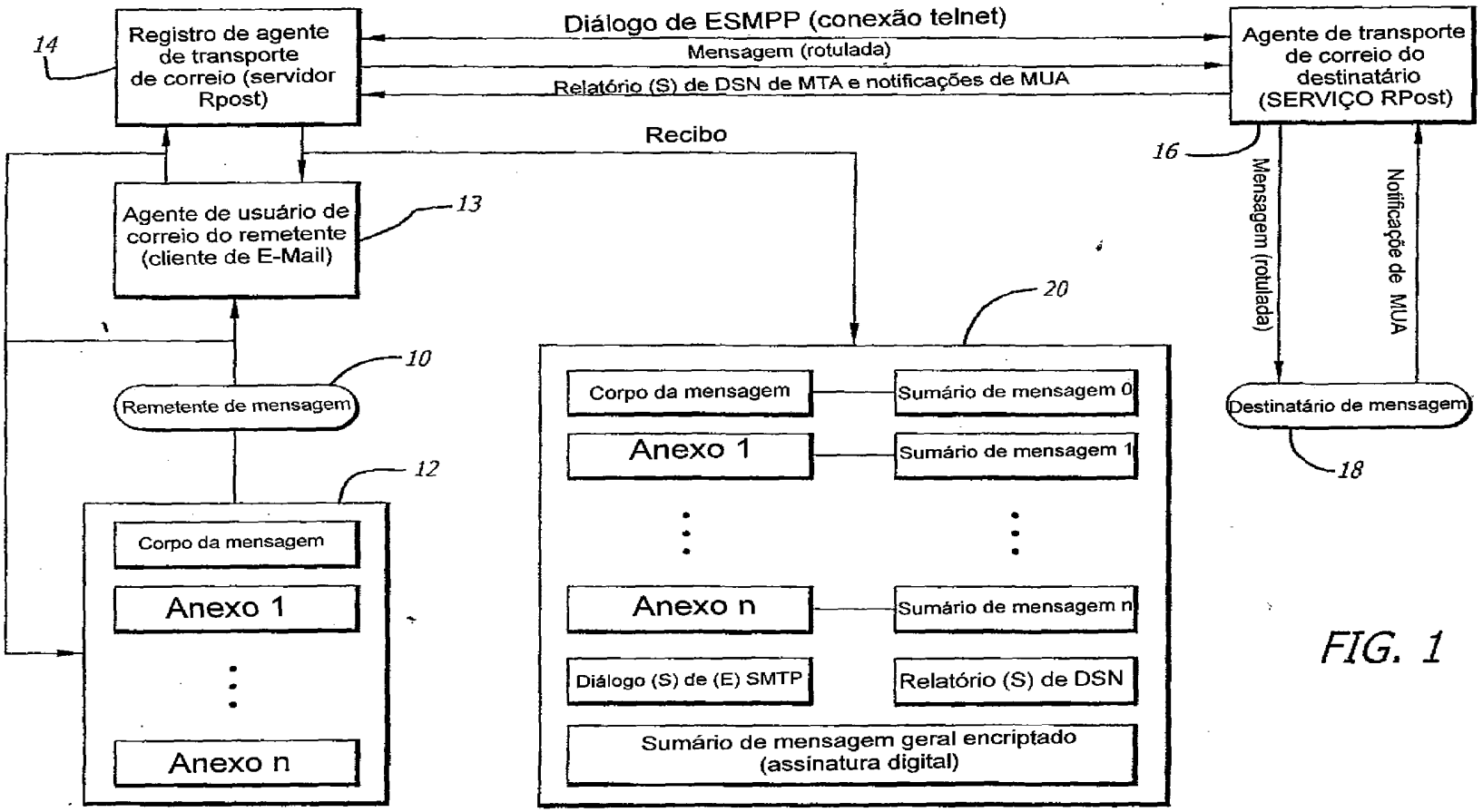

14
Registro de agente de transporte de correio (servidor Rpost)
Diálogo de ESMPP (conexão telnet)
Mensagem (rotulada)
Relatório (S) de DSN de MTA e notificações de MUA
Agente de transporte de correio do destinatário (SERVIÇO RPost)
Recibo
16
Mensagem (rotulada)
Notificação de MUA
Agente de usuário de correio do remetente (cliente de E-Mail)
13
20
10
Remetente de mensagem
Destinatário de mensagem
18
12
Corpo da mensagem
Anexo 1
Anexo n
Corpo da mensagem
Sumário de mensagem 0
Anexo 1
Sumário de mensagem 1
Anexo n
Sumário de mensagem n
Diálogo (S) de (E) SMTP
Relatório (S) de DSN
Sumário de mensagem geral encriptado (assinatura digital)

FIG. 1

FIG. 2A

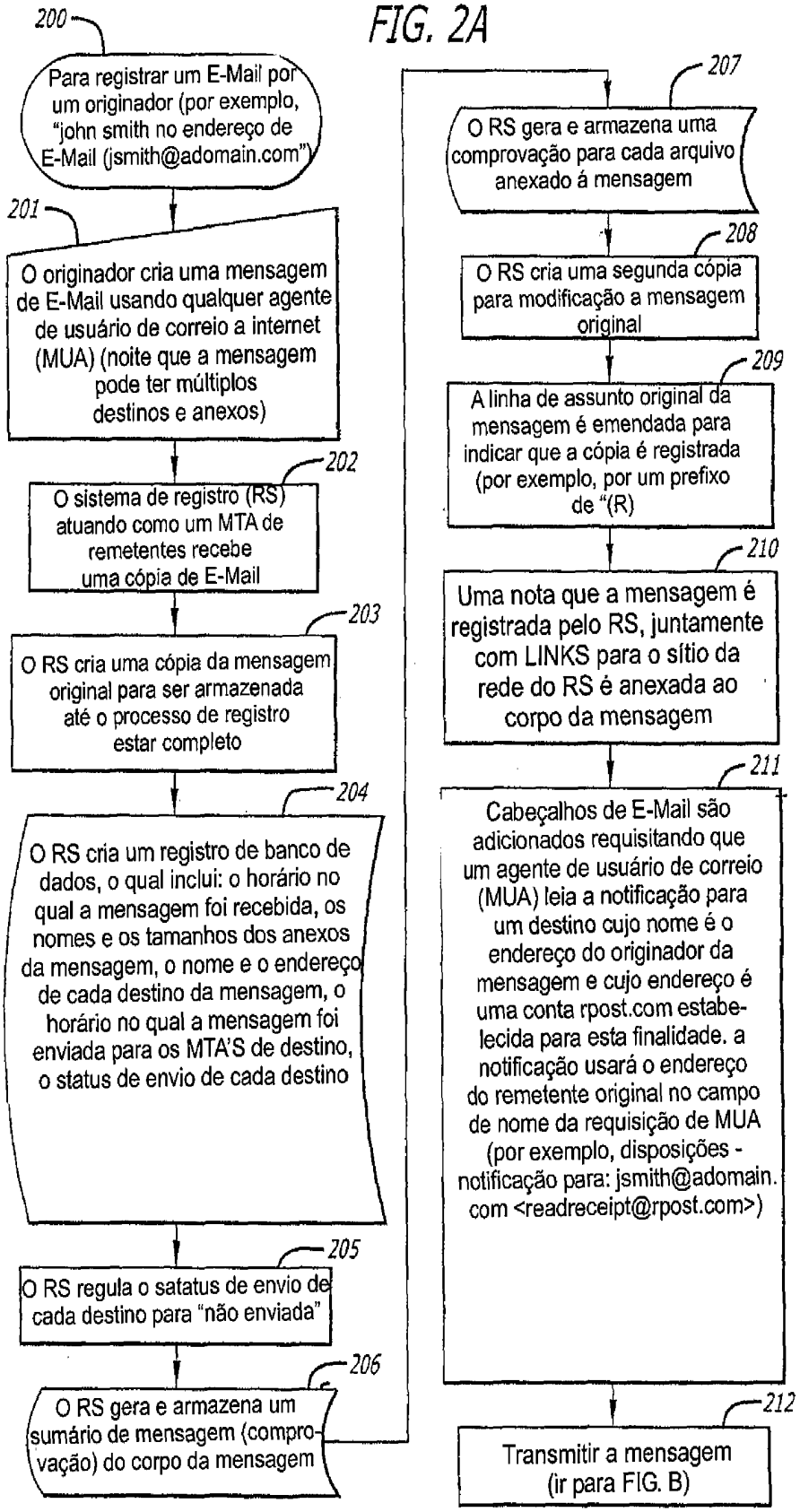
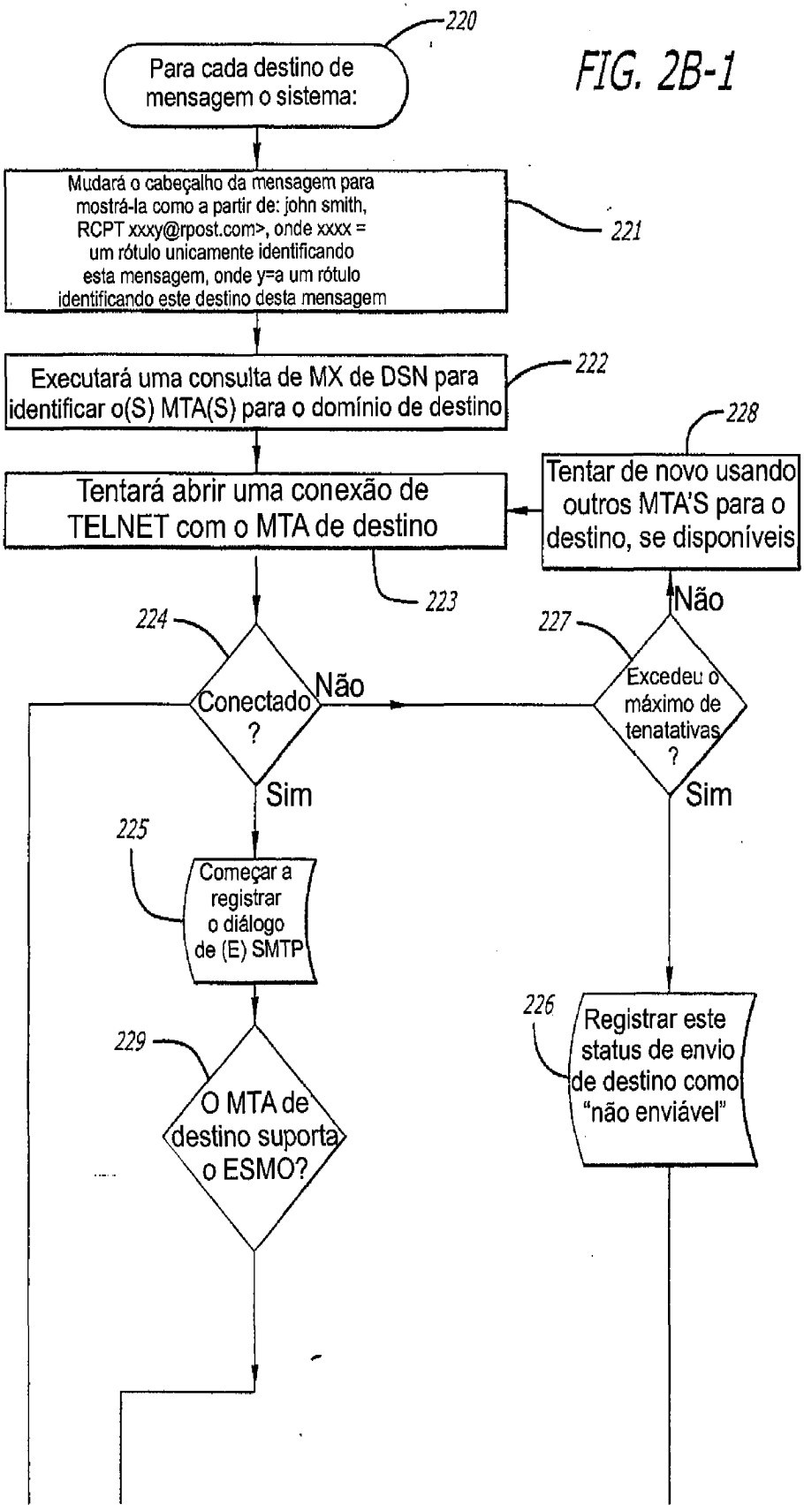

200
Para registrar um E-Mail por um originador (por exemplo, "john smith no endereço de E-Mail (jsmith@adomain.com")
201
O originador cria uma mensagem de E-Mail usando qualquer agente de usuário de correio a internet (MUA) (noite que a mensagem pode ter múltiplos destinos e anexos)
202
O sistema de registro (RS) atuando como um MTA de remetentes recebe uma cópia de E-Mail
203
O RS cria uma cópia da mensagem original para ser armazenada até o processo de registro estar completo
204
O RS cria um registro de banco de dados, o qual inclui: o horário no qual a mensagem foi recebida, os nomes e os tamanhos dos anexos da mensagem, o nome e o endereço de cada destino da mensagem, o horário no qual a mensagem foi enviada para os MTA'S de destino, o status de envio de cada destino
205
O RS regula o satatus de envio de cada destino para "não enviada"
206
O RS gera e armazena um sumário de mensagem (comprovação) do corpo da mensagem
207
O RS gera e armazena uma comprovação para cada arquivo anexado á mensagem
208
O RS cria uma segunda cópia para modificação a mensagem original
209
A linha de assunto original da mensagem é emendada para indicar que a cópia é registrada (por exemplo, por um prefixo de "(R)
210
Uma nota que a mensagem é registrada pelo RS, juntamente com LINKS para o sítio da rede do RS é anexada ao corpo da mensagem
211
Cabeçalhos de E-Mail são adicionados requisitando que um agente de usuário de correio (MUA) leia a notificação para um destino cujo nome é o endereço do originador da mensagem e cujo endereço é uma conta rpost.com estabelecida para esta finalidade. a notificação usará o endereço do remetente original no campo de nome da requisição de MUA (por exemplo, disposições - notificação para: jsmith@adomain.com <readreceipt@rpost.com>)
212
Transmitir a mensagem (ir para FIG. B)

FIG. 2B-1


220
Para cada destino de mensagem o sistema:
Mudará o cabeçalho da mensagem para mostrá-la como a partir de: john smith, RCPT xxxy@rpost.com>, onde xxxx = um rótulo unicamente identificando esta mensagem, onde y=a um rótulo identificando este destino desta mensagem
221
Executará uma consulta de MX de DSN para identificar o(S) MTA(S) para o domínio de destino
222
Tentará abrir uma conexão de TELNET com o MTA de destino
223
228
Tentar de novo usando outros MTA'S para o destino, se disponíveis
Não
224
Conectado ?
Não
227
Excedeu o máximo de tenatativas ?
Sim
Sim
225
Começar a registrar o diálogo de (E) SMTP
229
O MTA de destino suporta o ESMO?
226
Registrar este status de envio de destino como "não enviável"

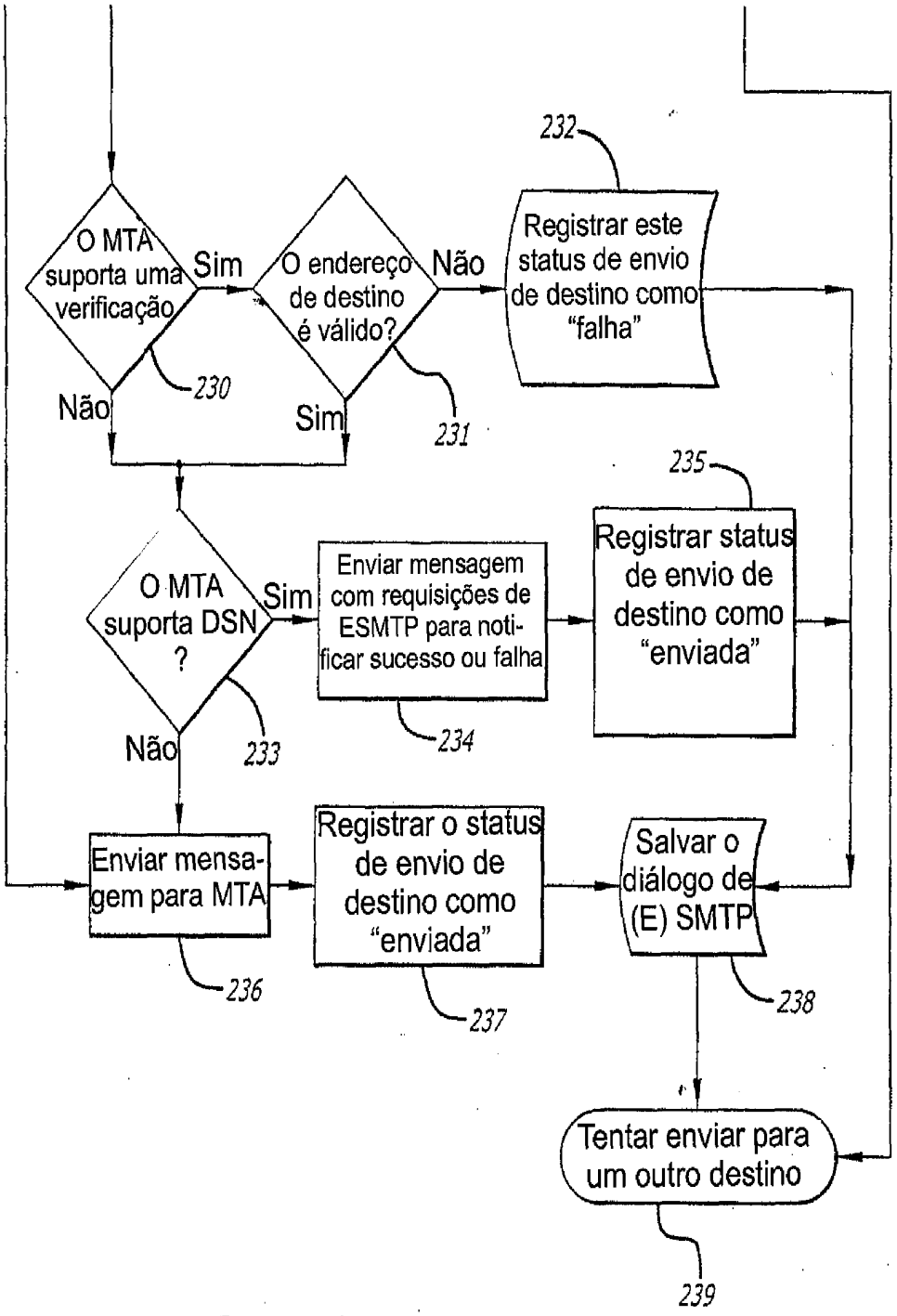

O MTA suporta uma verificação
Sim
O endereço de destino é válido?
Não
Registrar este status de envio de destino como "falha"
232
230
231
Não
Sim
O MTA suporta DSN ?
Sim
Enviar mensagem com requisições de ESMTP para notificar sucesso ou falha
Registrar status de envio de destino como "enviada"
235
233
234
Não
Enviar mensagem para MTA
Registrar o status de envio de destino como "enviada"
Salvar o diálogo de (E) SMTP
236
237
238
Tentar enviar para um outro destino
239

FIG. 2B-2

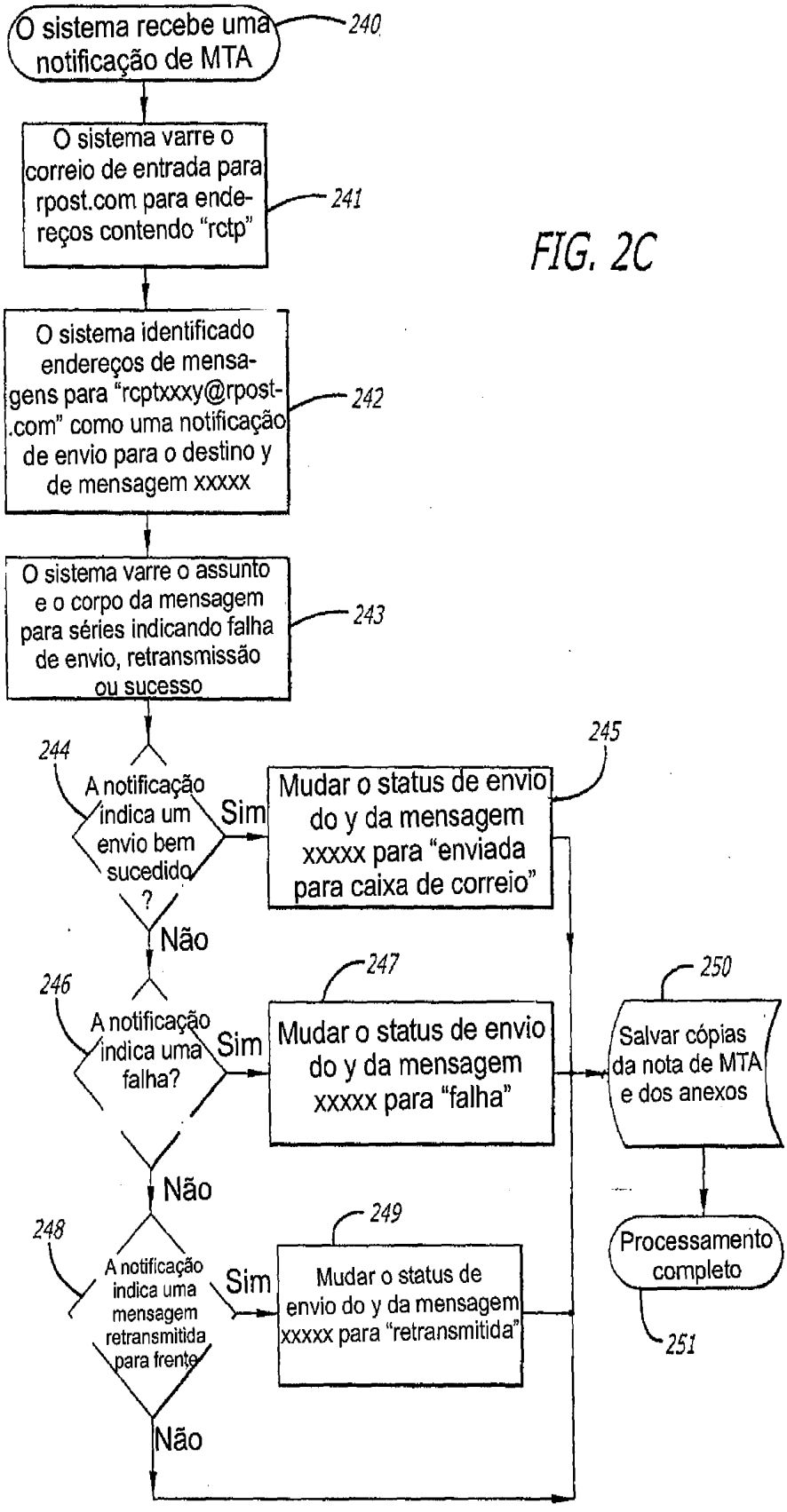

O sistema recebe uma notificação de MTA
240
O sistema varre o correio de entrada para rpost.com para endereços contendo "rctp"
241
O sistema identificado endereços de mensagens para "rcptxxxy@rpost-.com" como uma notificação de envio para o destino y de mensagem xxxxx
242
O sistema varre o assunto e o corpo da mensagem para séries indicando falha de envio, retransmissão ou sucesso
243
244
A notificação indica um envio bem sucedido ?
Sim
Não
245
Mudar o status de envio do y da mensagem xxxxx para "enviada para caixa de correio"
246
A notificação indica uma falha?
Sim
Não
247
Mudar o status de envio do y da mensagem xxxxx para "falha"
248
A notificação indica uma mensagem retransmitida para frente
Sim
Não
249
Mudar o status de envio do y da mensagem xxxxx para "retransmitida"
250
Salvar cópias da nota de MTA e dos anexos
Processamento completo
251

FIG. 2C

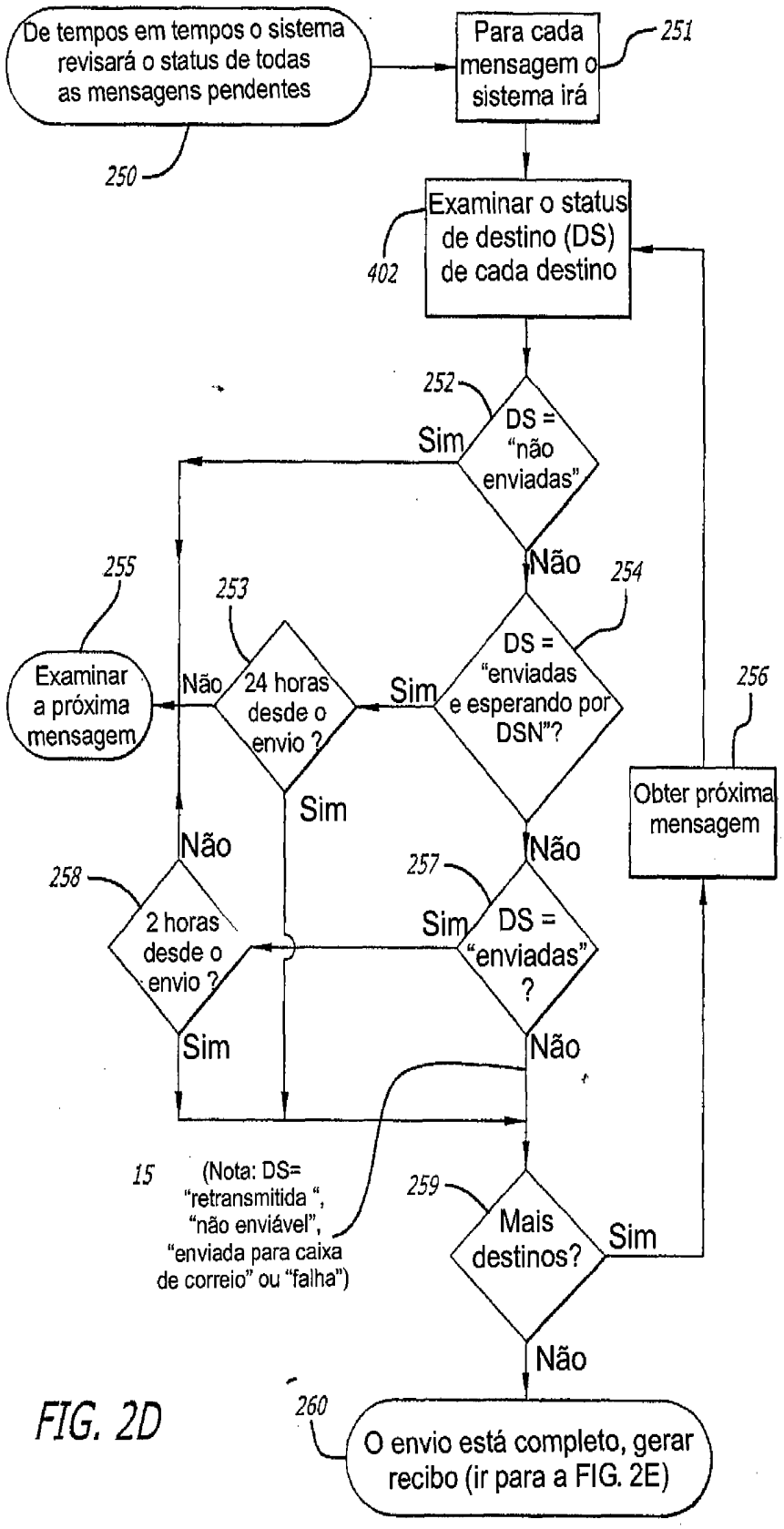
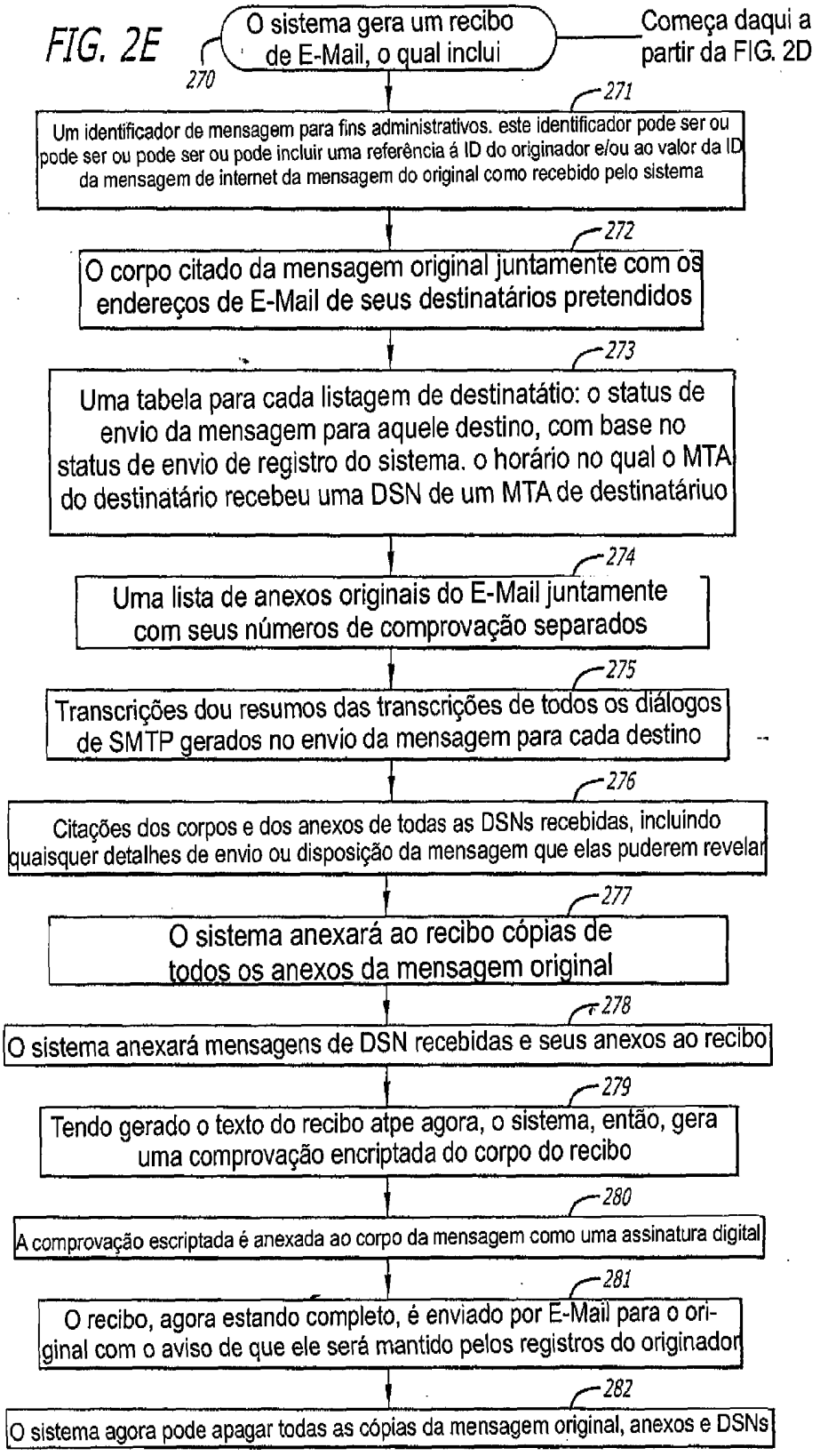

De tempos em tempos o sistema revisará o status de todas as mensagens pendentes
250
Para cada mensagem o sistema irá
251
Examinar o status de destino (DS) de cada destino
402
252
DS = "não enviadas"
Sim
Não
254
DS = "enviadas e esperando por DSN"?
Sim
253
24 horas desde o envio ?
Não
255
Examinar a próxima mensagem
Sim
Não
257
DS = "enviadas" ?
Sim
Não
258
2 horas desde o envio ?
Sim
Não
256
Obter próxima mensagem
15
(Nota: DS= "retransmitida ", "não enviável", "enviada para caixa de correio" ou "falha")
259
Mais destinos?
Sim
Não
260
O envio está completo, gerar recibo (ir para a FIG. 2E)

FIG. 2D

FIG. 2E


O sistema gera um recibo de E-Mail, o qual inclui
Começa daqui a partir da FIG. 2D
270
271
Um identificador de mensagem para fins administrativos. este identificador pode ser ou pode ser ou pode ser ou pode incluir uma referência á ID do originador e/ou ao valor da ID da mensagem de internet da mensagem do original como recebido pelo sistema
272
O corpo citado da mensagem original juntamente com os endereços de E-Mail de seus destinatários pretendidos
273
Uma tabela para cada listagem de destinatátio: o status de envio da mensagem para aquele destino, com base no status de envio de registro do sistema. o horário no qual o MTA do destinatário recebeu uma DSN de um MTA de destinatáriuo
274
Uma lista de anexos originais do E-Mail juntamente com seus números de comprovação separados
275
Transcrições dou resumos das transcrições de todos os diálogos de SMTP gerados no envio da mensagem para cada destino
276
Citações dos corpos e dos anexos de todas as DSNs recebidas, incluindo quaisquer detalhes de envio ou disposição da mensagem que elas puderem revelar
277
O sistema anexará ao recibo cópias de todos os anexos da mensagem original
278
O sistema anexará mensagens de DSN recebidas e seus anexos ao recibo
279
Tendo gerado o texto do recibo atpe agora, o sistema, então, gera uma comprovação encriptada do corpo do recibo
280
A comprovação escriptada é anexada ao corpo da mensagem como uma assinatura digital
281
O recibo, agora estando completo, é enviado por E-Mail para o original com o aviso de que ele será mantido pelos registros do originador
282
O sistema agora pode apagar todas as cópias da mensagem original, anexos e DSNs

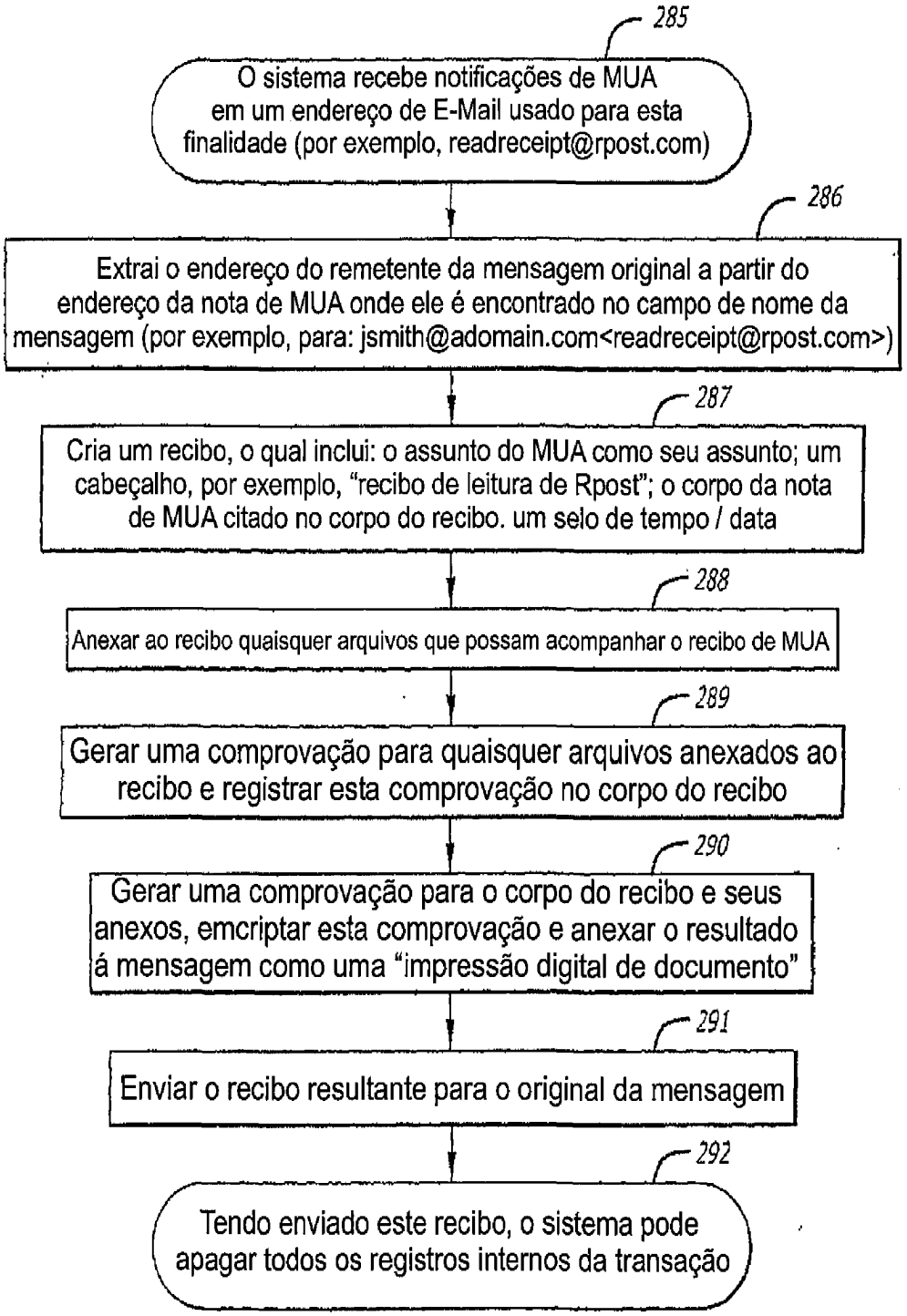

285
O sistema recebe notificações de MUA em um endereço de E-Mail usado para esta finalidade (por exemplo, readreceipt@rpost.com)
286
Extrai o endereço do remetente da mensagem original a partir do endereço da nota de MUA onde ele é encontrado no campo de nome da mensagem (por exemplo, para: jsmith@adomain.com<readreceipt@rpost.com>)
287
Cria um recibo, o qual inclui: o assunto do MUA como seu assunto; um cabeçalho, por exemplo, "recibo de leitura de Rpost"; o corpo da nota de MUA citado no corpo do recibo. um selo de tempo / data
288
Anexar ao recibo quaisquer arquivos que possam acompanhar o recibo de MUA
289
Gerar uma comprovação para quaisquer arquivos anexados ao recibo e registrar esta comprovação no corpo do recibo
290
Gerar uma comprovação para o corpo do recibo e seus anexos, emcriptar esta comprovação e anexar o resultado á mensagem como uma "impressão digital de documento"
291
Enviar o recibo resultante para o original da mensagem
292
Tendo enviado este recibo, o sistema pode apagar todos os registros internos da transação

FIG. 2F

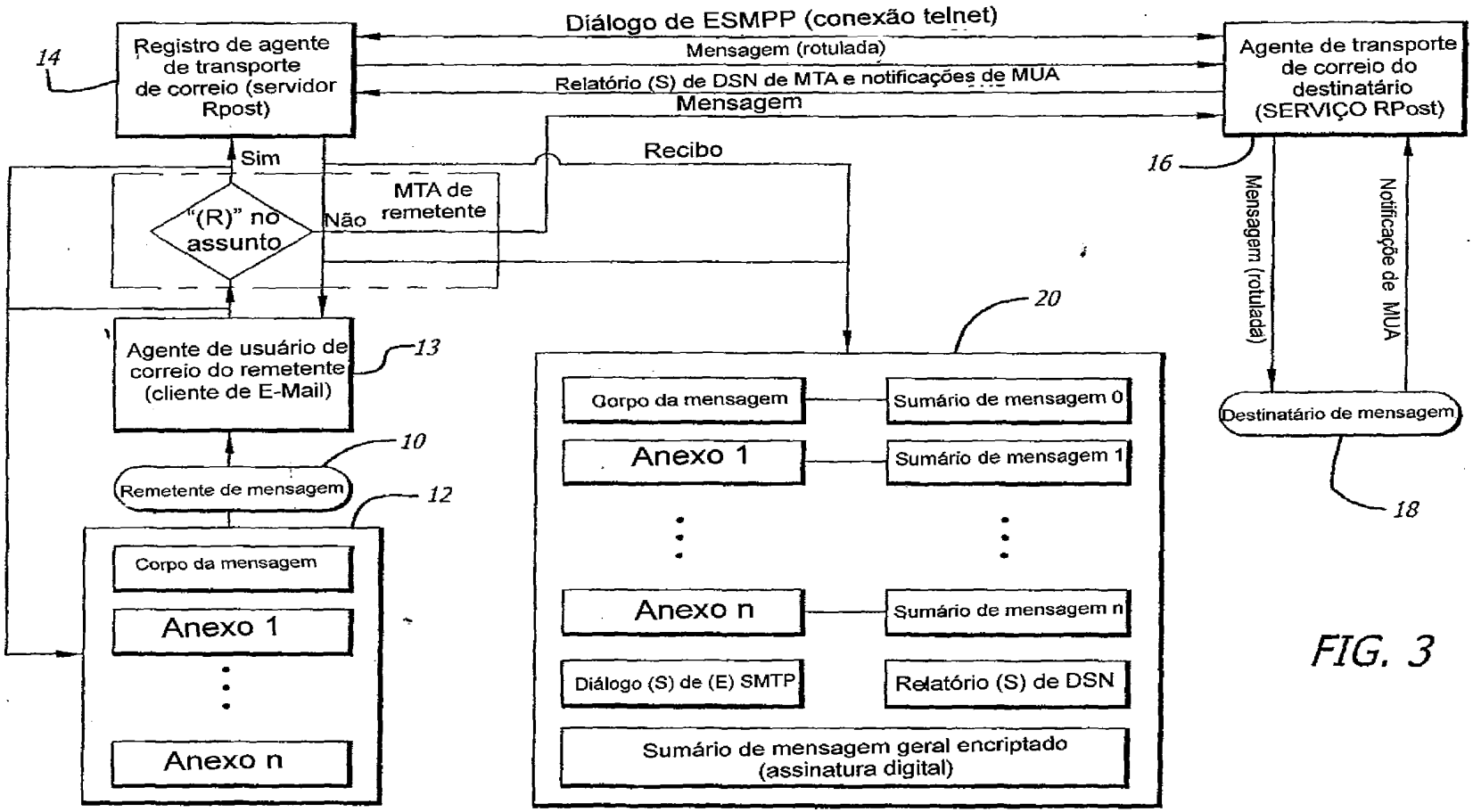

Diálogo de ESMPP (conexão telnet)
Mensagem (rotulada)
Relatório (S) de DSN de MTA e notificações de MUA
Mensagem
Recibo
14
Registro de agente de transporte de correio (servidor Rpost)
Agente de transporte de correio do destinatário (SERVIÇO RPost)
16
Sim
"(R)" no assunto
Não
MTA de remetente
Agente de usuário de correio do remetente (cliente de E-Mail)
13
10
Remetente de mensagem
12
Corpo da mensagem
Anexo 1
Anexo n
20
Corpo da mensagem
Sumário de mensagem 0
Anexo 1
Sumário de mensagem 1
Anexo n
Sumário de mensagem n
Diálogo (S) de (E) SMTP
Relatório (S) de DSN
Sumário de mensagem geral encriptado (assinatura digital)
Mensagem (rotulada)
Notificação de MUA
Destinatário de mensagem
18

FIG. 3

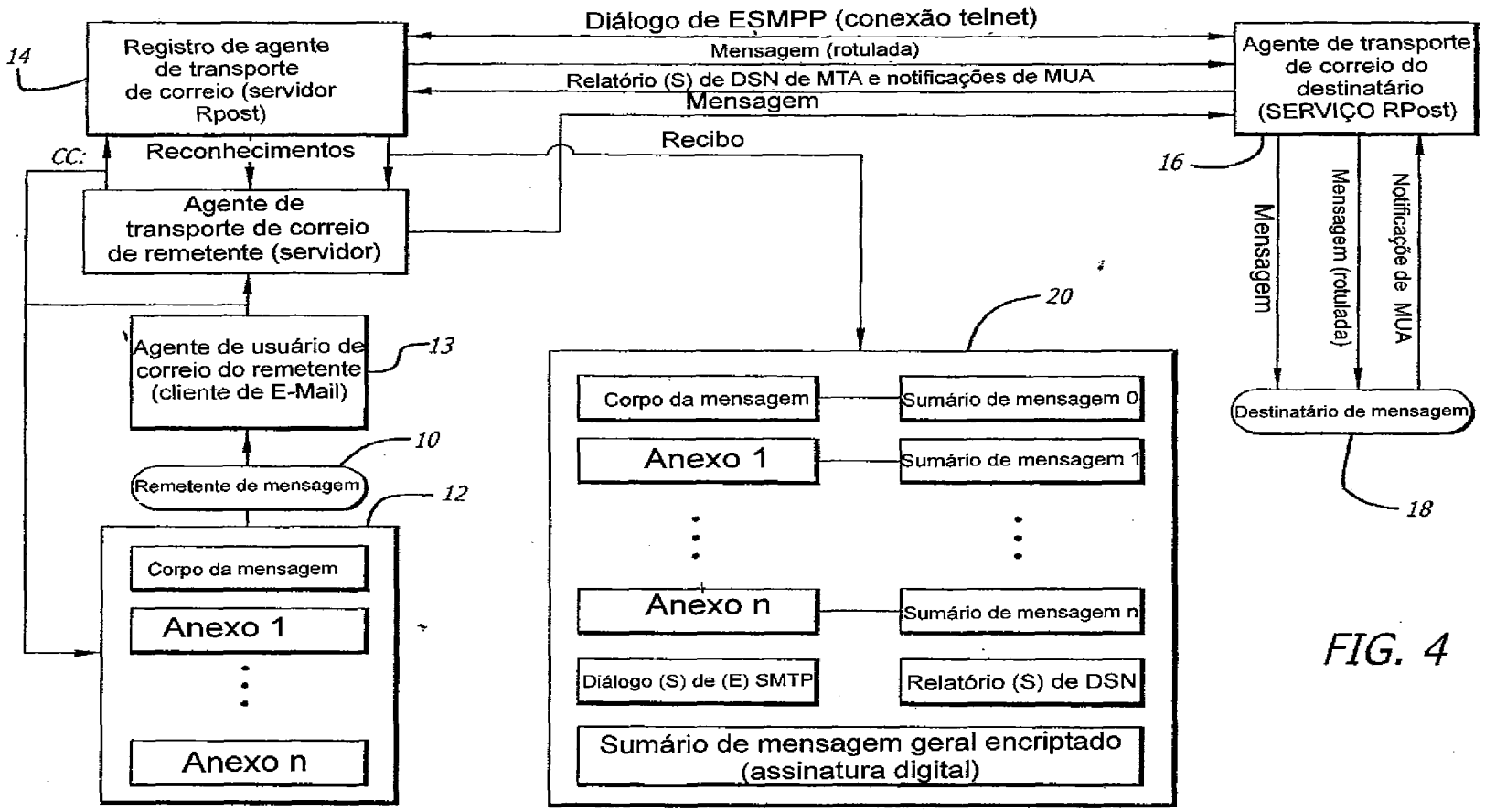

Diálogo de ESMPP (conexão telnet)
Mensagem (rotulada)
Relatório (S) de DSN de MTA e notificações de MUA
Mensagem
Recibo
14
Registro de agente de transporte de correio (servidor Rpost)
Agente de transporte de correio do destinatário (SERVIÇO RPost)
16
CC:
Reconhecimentos
Agente de transporte de correio de remetente (servidor)
Mensagem
Mensagem (rotulada)
Notificação de MUA
Destinatário de mensagem
18
Agente de usuário de correio do remetente (cliente de E-Mail)
13
10
Remetente de mensagem
12
Corpo da mensagem
Anexo 1
Anexo n
20
Corpo da mensagem
Sumário de mensagem 0
Anexo 1
Sumário de mensagem 1
Anexo n
Sumário de mensagem n
Diálogo (S) de (E) SMTP
Relatório (S) de DSN
Sumário de mensagem geral encriptado (assinatura digital)

FIG. 4

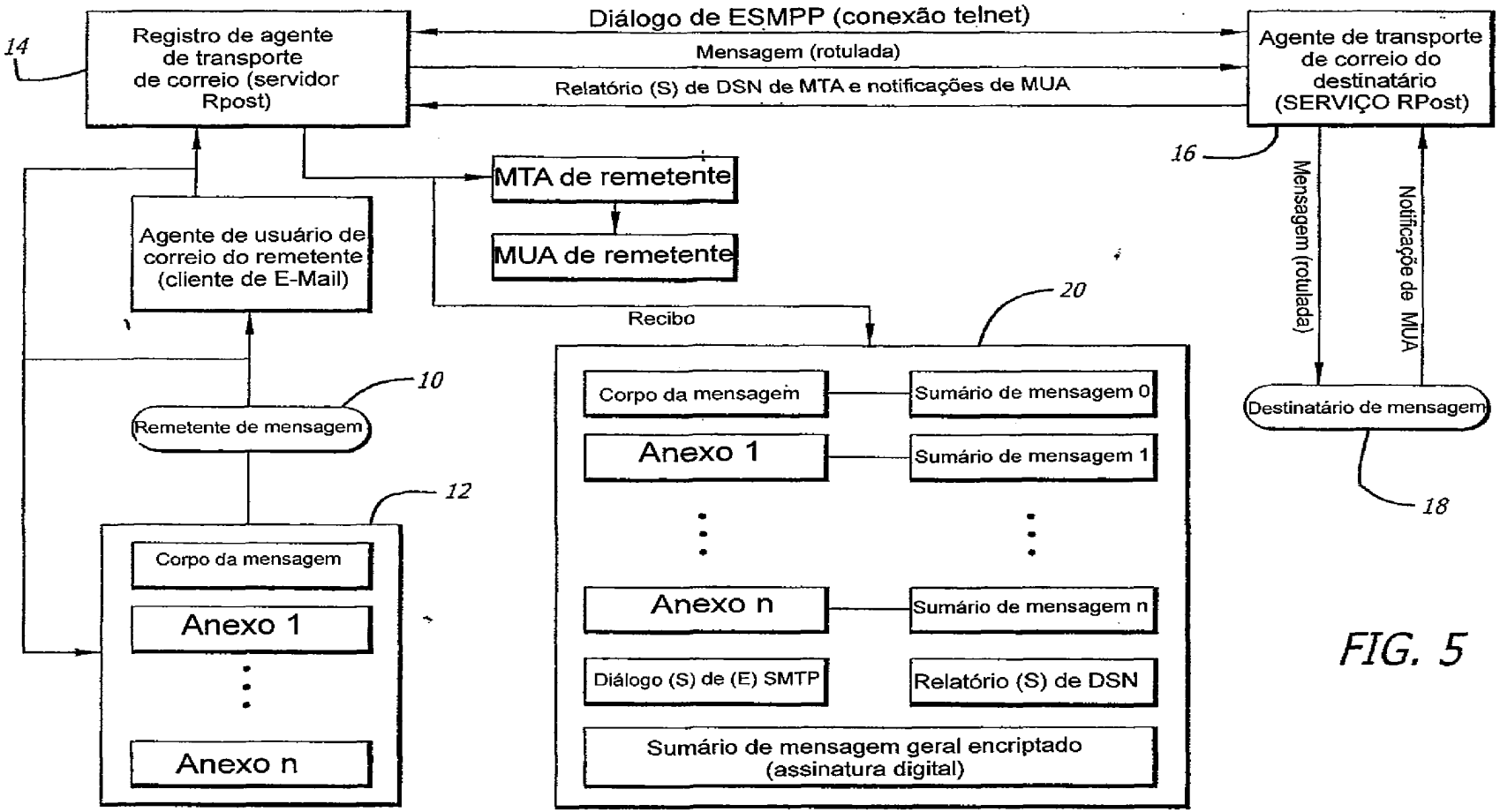

14
Registro de agente de transporte de correio (servidor Rpost)
Diálogo de ESMPP (conexão telnet)
Mensagem (rotulada)
Relatório (S) de DSN de MTA e notificações de MUA
Agente de transporte de correio do destinatário (SERVIÇO RPost)
16
MTA de remetente
MUA de remetente
Agente de usuário de correio do remetente (cliente de E-Mail)
Recibo
20
Mensagem (rotulada)
Notificação de MUA
10
Remetente de mensagem
Destinatário de mensagem
18
12
Corpo da mensagem
Anexo 1
Anexo n
Corpo da mensagem
Sumário de mensagem 0
Anexo 1
Sumário de mensagem 1
Anexo n
Sumário de mensagem n
Diálogo (S) de (E) SMTP
Relatório (S) de DSN
Sumário de mensagem geral encriptado (assinatura digital)

FIG. 5

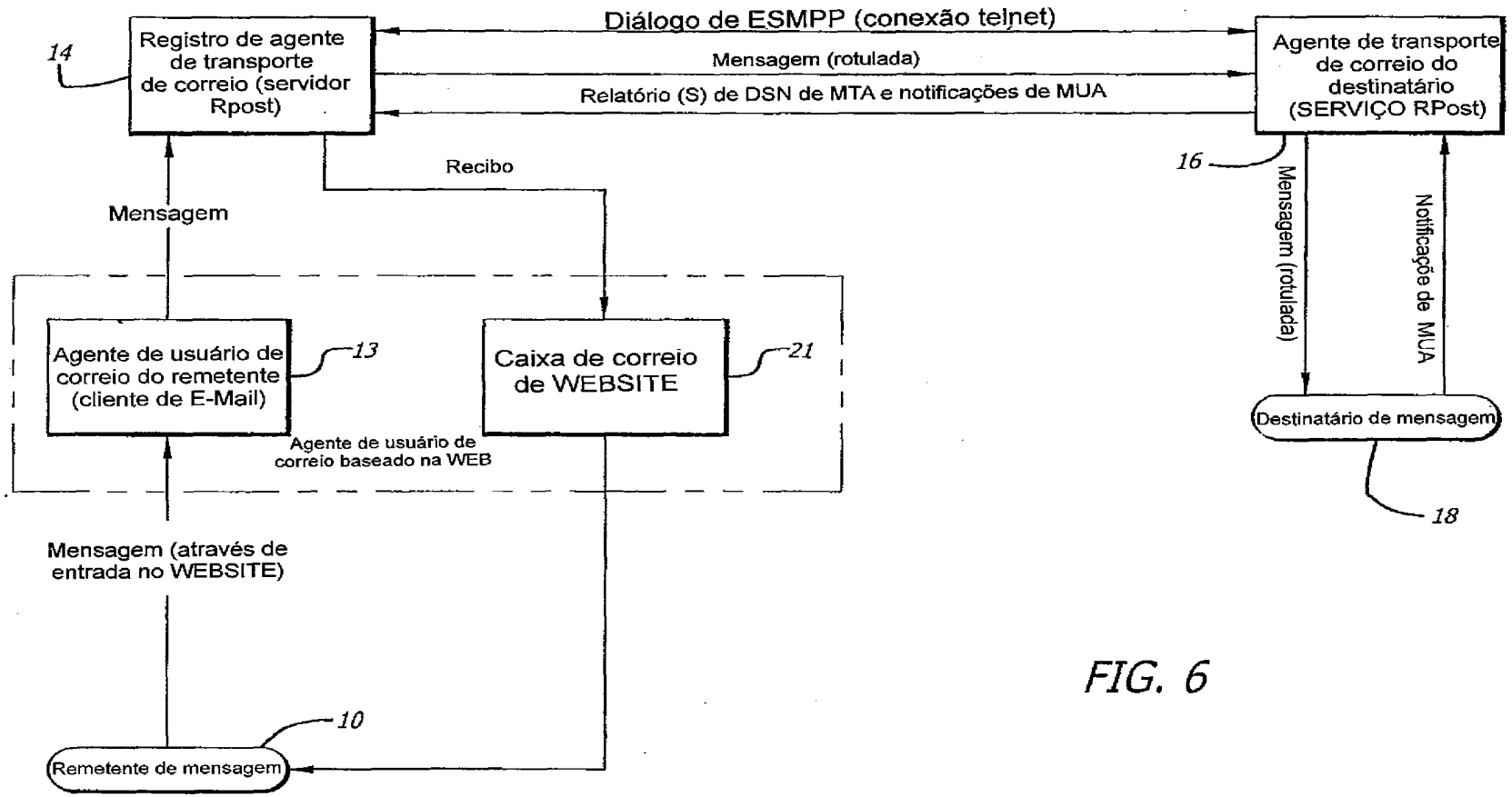

Diálogo de ESMPP (conexão telnet)
Mensagem (rotulada)
Relatório (S) de DSN de MTA e notificações de MUA
Registro de agente de transporte de correio (servidor Rpost)
14
Agente de transporte de correio do destinatário (SERVIÇO RPost)
16
Recibo
Mensagem
Mensagem (rotulada)
Notificação de MUA
Agente de usuário de correio do remetente (cliente de E-Mail)
13
Caixa de correio de WEBSITE
21
Agente de usuário de correio baseado na WEB
Destinatário de mensagem
18
Mensagem (através de entrada no WEBSITE)
10
Remetente de mensagem

FIG. 6

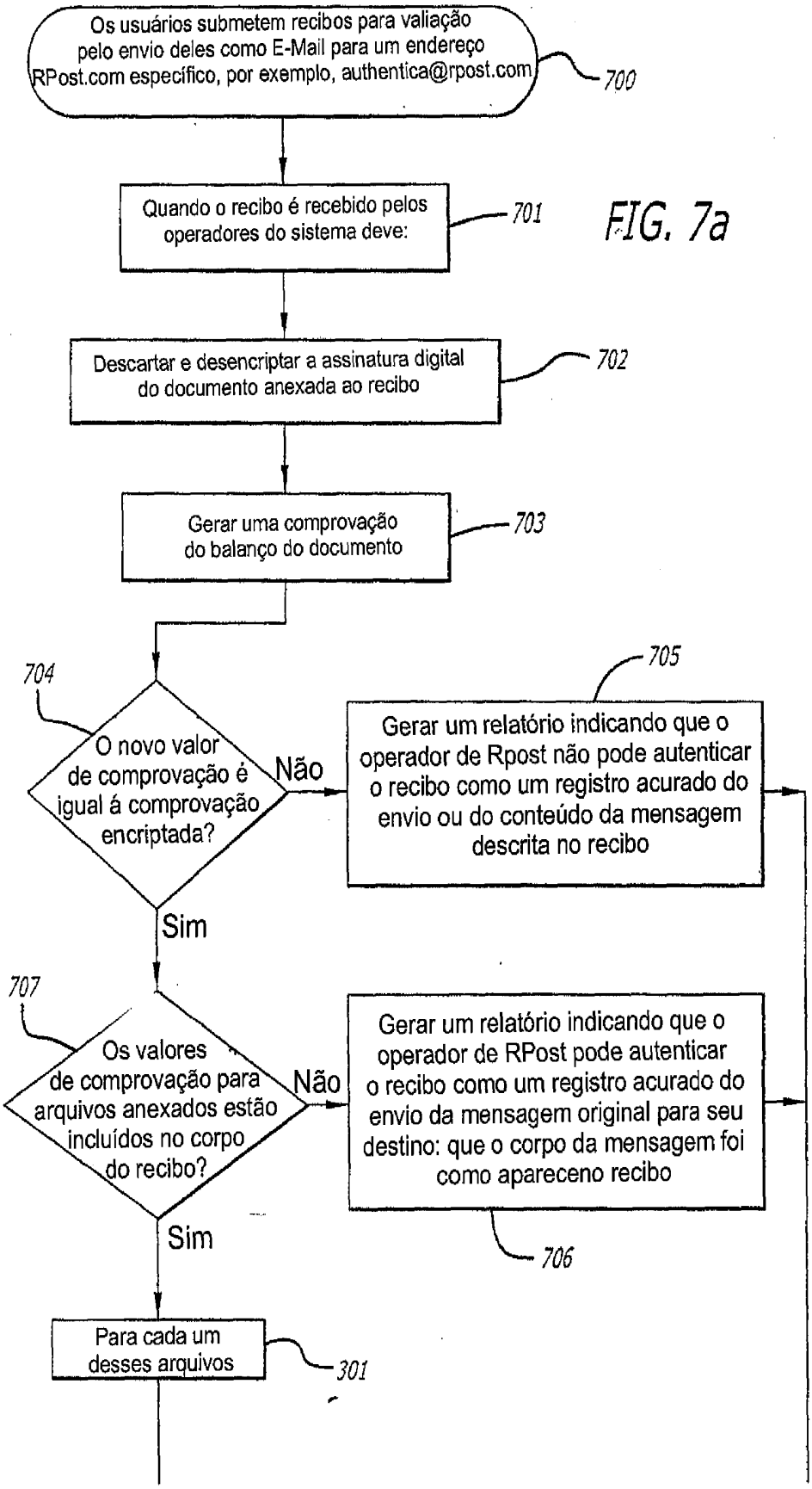

Os usuários submetem recibos para valiação pelo envio deles como E-Mail para um endereço RPost.com específico, por exemplo, authentica@rpost.com
700
Quando o recibo é recebido pelos operadores do sistema deve:
701
Descartar e desencriptar a assinatura digital do documento anexada ao recibo
702
Gerar uma comprovação do balanço do documento
703
704
O novo valor de comprovação é igual á comprovação encriptada?
Não
705
Gerar um relatório indicando que o operador de Rpost não pode autenticar o recibo como um registro acurado do envio ou do conteúdo da mensagem descrita no recibo
Sim
707
Os valores de comprovação para arquivos anexados estão incluídos no corpo do recibo?
Não
Gerar um relatório indicando que o operador de RPost pode autenticar o recibo como um registro acurado do envio da mensagem original para seu destino: que o corpo da mensagem foi como apareceno recibo
706
Sim
Para cada um desses arquivos
301

FIG. 7a

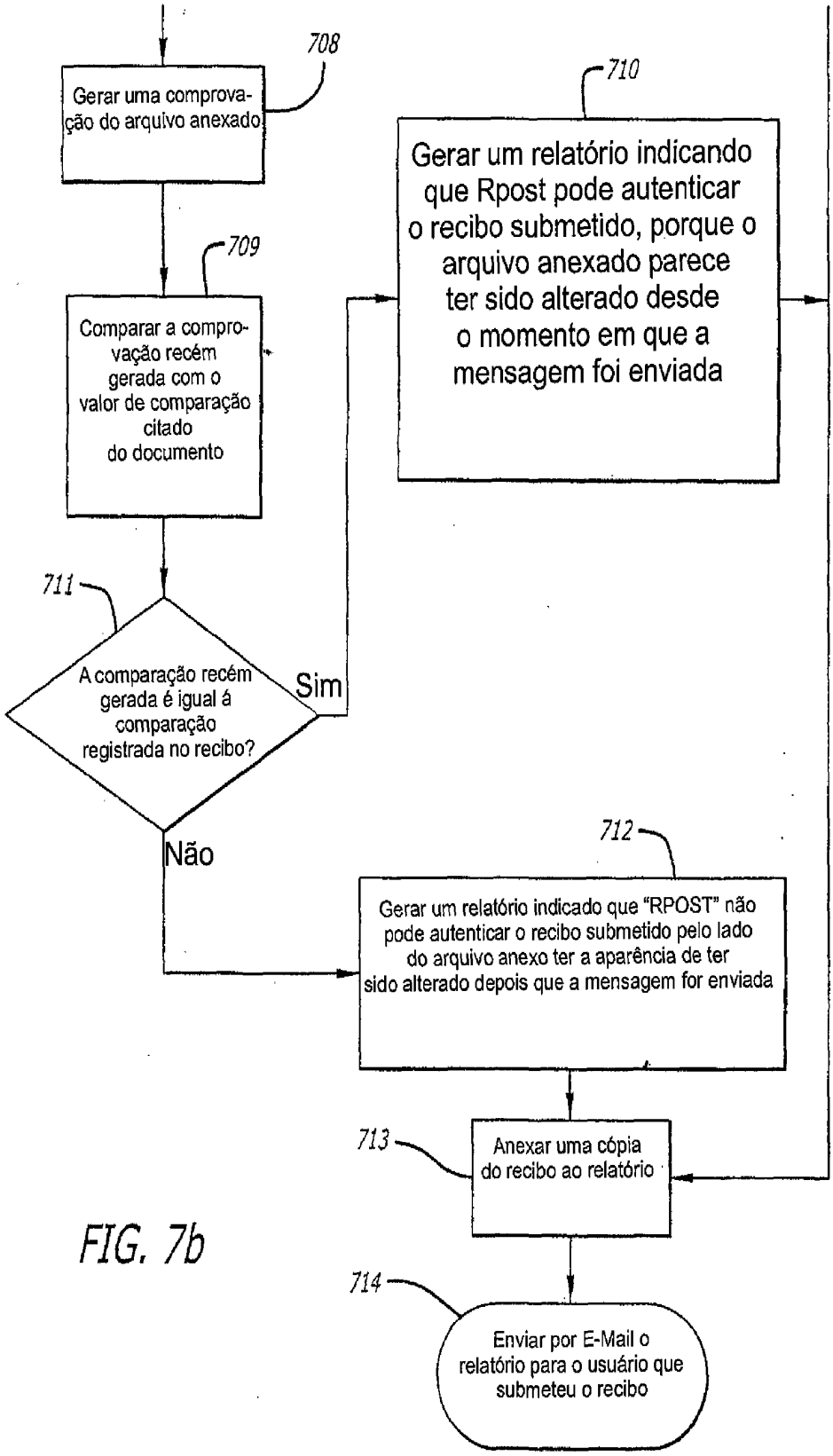

708
Gerar uma comprovação do arquivo anexado
709
Comparar a comprovação recém gerada com o valor de comparação citado do documento
711
A comparação recém gerada é igual á comparação registrada no recibo?
Sim
Não
710
Gerar um relatório indicando que Rpost pode autenticar o recibo submetido, porque o arquivo anexado parece ter sido alterado desde o momento em que a mensagem foi enviada
712
Gerar um relatório indicado que "RPOST" não pode autenticar o recibo submetido pelo lado do arquivo anexo ter a aparência de ter sido alterado depois que a mensagem for enviada
713
Anexar uma cópia do recibo ao relatório
714
Enviar por E-Mail o relatório para o usuário que submeteu o recibo

FIG. 7b

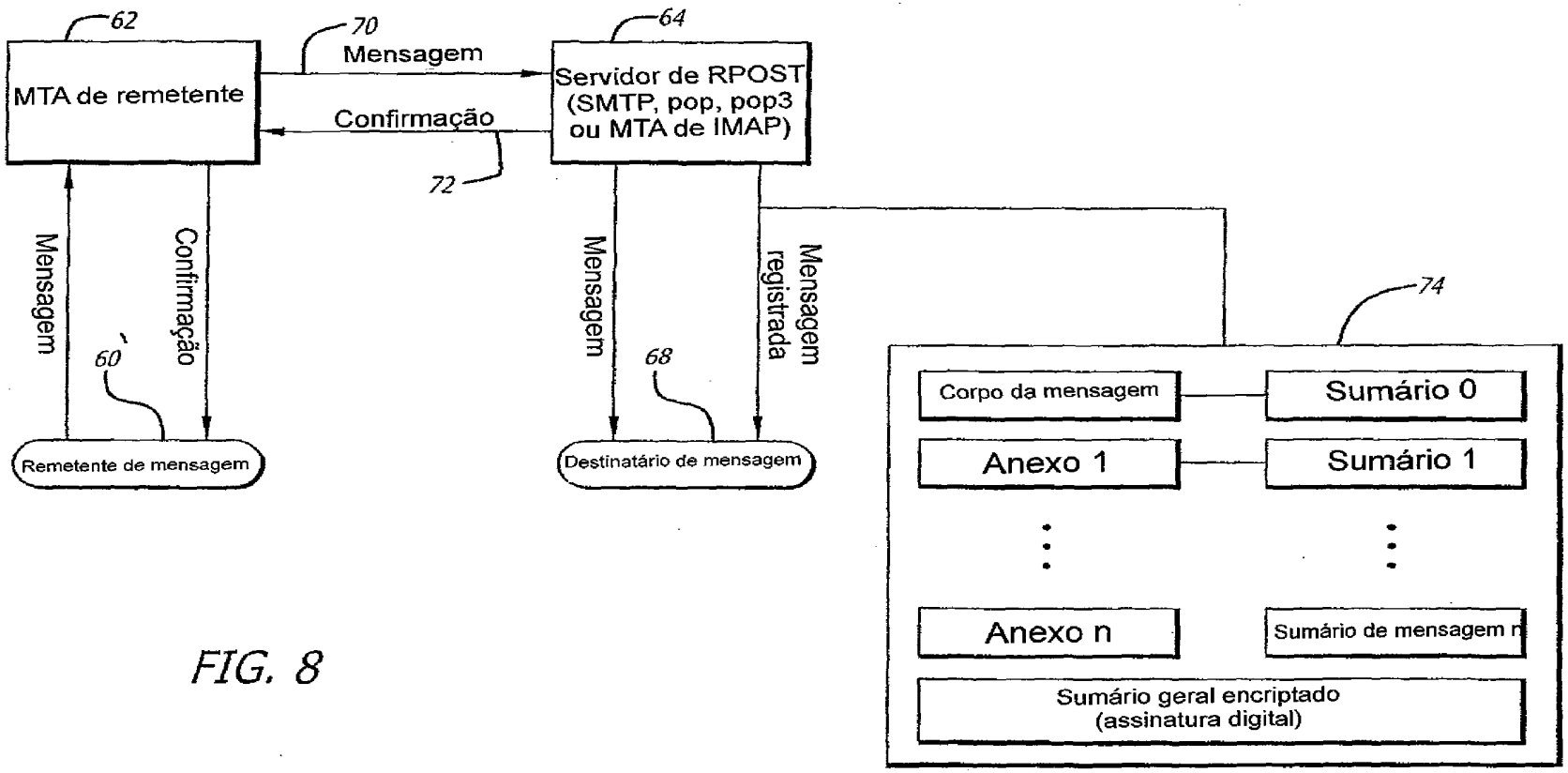
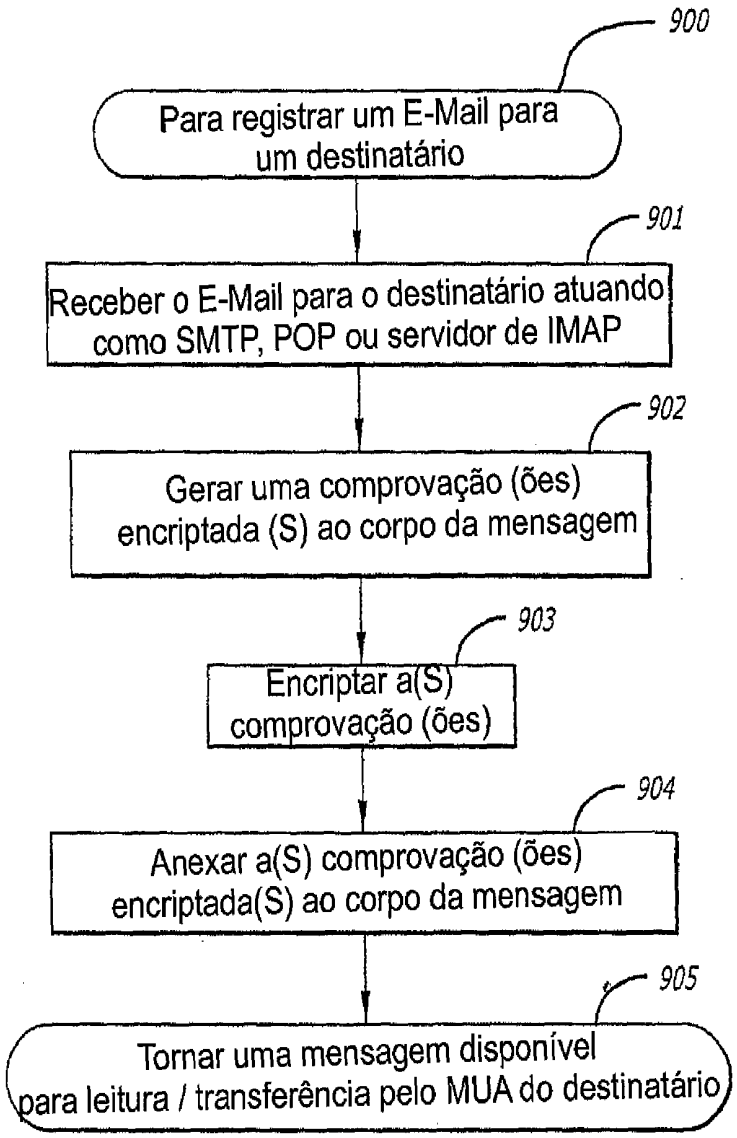

62
70
Mensagem
64
MTA de remetente
Servidor de RPOST
(SMTP, pop, pop3
ou MTA de IMAP)
Confirmação
72
Mensagem
Confirmação
60
Mensagem
68
Mensagem
registrada
74
Corpo da mensagem
Sumário 0
Anexo 1
Sumário 1
Anexo n
Sumário de mensagem n
Sumário geral encriptado
(assinatura digital)
Remetente de mensagem
Destinatário de mensagem

FIG. 8

FIG. 9


900
Para registrar um E-Mail para um destinatário
901
Receber o E-Mail para o destinatário atuando como SMTP, POP ou servidor de IMAP
902
Gerar uma comprovação (ões) encriptada (S) ao corpo da mensagem
903
Encriptar a(S) comprovação (ões)
904
Anexar a(S) comprovação (ões) encriptada(S) ao corpo da mensagem
905
Tornar uma mensagem disponível para leitura / transferência pelo MUA do destinatário

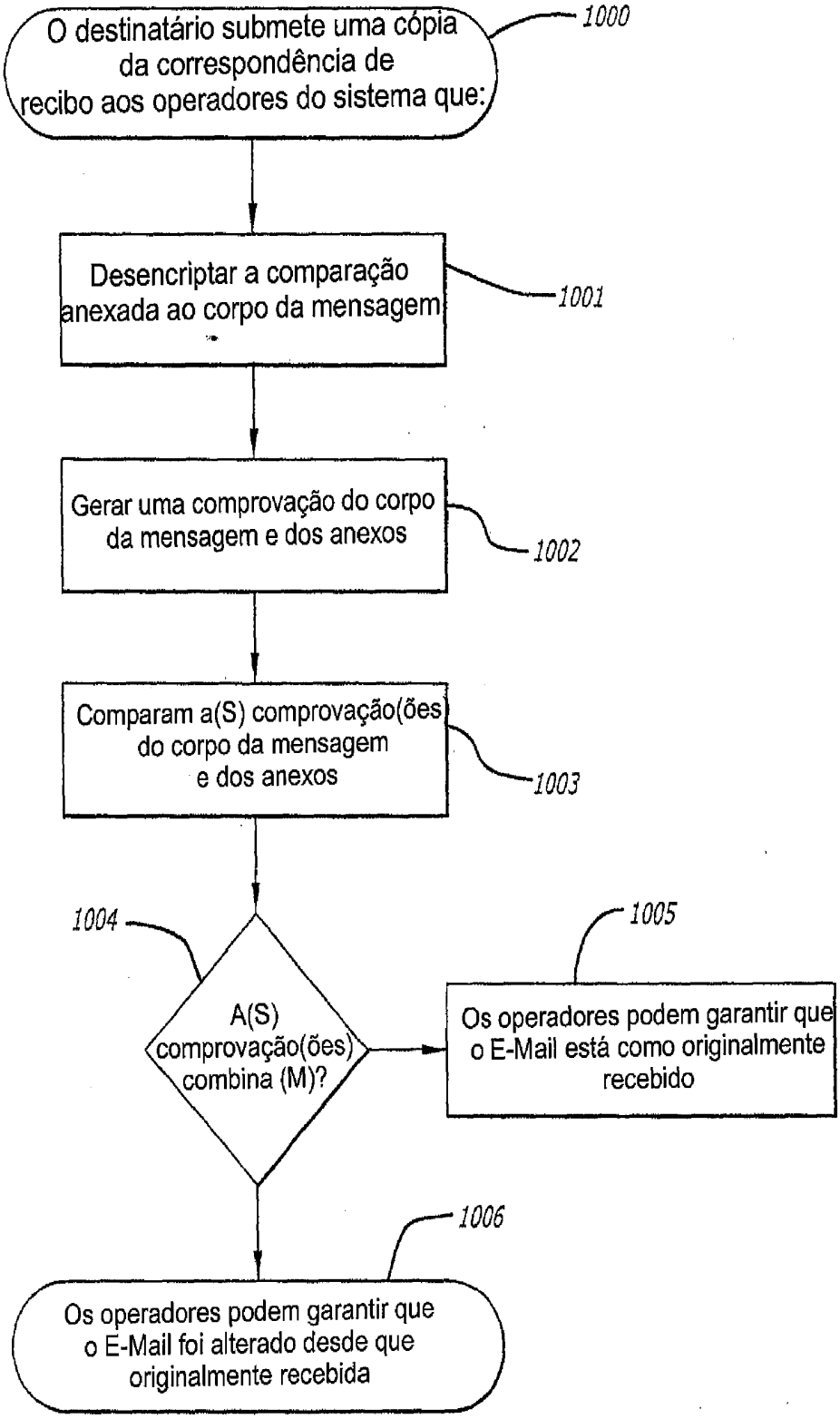

O destinatário submete uma cópia da correspondência de recibo aos operadores do sistema que:
1000
Desencriptar a comparação anexada ao corpo da mensagem
1001
Gerar uma comprovação do corpo da mensagem e dos anexos
1002
Comparam a(S) comprovação(ões) do corpo da mensagem e dos anexos
1003
1004
A(S) comprovação(ões) combina (M)?
1005
Os operadores podem garantir que o E-Mail está como originalmente recebido
1006
Os operadores podem garantir que o E-Mail foi alterado desde que originalmente recebida

FIG. 10

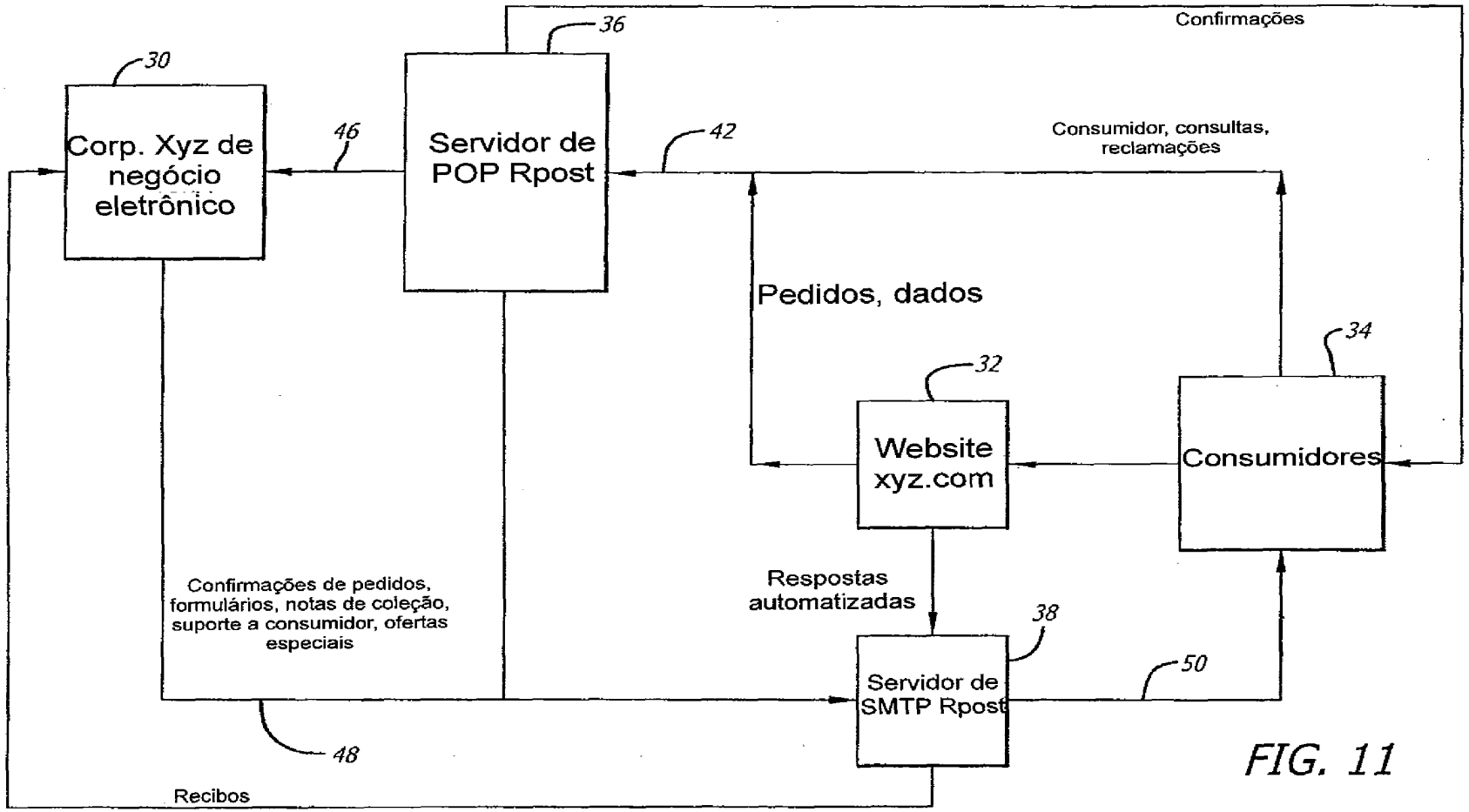

Confirmações
36
30
Corp. Xyz de negócio eletrônico
46
Servidor de POP Rpost
42
Consumidor, consultas, reclamações
Pedidos, dados
34
32
Website xyz.com
Consumidores
Respostas automatizadas
38
Confirmações de pedidos, formulários, notas de coleção, suporte a consumidor, ofertas especiais
Servidor de SMTP Rpost
50
48
Recibos

FIG. 11

RESUMO

Patente de Invenção: **"MÉTODO PARA A VERIFICAÇÃO DE ENVIO E INTEGRIDADE DE MENSAGENS ELETRÔNICAS".**

De modo a prover uma verificação por terceiros do conteúdo e do envio de uma mensagem eletrônica, tal como um e-mail, um servidor recebe o e-mail pretendido para ser enviado ou remetido para um endereçado especificado, e "rotula" a mensagem para indicar que ela é "registrada" com o provedor de serviços. O servidor, então, estabelece uma conexão de telnet direta com o Agente de Usuário de Correio (MUA) do Endereçado, e transmite o e-mail rotulado para o MUA do endereçado, bem como para os MUA's de quaisquer outros endereçados. Após o recebimento de respostas dos MUA's de recebimento que a mensagem foi recebida de forma bem sucedida, o servidor, então, cria e envia para o originador da mensagem um recibo eletrônico. O recibo inclui um ou mais e, preferencialmente, todos os seguintes: a mensagem original, incluindo quaisquer anexos originais; uma tabela de sucesso/falha no envio listando quais MUA's de endereçado receberam com sucesso a mensagem e em que horário, e para quais MUA's houve uma falha de envio; e uma assinatura digital correspondente à mensagem e aos anexos.