



INPI
Assinado
Digitalmente

REPÚBLICA FEDERATIVA DO BRASIL
MINISTÉRIO DA ECONOMIA
INSTITUTO NACIONAL DA PROPRIEDADE INDUSTRIAL

CARTA PATENTE Nº PI 0509538-7

O INSTITUTO NACIONAL DA PROPRIEDADE INDUSTRIAL concede a presente PATENTE DE INVENÇÃO, que outorga ao seu titular a propriedade da invenção caracterizada neste título, em todo o território nacional, garantindo os direitos dela decorrentes, previstos na legislação em vigor.

(21) Número do Depósito: PI 0509538-7

(22) Data do Depósito: 30/03/2005

(43) Data da Publicação do Pedido: 13/10/2005

(51) Classificação Internacional: H04L 9/30.

(30) Prioridade Unionista: US 60/559,092 de 02/04/2004; US 60/559,646 de 05/04/2004.

(54) Título: MÉTODO, SINAL DIGITAL, PORTADORA, E PRIMEIRO SISTEMA PARA ESTABELECEER UM PERCURSO DE COMUNICAÇÃO BIDIRECIONAL

(73) Titular: BLACKBERRY LIMITED. Endereço: 2200 UNIVERSITY AVENUE E., WATERLOO, ON, Canadá., CANADÁ(CA)

(72) Inventor: HERBERT ANTHONY LITTLE; MICHAEL KENNETH BROWN.

Prazo de Validade: 10 (dez) anos contados a partir de 15/01/2019, observadas as condições legais

Expedida em: 15/01/2019

Assinado digitalmente por:

Alexandre Gomes Ciano

Diretor Substituto de Patentes, Programas de Computador e Topografias de Circuitos Integrados

MÉTODO, SINAL DIGITAL, PORTADORA, E PRIMEIRO SISTEMA PARA
ESTABELECEER UM PERCURSO DE COMUNICAÇÃO BIDIRECIONAL

ANTECEDENTES

CAMPO TÉCNICO

5 Este pedido se refere a um aparelho e a um método de
estabelecimento de uma relação autêntica e segura entre
dois sistemas de envio de mensagem para a troca de dados.
Mais especificamente, este pedido descreve um aparelho e um
método para o estabelecimento de uma relação autêntica
10 entre um dispositivo portátil sem fio ("dispositivo móvel")
e um centro de mensagem ou sistema de hospedagem usando
métodos de autenticação baseados em senha. O aparelho e o
método descritos aqui são aplicáveis a ambientes de linha
em terra bem como a ambientes sem fio.

15 ANTECEDENTES DA TÉCNICA

Há vários mecanismos de encriptação baseados em senha
fortes atualmente conhecidos na indústria de computadores.
Algumas destas implementações incluem Troca de Chave
Encriptada (EKE), Módulos Derivados de Senha (PDM), e Troca
20 de Chave Exponencial Autenticada por Senha Simples (SPEKE).
Estes mecanismos são limitados nas suas implementações e
não se dirigiram à necessidade de dispositivos móveis.
Adicionalmente, estes mecanismos não se dirigem à
necessidade de implementação de um sigilo futuro perfeito,
25 de modo que se uma brecha de segurança não ocorrer todas as
mensagens prévias trocadas permanecem seguras. Um protocolo
provê um sigilo futuro perfeito se as chaves de sessão
passada não forem comprometidas mesmo se as chaves de longa
duração forem comprometidas. (Veja, por exemplo, Menezes et
30 al., Handbook of Applied Cryptography, 1996, p. 496). O

sigilo futuro perfeito, também conhecido como proteção de ruptura passada, significa que todas as mensagens trocadas seguramente prévias devem permanecer seguras apesar de qualquer coisa que aconteça no futuro.

5

SUMÁRIO

Um sistema de comunicação de encriptação baseado em senha, em ambientes sem fio ou com fio, tendo um sigilo futuro perfeito é descrito. Ele inclui o uso de um par de chaves geradas de longa duração em combinação com um par de chaves de autenticação de curta duração, geradas usando-se um segredo compartilhado, para se permitir a implementação de um sigilo futuro perfeito. A chave pública de longa duração é complementada com a chave pública de autenticação, para se permitir uma troca autêntica de chaves de longa duração. Isto permite que a parte correspondente que está de posse do segredo compartilhado receba e seja capaz de usar a chave pública de longa duração.

De acordo com um aspecto, um método realizado por um primeiro sistema para o estabelecimento de um percurso de comunicação bidirecional seguro entre o primeiro sistema e um segundo sistema para uma troca de uma ou mais mensagens é descrito. O método compreende a geração de um primeiro par de chaves que tem uma primeira chave pública e uma primeira chave privada, e a geração de um segundo par de chaves tendo uma segunda chave pública e uma segunda chave privada. A segunda chave pública é gerada com base em um segredo compartilhado conhecido pelo primeiro sistema e pelo segundo sistema. O método também compreende o envio da segunda chave pública e da primeira chave pública para o

segundo sistema, e o recebimento de uma terceira chave pública e de uma quarta chave pública geradas pelo segundo sistema, onde a quarta chave pública é gerada com base no segredo compartilhado. O método também compreende o cálculo
5 de uma chave mestra baseada na primeira chave privada, na segunda chave privada, na terceira chave pública e na quarta chave pública, onde a chave mestra é configurada para ser usada na encriptação de uma ou mais mensagens.

De acordo com um outro aspecto, um sistema compreende
10 uma memória e uma unidade de processamento acoplada à memória, onde a unidade de processamento é configurada para executar as etapas citadas acima.

De acordo com um outro aspecto, um portador legível em computador contém instruções de processamento adaptadas
15 para fazerem com que uma unidade de processamento execute as etapas citadas acima.

BREVE DESCRIÇÃO DOS DESENHOS

A Figura 1 mostra um diagrama de blocos de um primeiro sistema de comunicação de exemplo, entre um sistema fixo e
20 um sem fio.

A Figura 2 mostra um diagrama de blocos de um segundo sistema de comunicação de exemplo, entre dois sistemas sem fio.

A Figura 3 mostra um diagrama de blocos de um terceiro
25 sistema de comunicação de exemplo, entre dois sistemas fixos.

A Figura 4 mostra um diagrama de troca de mensagem de um conjunto de exemplo de trocas de dados para a implementação do sistema de comunicação da Figura 1, onde
30 um usuário é o iniciador da troca de dados.

A Figura 5 mostra um diagrama de troca de mensagem de um conjunto de exemplo de trocas de dados para a implementação do sistema de comunicação da Figura 1, onde um provedor de serviços é o iniciador da troca de dados.

5 A Figura 6 mostra um fluxograma de dados das etapas no software de usuário para a realização das etapas na Figura 4, onde o usuário é o iniciador da troca de chave.

A Figura 7 mostra um fluxograma de dados das etapas no software de serviço para a realização das etapas na Figura 10 4, onde o usuário é o iniciador da troca de chave.

A Figura 8 mostra um fluxograma de dados das etapas no usuário de serviço para uma seqüência de rechaveamento quando da nova geração de uma outra chave no ambiente ilustrado nas Figuras 1, 2 e 3.

15 A Figura 9 mostra um fluxograma das etapas necessárias no provedor de serviços para uma seqüência de rechaveamento quando da nova geração de uma outra chave no ambiente ilustrado nas Figuras 1, 2 e 3.

DESCRIÇÃO DETALHADA

20 Com referência à Figura 1, é mostrado um diagrama de blocos de um primeiro sistema de comunicação de exemplo entre um sistema fixo e um sem fio. Este diagrama de visão geral mostra um ambiente de rede em que a invenção é usada. O diagrama mostra uma modalidade de exemplo da invenção e
25 se concentra em uma topologia de rede, que inclui um dispositivo móvel que é sem fio. Nesta figura, há sistemas oferecendo serviços 20 e 22 e sistemas usando os serviços 30 e 32. Entre a oferta de serviço (também referida aqui como provedor de serviços) e o usuário de serviço estão uma
30 ou mais redes e uma ou mais conexões, para se permitir o

fluxo de dados entre os dois sistemas.

Voltando-nos, agora, para a Figura 1, a oferta de serviço 20 ou 22 pode ser muitos possíveis computadores oferecendo serviços para os usuários. Para alguém versado na técnica, alguns provedores de serviços bem conhecidos poderiam ser computadores na Internet em um Provedor de Serviços de Internet (ISP) ou um escritório de Provedor de Serviços de Aplicativo (ASP). As ofertas de serviço 20 e 22 também podem ser um ou mais computadores rodando em uma companhia privada ou pública, como um banco, uma corretora de ações, uma corretora de seguros ou alguma outra companhia orientada para serviços. A oferta de serviço 20 ou 22 também pode ser rodada como parte de um agrupamento de computadores operando ao redor do mundo, constituindo um Agrupamento de Descrição, Descoberta e Integração Universal (agrupamento de UDDI). O elemento comum em todas estas ofertas de serviço 20 e 22 é que estas ofertas de serviço 20 e 22 precisam estabelecer um canal de dados seguro com um usuário. No caso de UDDI, a relação segura poderia ser necessária para a troca de listagens de serviço privado, ou mesmo para se permitir que uma UDDI represente uma oferta de serviço.

Os dispositivos móveis e as hospedagens de serviço podem ser endereçados de uma variedade de formas diferentes. Em algumas modalidades, eles podem ser endereçados com endereços de IP (protocolo de internet). Em outras modalidades, o sistema de hospedagem pode ser endereçado por um endereço de e-mail. Ainda em uma outra modalidade, o endereço de destino pode ser um endereço de e-mail de um usuário do dispositivo móvel no sistema de

hospedagem.

Uma pessoa versada na técnica apreciará que o usuário do serviço 30 ou 32 poderia ser um navegador de protocolo de transferência de hipertexto (HTTP) de móvel, um navegador de protocolo de aplicativo sem fio (WAP) de móvel, um aplicativo baseado em protocolo de controle de transmissão / protocolo de internet (TCP/IP) proprietário ou alguma outra solução corporativa proprietária. Neste campo, há novos métodos sendo desenvolvidos rapidamente, incluindo, por exemplo, a nova solução Java 2 Micro Edition (J2ME) para pequenos dispositivos móveis sem fio, como telefones celulares e assistentes digitais pessoais (PDAs). Para dispositivos que usam J2ME, a opção de anexação e transferência de um software através de uma oferta de serviço está se tornando lugar comum. De modo similar, as ofertas de serviço 20 e 22 podem ser baseadas em uma solução de servidor da web de HTTP, uma solução de Java Enterprise, uma oferta de serviço baseada em linguagem de marcação sem fio (WML) ou alguma solução de serviço proprietária criada para uma finalidade específica.

Será apreciado que sistemas móveis e sistemas de hospedagem referidos aqui podem compreender, cada um, uma ou mais respectivas memórias (por exemplo, contendo instruções de processador) e uma ou mais respectivas unidades de processamento, tais como aquelas convencionalmente conhecidas, por exemplo, unidades de processamento de finalidade geral e/ou unidades de processamento de finalidade especial, tais como circuitos integrados específicos de aplicação (ASICs) e arranjos de porta programáveis de campo (FPGAs), onde as unidades de

processamento podem ser configuradas (por exemplo, programadas com instruções de software e/ou firmware adequadas, e/ou produzidas com circuitos de hardware especializados) para a realização das abordagens descritas aqui. Cada um desses sistemas também pode incluir qualquer (quaisquer) interface(s) adequada(s), tais como aquelas convencionalmente conhecidas, a(s) qual(is) pode(m) operar em conjunto com uma respectiva(s) unidade(s) de processador para facilitação da comunicação com outros sistemas.

Os pontos de extremidade no percurso de comunicação são acoplados através de uma ou mais redes de dados que permitem a troca de dados, voz, vídeo, música, fotografias ou qualquer outra mídia digital que pode ser trocada através de um canal de comunicações de dados. As duas redes principais incluídas nesta ilustração são a Rede de Área Ampla (WAN) 26, a mais comum sendo a Internet, e uma rede sem fio 28. A rede sem fio 28 poderia ser uma rede GSM/GPRS, uma rede CDMA/1XRTT, uma rede CDMA2000, uma rede de 3ª Geração como EDGE ou UMTS ou muitas outras redes sem fio públicas logo disponíveis. Em um sistema de exemplo, estas redes são acopladas usando-se ligações 24 como ISDN, T1, Ethernet (linha em terra e 802.11), Envio de Quadro, ATM, ADSL ou alguma outra conexão de Internet de alta velocidade para o serviço de hospedagem 22. Conforme quantidades maiores de dados estão sendo trocadas, é claro que a segurança precisa ser melhorada e tornada mais inviolável para hackers e pessoas acompanhando em segredo. A invenção trabalha com estes percursos de comunicação de dados existentes para a provisão de uma autenticação baseada em senha avançada. Este nível de segurança provê

maior confiança de que o destinatário de quaisquer dados comunicados seja exatamente a entidade que se espera. Uma modalidade para um percurso de comunicação de dados 36 é ilustrada entre uma oferta de serviço de Sistema de Hospedagem 22 e um usuário do serviço em um dispositivo móvel 32. Uma outra modalidade para um percurso de comunicação de dados 40 é ilustrada entre uma oferta de serviço de UDDI 20 e um usuário do serviço em um dispositivo móvel 30.

10 Em uma modalidade, a oferta de serviço de sistema de hospedagem 22 tem uma comunicação fora de banda 34 (isto é, uma comunicação por qualquer canal seguro adequado) com um usuário de um dispositivo móvel 32. O percurso de comunicação fora de banda 34 é usado para a troca de um
15 segredo compartilhado, evitando-se um percurso inseguro que é para ser tornado seguro. Uma vez que a nuvem de serviço de UDDI provê algum nível de segurança, uma nuvem de serviço de UDDI poderia ser usada para a localização do serviço e a recepção do segredo compartilhado fora de banda
20 com o serviço de destino final. O que vem a seguir são uns poucos exemplos de percursos de comunicação 34 e 38:

- (a) O usuário de dispositivo móvel 30 ou 32 e um operador no sistema de hospedagem 20 ou 22 estabelecem uma chamada telefônica um com o outro para a troca do
25 segredo compartilhado. O segredo então é introduzido em cada sistema e usado no processo de criação de uma chave de encriptação.
- (b) O usuário de dispositivo móvel 30 ou 32 se conecta a um website seguro 20 ou 22, de forma sem fio ou por
30 uma rede com fio, e requisita uma chave. A chave é

recebida e manualmente introduzida no dispositivo móvel 30 ou 32. O sistema de hospedagem 20 ou 22 poderia receber a chave automaticamente a partir do servidor da web, ou também poderia ser introduzida manualmente. Em algumas modalidades, um registro é automaticamente gerado após um segredo compartilhado ser requisitada.

(c) O usuário do dispositivo móvel 30 ou 32 faz a requisição pelo serviço e o segredo compartilhado é enviado por e-mail para o sistema de hospedagem 20 ou 22 para sua caixa de correio corporativa que é conhecida por estar em uma área segura. O usuário recupera o segredo compartilhado a partir de sua caixa de correio eletrônica e manualmente a introduz no dispositivo móvel 30 ou 32.

(d) O usuário do dispositivo móvel 30 ou 32 faz a requisição pelo serviço e a operadora no serviço 20 ou 22 gera um segredo compartilhado e este é dado a uma pessoa especificada que é conhecida por ser confiável e segura. Esta pessoa poderia ser um secretário ou um administrador de um dado grupo; de modo ideal, ele é alguém que pode confirmar a identidade do usuário fazendo a requisição. Esta pessoa de confiança então dá o segredo compartilhado ao usuário final do dispositivo móvel 30 ou 32 e ele é manualmente introduzido no dispositivo móvel 30 ou 32.

Esta lista curta mostra que há muitas formas de se ar de forma autentica um segredo compartilhado a um usuário de dispositivo móvel. A propriedade comum destas comunicações fora de banda de exemplo 34 e 38 é que algum nível de

autenticação é construído ou assumido na escolha feita. Este percurso de comunicação autenticado é diferente do percurso de comunicação de dados não autenticado.

Uma vez que o segredo compartilhado seja
5 compartilhado, a próxima etapa na criação de um percurso de comunicação seguro pode ocorrer em 36 e 40. Um dos métodos mais bem conhecidos para a criação de uma ligação segura e autenticada é usar um método de encriptação baseado em senha forte como SPEKE. SPEKE é um método criptográfico
10 para uma autenticação baseada em conhecimento que alavanca e protege senhas fáceis de lembrar - isto é, segredos compartilhados. SPEKE é o mais simples dos métodos de senha forte conhecidos. É uma troca de Diffie-Hellman autenticada por senha, onde a senha forma a base ou um "gerador" da
15 troca. (Em Diffie-Hellman padronizado, a base usualmente é um número público fixo.) Uma vez que o percurso de comunicação através da WAN 26 e da rede sem fio 28 tenha sido tornado seguro, a seqüência de rechaveamento pode ser iniciada. A seqüência de rechaveamento permite a geração de
20 um novo conjunto de chaves após um número predeterminado de semanas ou meses. Durante esta seqüência de rechaveamento, o uso avançado de chaves de encriptação de longa duração permite a implementação de um sigilo futuro perfeito. Uma vez que o segredo de autenticação (segredo compartilhado)
25 seja usado para a criação de um percurso seguro, ele pode ser reusado para a criação de novas chaves em datas posteriores. Pelo uso desta invenção, a operação de rechaveamento não compromete as chaves prévias e todas as conversações prévias permanecem secretas no futuro.

30 Voltando-nos para a Figura 2, é mostrado um diagrama

de blocos de um sistema de comunicação de exemplo entre dois sistemas sem fio, de acordo com uma modalidade da presente invenção. Nesta modalidade, um percurso seguro 52 pode ser criado entre dois dispositivos móveis. Nesta 5 modalidade, o dispositivo móvel 1 46 e o dispositivo móvel 2 48 trocam um segredo e são capazes de estabelecerem uma chave comum usando aquele segredo compartilhado. A conversação fora de banda 50 poderia ocorrer através de uma chamada telefônica entre as duas partes, um encontro face a 10 face ou usando-se um dos outros métodos já destacados ou qualquer outro método adequado. Uma vez que o segredo seja compartilhado, ele pode ser manualmente digitado nos dispositivos móveis 46 e 48, e uma estação poderia iniciar a troca de mensagens para a criação de uma chave de 15 segurança mestra comum. Este tipo de modalidade poderia ser comumente usado para conversações por e-mail de ponto a ponto privadas. Também poderia ser usada para trocas de dados de envio de mensagem instantânea segura de ponto a ponto. Em um uso avançado, o dispositivo móvel 1 46, o qual 20 está provendo o serviço, poderia estar rodando um servidor da web no dispositivo móvel 46 e oferecendo alguma forma de oferta de serviço seguro que também seja móvel.

Voltando-nos para a Figura 3, é mostrado um diagrama de blocos de um sistema de comunicação de exemplo, entre 25 dois sistemas fixos, de acordo com uma modalidade da presente invenção. Nesta modalidade, a comunicação ocorre entre dois sistemas de hospedagem 60 e 62. Nesta ilustração, a oferta de serviço 60 e o consumidor de serviço 62 têm uma conversação fora de banda 66 e trocam 30 uma chave secreta. Conforme já descrito, esta comunicação

fora de banda poderia ser uma chamada telefônica, uma comunicação através de um navegador com uma conexão de SSL segura para a geração e a recuperação da chave, ou alguma outra comunicação adequada, tal como provido anteriormente.

5 Uma vez que o segredo seja trocado, uma chave de encriptação pode ser gerada usando-se métodos de geração de chave baseados em senha forte, como SPEKE. O percurso de comunicação para a troca da chave nesta ilustração poderia ser por uma rede WAN, tal como a Internet 26, ou através de
10 uma Intranet interna 64, ou qualquer outro percurso de comunicação adequado tal como ou similar a uma ligação 802.11 ou de Bluetooth. Nestes últimos exemplos, o consumidor de serviço 62 poderia estar rodando um laptop ou um palmtop e já ter um acesso limitado à Intranet, mas
15 maior segurança seria requerida. É bem conhecido na técnica que 802.11b carece das exigências de segurança robusta requisitadas pela maioria dos departamentos computacionais grandes dentro de companhias. Esta modalidade ilustra que a invenção pode ser usada para a provisão da opção de sigilo
20 futuro perfeito quando se usa um mecanismo de autenticação baseado em senha. Uma vez que mensagens adequadas sejam trocadas para a criação da chave mestra, o percurso de comunicação de dados 68 pode ser usado para a troca de todas as formas de dados secretamente com alta segurança.

25 Voltando-nos para a Figura 4, é mostrado um diagrama de troca de mensagem que mostra um conjunto de exemplo de trocas de dados para a geração e a verificação de uma chave mestra, onde o usuário é o iniciador da troca de dados. Esta ilustração mostra etapas de exemplo e trocas de
30 mensagem entre um consumidor de serviço 100 (usuário) e um

provedor de serviços 102. Nesta ilustração, uma extremidade da conexão é considerada um consumidor ou usuário de serviço 100, e a ela foi dado o rótulo sistema A. A outra extremidade da conexão é considerada o provedor de serviços (também referido como uma oferta de serviço) ou sistema de hospedagem 102, e recebeu o rótulo sistema B. Neste exemplo, o usuário 100 inicia a troca de dados para a criação de uma conexão segura. Entre o Sistema A e o Sistema B está uma troca de mensagem por uma ou mais redes de comunicação, tal como ilustrado na Figura 1. De modo similar, conforme mostrado nas Figuras 1, 2 e 3, o usuário poderia ser um dispositivo móvel 30, 32 ou 48, ou um Sistema de Hospedagem 62. Da mesma forma, o provedor de serviços poderia ser um dispositivo móvel 46 ou um Sistema de Hospedagem 20, 22 ou 60.

Conforme mostrado na etapa 104, o usuário 100 contata um provedor de serviços conhecido 102 através de um dos métodos já descrito para comunicação fora de banda ou através de um outro método adequado para a troca de um segredo compartilhado. Este provedor de serviços 102 quer facilitar esta troca e emite uma senha secreta ou cadeias de senha simples, fáceis de lembrar (etapa 106). Através deste mecanismo, um segredo compartilhado é gerado e trocado entre as duas partes. O usuário 100 recebe e salva o segredo para ajudar na geração da chave de encriptação. Alternativamente, o provedor de serviços 102 pode receber uma senha secreta (segredo compartilhado) a partir do usuário 100. Em qualquer caso, o provedor de serviços salva o segredo compartilhado em relação a este usuário.

Após a troca do segredo compartilhado, o usuário 100

então inicia (neste exemplo) etapas de geração de pares de chaves (etapa 108) e de transferência de informação de chave para o provedor de serviços (etapa 110). Em particular, o usuário 100 gera um par de chaves de encriptação de longa duração na etapa 108, isto é, as partes pública e privada de uma chave de encriptação. Um par de chaves de autenticação de curta duração também é gerado na etapa 108 pelo usuário 100. Este par de chaves de curta duração é referido como um par de chaves de autenticação neste exemplo, porque é gerado usando-se o segredo compartilhado, conforme discutido adicionalmente abaixo.

Uma vez que os pares de chave de curta duração e de longa duração de usuário sejam gerados, as chaves de usuário dos mesmos são transmitidas na etapa 110 para o provedor de serviços 102 para ainda gerar a chave mestra final (por exemplo, referida como um segredo mestre). Esta transferência pode ocorrer por uma linha insegura, já que apenas o sistema de hospedagem 102 que emitiu o segredo compartilhado pode compreender e usar a chave de autenticação de curta duração para a geração da chave mestra. Uma vez que as chaves de usuário de usuário sejam recebida pelo provedor de serviços (etapa 112), o usuário é verificado e o segredo compartilhado para aquele usuário é lembrado em 112. Uma vez que o usuário seja verificado e o segredo compartilhado para o usuário seja lembrado, o provedor de serviços 102 prossegue para gerar seu próprio par de chaves de autenticação de curta duração usando o segredo compartilhado (etapa 114). O provedor de serviços 102 também gera seu próprio par de chaves de autenticação

de longa duração (etapa 114). Usando as chaves de usuário geradas pelo usuário 100 e usando o segredo compartilhado, o provedor de serviços 102 gera uma chave de encriptação mestra (ou segredo mestre), conforme mostrado na etapa 116.

5 O segredo compartilhado provê a autenticação necessária para se confinar na informação trocada. A chave de autenticação pública de curta duração do provedor de serviços, a chave de encriptação pública de longa duração do provedor de serviços e um valor de confirmação de chave
10 que foi calculado pelo provedor de serviços usando-se a chave de encriptação mestra recém gerada e alguma cadeia conhecida, são enviados para o usuário (etapa 116).

O usuário recebe a informação (etapa 118) enviada a partir do provedor de serviços 102, incluindo as chaves de
15 usuário de curta duração e de longa duração do provedor de serviços e gera a própria chave mestra do usuário (etapa 120). Com esta chave mestra, o usuário verifica o valor de confirmação de chave (etapa 120). Neste exemplo, o valor de confirmação de chave poderia ser o valor de comprovação da
20 chave mestra e o nome do serviço ou alguma outra cadeia conhecida, acordada pelo usuário e pelo provedor de serviços. Se o valor de confirmação de chave não for verificado, a chave mestra criada pelo usuário 100 não é confiável, e é assumido que alguém está tentando
25 comprometer a conexão. Se a chave de encriptação mestra gerada pelo usuário 100 parecer válida, o usuário então envia um valor de confirmação de chave final de volta para o provedor de serviços (etapa 122). O provedor de serviços recebe a mensagem, verifica o valor de confirmação de
30 chave, e marca o usuário como pronto para ir (etapa 124).

Isto permite que uma troca de dados plena ocorra do ponto de vista do provedor de serviços (etapa 128). No lado de usuário, uma vez que a mensagem de verificação seja enviada, haveria uma ligeira pausa na transmissão, mas, 5 então, uma troca de dados plena pode começar (etapa 126).

As transmissões podem compreender mensagens de e-mail, tráfego baseado em HTTP (protocolo de transferência de hipertexto), tais como XML (linguagem de marcação extensível), WML (linguagem de marcação sem fio), etc., ou 10 outros tipos de tráfego.

Em algumas modalidades, o sistema de hospedagem é capaz de enviar uma carga útil de dados em uma mensagem enviada para o dispositivo móvel, antes do valor de confirmação final ser enviado para ele a partir do 15 dispositivo móvel. A carga útil nesta mensagem pode ser uma entrada de livro de serviço, que define o serviço de hospedagem no sistema de hospedagem. Em algumas modalidades, a entrada de livro de serviço pode ser uma entrada de serviço de UDDI, que define atributos de um 20 serviço de hospedagem no sistema de hospedagem sendo acessado.

Será apreciado que o par de chaves de encriptação de longa duração gerado por uma primeira parte (por exemplo, um usuário), conforme descrito aqui, é um exemplo de, mais 25 geralmente, um primeiro par de chaves, onde a porção de chave pública e a porção de chave privada do mesmo podem ser referidas como uma primeira chave pública e uma primeira chave privada. De modo similar, o par de chaves de autenticação de curta duração (também referido como par de 30 chaves de encriptação de curta duração) gerado pela

primeira parte (por exemplo, o usuário), conforme descrito aqui, é um exemplo, mais geralmente, de um segundo par de chaves, onde a porção de chave pública e a porção de chave privada do mesmo podem ser referidas como uma segunda chave pública e uma segunda chave privada. Também, o par de chaves de encriptação de longa duração gerado por uma segunda parte (por exemplo, um provedor de serviços), conforme descrito aqui, é um exemplo, mais geralmente, de um terceiro par de chaves, onde a porção de chave pública e a porção de chave privada do mesmo podem ser referidas como uma terceira chave pública e uma terceira chave privada. De modo similar, o par de chaves de autenticação (ou de encriptação) de curta duração gerado pela segunda parte (por exemplo, o provedor de serviços), conforme descrito aqui, é um exemplo, mais geralmente, de um quarto par de chaves, onde a porção de chave pública e a porção de chave privada do mesmo podem ser referidas como uma quarta chave pública e uma quarta chave privada. A primeira parte que gera os primeiro e segundo pares de chaves poderia ser um usuário, tal como descrito no exemplo acima, ou um provedor de serviços, tal como descrito no exemplo abaixo.

Voltando-nos para a Figura 5, é mostrado um diagrama de troca de mensagem que mostra um conjunto de exemplo de trocas de dados para a geração e a verificação de uma chave mestra, onde o provedor de serviços é o iniciador da troca de dados. As etapas na Figura 5 substancialmente correspondem às etapas na Figura 4, exceto pelo fato de o provedor de serviços efetuar a primeira etapa. Este exemplo destaca que o usuário ou o provedor de serviços pode ser o iniciador da troca de dados. Nesta ilustração, uma

extremidade da conexão é considerada o usuário 100, e é rotulada sistema A - consumidor de serviço. A outra extremidade da conexão é considerada o serviço 102, e é rotulada sistema B - Provedor de Serviços. Entre o Sistema A 100 e o Sistema B 102 está uma troca de mensagem por uma ou mais redes de comunicação de dados 26, 28 e 64, tal como ilustrado nas Figuras 1, 2 e 3. De modo similar, conforme mostrado nas Figuras 1, 2 e 3, o usuário poderia ser um dispositivo móvel 30, 32 ou 48 ou um Sistema de Hospedagem 20, 22, 46 ou 60.

Conforme mostrado nas etapas 200/202, o provedor de serviços 102 contata o usuário 100 (neste exemplo) para a troca de um segredo compartilhado. Alternativamente, o usuário poderia iniciar esta comunicação. É contemplado que um administrador em uma companhia de hospedagem 102 poderia contatar o usuário 100 e informar ao usuário que o usuário tem de realizar alguma ação com o segredo compartilhado sendo provido. Usando qualquer método adequado selecionado a partir da lista extensiva de comunicações fora de banda já provida, ou algum outro método adequado, o segredo compartilhado é gerado e trocado (etapas 200 e 202). O componente de Usuário recebe e salva o segredo compartilhado para ajudar na geração da chave de encriptação. Alternativamente, o provedor de serviços 102 pode receber uma senha secreta (segredo compartilhado) a partir do usuário 100. Em qualquer caso, o provedor de serviços salva o segredo compartilhado em relação a este usuário.

Após a troca do segredo compartilhado, o provedor de serviços 102 pode iniciar (neste exemplo) as etapas de

geração de pares de chaves (etapa 204) e de transferência da informação de chave para o usuário 100 (etapa 206). Em particular, o provedor de serviços 102 gera um par de chaves de autenticação de curta duração e um par de chaves de encriptação de longa duração (etapa 204). Isto corresponde à etapa 108 na Figura 4.

Uma vez que os pares de chaves de curta duração e de longa duração do provedor de serviços sejam gerados, as chaves de usuário do mesmo são transmitidas para o usuário (etapa 206) para se gerar ainda a chave mestra final (também referida como um segredo mestre). Esta transferência pode ocorrer por uma linha insegura, já que apenas o proprietário do segredo compartilhado seria capaz de compreender e usar a chave de autenticação de curta duração para a geração da chave mestra. As chaves de usuário de provedor de serviços são recebidas pelo usuário, e ele checa a memória para verificar a criação de serviço que é esperada e que ele tem um segredo compartilhado salvo na memória (etapa 208). O usuário lembra o segredo compartilhado para aquele provedor de serviços 102 e gera um par de chaves de autenticação de curta duração usando o segredo compartilhado (etapa 210). O usuário também gera um par de chaves de encriptação de longa duração (etapa 210). Usando as chaves de usuário geradas e enviadas pelo provedor de serviços 102 e usando o segredo compartilhado, o usuário 100 gera uma chave de encriptação mestra (ou segredo mestre), conforme mostrado na etapa 212. Após a geração da chave mestra, o usuário 100 também gera um valor de confirmação de chave pela combinação de uma cadeia conhecida (isto é, conhecido para si mesmo ou a oferta de

serviço) com a chave mestra (etapa 212). A chave de autenticação pública de curta duração, a chave de encriptação pública de longa duração e o valor de confirmação de chave são enviados para o provedor de serviços (etapa 212).

O provedor de serviços recebe as chaves de usuário de usuário e o valor de confirmação de chave e verifica o remetente da informação (etapa 214) e também lembra o segredo compartilhado para este usuário. Com os valores de chave pública recebidos do usuário, o provedor de serviços lembra seus próprios valores de chave privada salvos para este usuário (etapa 214). Usando as chaves de usuário recebidas do usuário e as chaves privadas salvas do provedor de serviços, o provedor de serviços agora pode gerar uma chave mestra (etapa 216). Após a geração da chave mestra, o provedor de serviços 102 verifica o valor de confirmação de chave pelo cálculo de seu próprio valor de confirmação de chave, usando a cadeia conhecida e a chave mestra recém criada, e comparando-o em relação ao valor de confirmação de chave recebido (etapa 216). Se o valor de confirmação de chave não verificar, a chave mestra criada não é confiável e, assim, é assumido que alguém está tentando comprometer a conexão. Se o valor de confirmação de chave realmente verificar, a chave de encriptação mestra é considerada válida e o provedor de serviços 102 envia um valor de confirmação de chave final de volta para o usuário (etapa 218). O usuário recebe a mensagem (etapa 220), verifica o valor de confirmação de chave e marca o provedor de serviços como pronto para ir (etapa 220). Isto permite que uma plena troca de dados ocorra do ponto de vista do

usuário (etapa 222). No lado de oferta de serviço, uma vez que a mensagem de verificação seja enviada haveria uma pausa na transmissão, mas, então, uma troca de dados plena pode começar (etapa 224). Na maioria dos casos, será o usuário que iniciará a primeira troca de dados; então, ter a confirmação enviada para o usuário realmente tem algumas vantagens.

As transmissões podem compreender mensagens de e-mail, tráfego baseado em HTTP (protocolo de transferência de hipertexto), tais como XML (linguagem de marcação extensível), WML (linguagem de marcação sem fio), etc., ou outros tipos de tráfego.

A Figura 6 é um fluxograma de dados de etapas de exemplo realizadas pelo usuário (por exemplo, no software de usuário) para a realização da abordagem de exemplo mostrada na Figura 4, quando o usuário é o iniciador da troca de chave. A primeira etapa ocorre quando o usuário descobre um novo serviço e deseja acessá-lo (etapa 300). Isto poderia ocorrer através de um serviço tipo de UDDI, através de um serviço de Intranet corporativa, através de navegação pela rede mundial, através de uma conversa com um amigo ou através de uma chamada telefônica. Uma vez que o serviço e o usuário tenham sido conectados, eles trocam um segredo compartilhado 's' que apenas os dois sabem (etapa 302). Os métodos de exemplo desta troca já foram descritos em detalhes. Este segredo compartilhado 's' será usado mais tarde como um PIN (Número de Identificação Pessoal) para autenticação do usuário e do serviço um com o outro. Quando o usuário está pronto para acessar o serviço, o usuário (por exemplo, em software) gera um par de chaves

de longa duração para o serviço requisitado (etapa 304). Este par de chaves de longa duração é um dos valores de chave usados durante todas as operações de rechaveamento futuras. Para todos os cálculos matemáticos no restante deste pedido, nós assumimos que todas as partes envolvidas nas transações acordaram de antemão em um grupo G , de tamanho de ordem (q) e um elemento g de G , de modo que $q = \text{ordem}(g)$ seja um número primo grande. G e g podem ser publicamente conhecidos, isto é, eles não precisam ser mantidos secretos. Os cálculos matemáticos de exemplo para a criação de valores de chave são como se segue (usando-se um método SPEKE), e embora os cálculos de exemplo mostrados abaixo utilizem um grupo multiplicativo, será evidente que cálculos adequados poderiam ser realizados usando-se um grupo aditivo:

Capturar um Par de Chaves de Longa Duração (por exemplo, por um Usuário)

Capturar a randômico, $1 < a < q-1$;

Calcular $A = g^a$;

Se $A = 1$, continuar escolhendo a 's diferentes até $A \neq 1$.

O valor ' A ' é a chave pública de longa duração de usuário (ou, mais geralmente, uma primeira chave pública), e o valor ' a ' é a chave privada de longa duração de usuário (ou, mais geralmente, a primeira chave privada).

O número selecionado ' a ' é maior do que 1 e menor do que o número primo $q - 1$. Uma vez que a chave privada seja selecionada (isto é, ' a ') e a chave pública seja gerada (isto é, ' A '), a chave privada ' a ' é armazenada de forma segura, e a chave pública ' A ' é eventualmente transmitida

para o provedor de serviços.

Um par de chaves de autenticação de curta duração também é gerado pelo usuário, com base no segredo compartilhado 's' (etapa 306). Usando-se um cálculo similar seguindo-se um método de geração de chave SPEKE de exemplo, os cálculos matemáticos de exemplo para esta etapa são (usando, por exemplo, as mesmas hipóteses para q e 'a' (como agora aplicado a x) como antes):

Capturar um Par de Chaves de Autenticação de Curta Duração

10 (por exemplo, por um Usuário)

Capturar x randômico, $1 < x < q-1$;

Calcular $X = s^x$;

Se $X = 1$, continuar escolhendo novos x's até $X \neq 1$.

O valor 'X' é a chave pública de curta duração de usuário (ou, mais geralmente, uma segunda chave pública), e o valor 'x' é a chave privada de curta duração de usuário (ou, mais geralmente, a segunda chave privada). O valor 's' é o segredo compartilhado.

A seleção de 'x' é entre 1 e o número primo q-1. O software de usuário então envia os valores de chave pública 'A' e 'X' para a oferta de serviço (provedor de serviços), conforme mostrado na etapa 308. Esta etapa prossegue para (A), onde a oferta de serviço recebe os valores e realiza cálculos adicionais, mostrados na Figura 7. Uma vez que a oferta de serviço tenha completado aqueles cálculos, ela retorna um par similar de seus próprios valores de chave pública 'B' e 'Y' com um valor de confirmação de chave para o usuário para verificação (etapa 312), conforme discutido abaixo em relação à Figura 7. Isto é mostrado como uma entrada (B) na Figura 6 vindo da Figura 7. Neste ponto, o

usuário é capaz de usar 'B' e 'Y' para a criação de uma chave mestra usando, por exemplo, cálculos de SPEKE avançados. Pelo uso de 'B' e 'Y' em conjunto para a geração da chave mestra, o método de encriptação permite a implementação de um sigilo futuro perfeito. Isto é visto mais claramente na sequência de rechaveamento mostrada mais tarde. Um cálculo de chave mestra de exemplo é como se segue:

Calcular Chave Mestra (por exemplo, por Usuário):

```

10      k1 = Yx;
        k2 = Ba;
        verificar que k1, k2 != 0, 1 ou ordem (G) - 1;
        k = hash (k1 || k2), onde || é uma função de
        concatenação.

```

15 Aqui, 'x' é a chave de autenticação privada de curta duração de usuário (ou, mais geralmente, a segunda chave privada), e 'Y' é a chave de autenticação pública de curta duração recebida da oferta de serviço (ou, mais geralmente, a quarta chave pública). Também, 'a' é a chave de encriptação privada de longa duração de usuário (ou, mais

20 geralmente, a primeira chave privada), e 'B' é a chave de encriptação pública de longa duração recebida da oferta de serviço (ou, mais geralmente, a terceira chave pública).

O valor 'k' representa a chave mestra que pode ser usada para a encriptação de dados entre o usuário e o

25 serviço. O valor 'k' é a combinação das chaves intermediárias 'k1' (com base nas chaves de autenticação de curta duração) e 'k2' (com base nas chaves de encriptação de longa duração). Uma verificação importante é feita nos

30 valores de chave intermediários de k1 e k2 na etapa 314,

para verificar se estes dois valores não são 0, 1 ou ordem (G) - 1; caso contrário, isto poderia significar que há um ataque de segurança sendo tentado em 314. Este ataque poderia resultar se a chave estivesse sendo forçada em um pequeno subconjunto de possíveis chaves totais. Se o atacante enviasse um $X = 0$ ou $Y = 0$, as partes se comunicando poderiam obter um valor de chave resultante de 0. Esta verificação rápida assegura que um ataque não está sendo posto em prática. Se, contudo, o valor de k_1 ou k_2 cair realmente em um destes pequenos grupos de subconjunto, a negociação para uma chave pode ser abortada em 316.

Se um ataque de subconjunto não for detectado, a chave mestra 'k' pode ser usada pelo usuário para testar o valor de confirmação de chave enviado pela oferta de serviço (etapa 318). Um método para a geração de um valor de confirmação de chave é aplicar um hash à chave com uma cadeia conhecida, tais como os bytes na chave pública "A". Um cálculo de exemplo para se testar o valor de confirmação de chave seria:

20 Testar Valor de Confirmação de Chave

" h_A recebido" = h_A = hash ($k ||$ bytes de chave pública "A"), onde " h_A recebido" veio da oferta de serviço e 'k' é a chave mestra local.

Se o valor de confirmação de chave gerado por software para 'A' não combinar (etapa 320) com o valor de confirmação de chave recebido, então, ele está incorreto (etapa 322). Um valor de confirmação de chave incorreto poderia significar que um ataque *man-in-the-middle* (homem no meio) ou algum outro ataque está sendo tentado. A operação será abortada neste caso (etapa 322). Se os dois

valores de confirmação combinarem, então, é assumido que uma ligação plenamente segura foi estabelecida (etapa 324). A ligação é marcada como válida e, após um curto atraso será usada para comunicações (etapa 324). Usando a chave de verificação recém gerada, o usuário envia este valor de volta para o serviço (etapa 326). Este segue de volta para a Figura 6 seguindo o rótulo (C). Após uma pausa de poucos momentos, isto é, para se garantir que a confirmação seja recebida pela oferta de serviço, o usuário pode começar a trocar dados (etapa 328).

Quaisquer métodos de encriptação e de desencriptação adequados podem ser usados para a encriptação e a desencriptação de mensagens usando-se a chave mestra, tais como métodos de encriptação / desencriptação de chave simétrica, como o Padrão de Encriptação Avançado (AES) (Federal Information Processing Standards Publication 197, 26 de novembro de 2001, National Institute of Standards and Technology).

A Figura 7 é um fluxograma de dados de etapas de exemplo realizadas pela oferta de serviço (por exemplo, no software de provedor de serviços) para a realização da abordagem de exemplo mostrada na Figura 4, quando o usuário é o iniciador da troca de chave, conforme mostrado na Figura 4. O processo começa quando um usuário contata um provedor de serviços 'fora de banda' para trocar um segredo compartilhado (etapa 398). Isto corresponde à etapa 302 na Figura 6 no dispositivo de usuário. Esta troca fora de banda foi discutida várias vezes e também provê um nível de autenticação que o usuário e o serviço são quem eles dizem ser. Uma vez que esta troca esteja completa, o usuário está

livre em qualquer ponto no tempo para contatar o serviço para começar o processo. Uma vez que o usuário realmente contate o serviço de hospedagem, mostrado com a mensagem (A) chegando a partir do fluxograma de usuário na Figura 6, 5 o novo usuário é verificado (etapa 400). Uma vez que um provedor de serviços poderia ter dezenas ou centenas de usuários desejando começar a usar seu serviço em qualquer tempo, o provedor de serviços é passivo até o usuário decidir que ele quer começar o serviço. Embora um segredo 10 compartilhado tenha sido trocado, isto pode significar muito pouco, e segredos compartilhados velhos poderiam mesmo ser purgados após algum número de dias, se o usuário falhar em se conectar por aquele período de tempo. A chegada da mensagem permite que o provedor de serviços 15 encontre o novo usuário e verifique que um segredo compartilhado existe (etapa 400). Na mensagem está a chave de autenticação de curta duração pública do usuário, a qual é baseada no segredo compartilhado (etapa 400). A mensagem também contém a chave de encriptação de longa duração 20 pública do usuário (etapa 400), a qual pode ser usada na implementação para a criação do sigilo futuro perfeito, quando operações de rechaveamento ocorrerem, Figuras 7 e 8.

A oferta de serviço gera um par de chaves de encriptação de longa duração para este usuário, de uma 25 maneira similar ao par de chaves de encriptação de longa duração criado pelo usuário (etapa 402). Os cálculos matemáticos para a criação do par de chaves de encriptação de longa duração de oferta de serviço são como se segue (por exemplo, usando-se um método SPEKE):

30 Capturar um Par de Chaves de Longa Duração (por exemplo,

por um Provedor de Serviços)

Capturar b randômico, $1 < b < q-1$;

Calcular $B = g^b$;

Se $B = 1$, continuar escolhendo b 's diferentes até $B \neq 1$.

5 1.

O valor ' B ' é a chave pública de longa duração de oferta de serviço (ou, mais geralmente, uma terceira chave pública), e o valor ' b ' é a chave privada de longa duração de oferta de serviço (ou, mais geralmente, a terceira chave privada).

O número selecionado ' b ' é maior do que 1 e menor do que o número primo $q - 1$. Uma vez que a chave privada ' b ' seja selecionada e a chave pública ' B ' seja gerada, a chave privada ' b ' é armazenada de forma segura, e a chave pública ' B ' é eventualmente transmitida de volta para o usuário, de modo que ele possa usá-la em seus cálculos.

A oferta de serviço também gera um par de chaves de autenticação de curta duração, com base no segredo compartilhado (etapa 404). Usando-se um cálculo similar seguindo-se um método de geração de chave SPEKE de exemplo, os cálculos matemáticos de exemplo para esta etapa são (usando, por exemplo, as mesmas hipóteses para q e ' x ' (como agora aplicado a y) como antes):

25 Capturar um Par de Chaves de Autenticação de Curta Duração (por exemplo, por um Provedor de Serviços)

Capturar y randômico, $1 < y < q-1$;

Calcular $Y = s^y$;

Se $Y = 1$, continuar escolhendo novos y 's até $Y \neq 1$.

O valor ' Y ' é a chave de autenticação de curta duração pública de oferta de serviço (de provedor de serviços) (ou,

30 pública de oferta de serviço (de provedor de serviços) (ou,

mais geralmente, uma quarta chave pública), e o valor 'y' é a chave de autenticação de curta duração privada de oferta de serviço (ou, mais geralmente, a quarta chave privada).

A seleção de 'y' é entre 1 e o número primo $q - 1$. Os valores de chave pública 'B' e 'Y' serão eventualmente enviados para o usuário para a geração da própria chave mestra de usuário.

A oferta de serviço então usa as chaves de usuário 'A' e 'X' recebidas do usuário e as chaves privadas recém calculadas para a geração de uma chave mestra (etapa 406). Pelo uso de 'A' e 'X' em conjunto para a geração da chave mestra, o método de encriptação provê um sigilo futuro perfeito. Para a provisão do sigilo futuro perfeito, a implementação também usa as chaves privadas na nova geração das chaves subseqüentes, durante qualquer seqüência de rechaveamento. Um cálculo de chave mestra de exemplo é como se segue:

Calcular Chave Mestra (por exemplo, por Provedor de serviços)

20 $k1 = X^y;$
 $k2 = A^b;$
 verificar que $k1, k2 \neq 0, 1$ ou ordem $(G) - 1;$
 $k = \text{hash}(k1 || k2).$

Aqui, 'y' é a chave de encriptação privada de curta duração de oferta de serviço (ou, mais geralmente, a quarta chave privada), e 'X' é a chave de encriptação pública de curta duração recebida do usuário (ou, mais geralmente, a segunda chave pública). Também, 'b' é a chave privada de longa duração de oferta de serviço (ou, mais geralmente, a terceira chave privada), e 'A' é a chave de encriptação

pública de longa duração recebida do usuário (ou, mais geralmente, a primeira chave pública).

O valor 'k' representa a chave mestra gerada pela oferta de serviço, e é a mesma que a chave mestra gerada pelo usuário. Esta chave mestra pode ser usada para a encriptação de dados entre o serviço e o usuário. O valor 'k' é a combinação das chaves intermediárias 'k1' (com base nas chaves de autenticação de curta duração) e 'k2' (com base nas chaves de encriptação de longa duração). Uma verificação importante pode ser feita nos valores de chave intermediários de k1 e k2 na etapa 408, para verificar se estes dois valores não são 0, 1 ou ordem (G) - 1; caso contrário, isto poderia significar que há um ataque de segurança sendo tentado. Este ataque resultaria se a chave estivesse sendo forçada em um pequeno subconjunto de possíveis chaves totais. Se o atacante enviasse um $X = 0$ ou $Y = 0$, as partes se comunicando poderiam obter um valor de chave resultante de 0. Esta verificação rápida assegura que um ataque não está sendo posto em prática. Se, contudo, o valor de k1 ou k2 cair realmente em um destes pequenos grupos de subconjunto, a negociação para uma chave pode ser abortada (etapa 410).

Se um ataque de subconjunto não for detectado, a chave mestra 'k' poderá ser usada pelo usuário para testar o valor de confirmação de chave enviado pela oferta de serviço (etapa 416). Um método para a geração de um valor de confirmação de chave é aplicar um hash à chave com uma cadeia conhecida, tais como os bytes na chave pública "B". A criação de uma cadeia de teste de amostra ocorre na etapa 412. Um cálculo de exemplo para se testar a cadeia (valor

de confirmação de chave) seria:

Testar Valor de Confirmação de Chave

$h_B = \text{hash}(k \parallel \text{bytes de chave pública "B"})$.

A oferta de serviço então transmitiria a cadeia de
5 teste para o usuário, de modo que ele possa verificar que a
chave mestra gerada pelo usuário combina com a chave mestra
criada pela oferta de serviço. A oferta de serviço então
envia a chave de encriptação pública de longa duração 'B',
a chave de autenticação pública de curta duração 'Y' (ou a
10 quarta chave pública) e a cadeia de verificação h_B para o
usuário (etapa 414).

Uma vez que o usuário tenha gerado sua própria chave
mestra 'k', ele envia de volta um valor de confirmação de
chave final para garantir que a oferta de serviço sabe que
15 tudo funcionou corretamente (C). Esta etapa final (C) é
mostrada na Figura 7 como uma entrada para a oferta de
serviço na etapa 416. Se o valor de confirmação de chave
foi calculado com base em 'A' e enviado para a oferta de
serviço (etapa 416), então, isto é o que o teste procura
20 (etapa 418). Se o valor de confirmação de chave não
combinar com o valor esperado, a operação é abortada (etapa
420). Se o valor de confirmação de chave for combinado,
então, será assumido que existe um percurso de comunicação
de dados plenamente encriptado de duas vias e seguro (etapa
25 422).

A Sequência de Fluxo de Dados de Rechaveamento

A Figura 8 é um fluxograma de dados que mostra etapas
de exemplo no usuário (por exemplo, no software) para uma
seqüência de rechaveamento quando da nova geração de uma
30 outra chave no ambiente ilustrado nas Figuras 1, 2 e 3.

Este procedimento ilustra a utilidade de uso de uma chave de encriptação de longa duração para se permitir a implementação de um sigilo futuro perfeito. O processo começa com quando o usuário ou a oferta de serviço decide que uma nova chave é requerida. Para este exemplo, nós assumimos que a hospedagem (provedor de serviços) está rodando um temporizador de expiração de chave de encriptação. Contudo, há muitas outras formas pelas quais a chave de encriptação poderia ser gerada de novo. O usuário poderia decidir que é o momento de uma nova chave, o usuário ou o serviço poderia temer que alguém estivesse tentando atacar e determinar o valor de chave atual. Qualquer que seja o caso, uma nova chave é desejada, e um método único, não baseado no segredo compartilhado original, pode ser usado para a geração da nova chave.

Como mostrado no exemplo da Figura 8, uma requisição de rechaveamento é recebida pelo usuário, ou o usuário decide partir para uma nova chave (etapa 430). Obviamente, a etapa 430 poderia ser executada pelo provedor de serviços ao invés de pelo usuário. O software de usuário gera uma nova chave de encriptação de curta duração (etapa 432). Um cálculo matemático de exemplo é baseado em SPEKE e usa a mesma sequência como mostrado antes:

Capturar um Novo Par de Chaves de Longa Duração (por exemplo, por um Usuário)

Capturar x randômico, $1 < x < q-1$;

Calcular $X = g^x$;

Se $X = 1$, continuar escolhendo x 's diferentes até $X \neq 1$.

Aqui, ' x ' é um valor "novo" gerado para a chave de

encriptação privada de curta duração de usuário. O valor 'x' pode ser referido como uma chave "de encriptação" ou como uma chave de "autenticação" (como foi feito previamente), porque o valor 'x' contribui para ambos os aspectos. A seleção de 'x' deve ser entre 1 e o número primo $q - 1$. O software de usuário então envia o valor de chave pública recém gerado 'X' para o provedor de serviços 434. Esta etapa prossegue para (D), onde o provedor de serviços recebe o valor e realiza cálculos adicionais. A etapa (D) então é feita na Figura 9 como uma entrada no lado de provedor de serviços da conexão.

Uma vez que o provedor de serviços tenha completado aqueles cálculos com (D) mostrado na Figura 9, ele retorna uma chave de encriptação pública nova similar 'Y' (discutida adicionalmente abaixo) com i, valor de confirmação de chave para verificação pelo usuário (E). Isto é mostrado como a entrada (E) na Figura 8. Neste ponto, o usuário é capaz de usar a nova chave 'Y' do provedor de serviços com a chave 'B' pública de longa duração mais antiga do provedor de serviços para a criação de uma chave mestra na etapa 440 seguindo-se cálculos avançados de SPEKE, por exemplo. Pelo uso da 'B' existente e da nova 'Y' em conjunto para a geração da chave, o método de encriptação pode prover uma implementação de sigilo futuro perfeito. O sigilo futuro perfeito pode ser obtido porque nem a 'B' existente nem a nova 'Y' são baseadas no segredo compartilhado original, e a 'B' existente é combinada com a nova 'Y' para a criação de uma nova chave não diretamente baseada na chave prévia. Adicionalmente, a chave 'B' existente realiza parte da autenticação gerada

com o segredo compartilhado original. Apenas um usuário de serviço autenticado que originalmente possuía o segredo compartilhado teria sido capaz de ter a chave privada 'b' salva em disco. Isto é visto mais claramente no cálculo matemático de rechaveamento de exemplo para a criação de uma nova chave mestra 'k':

Calcular Chave Mestra (por exemplo, por Usuário)

```
k1 = Yx;  
k2 = Ba;  
10 verificar que k1, k2 != 0, 1 ou ordem (G) - 1;  
k = hash (k1 || k2).
```

Aqui, 'x' é a chave de encriptação privada de curta duração de usuário e 'Y' é a nova chave de encriptação pública de curta duração recebida gerada pelo provedor de serviços. O valor 'a' é a chave de encriptação privada de longa duração de usuário e 'B' é a chave de encriptação pública de longa duração existente do provedor de serviços.

O valor 'k' representa a nova chave mestra que pode ser usada para a encriptação de dados entre o usuário e o provedor de serviços. O valor 'k' é a combinação das chaves intermediárias 'k1' (com base na chave de encriptação de curta duração) e 'k2' (com base nas chaves de encriptação de longa duração). Uma verificação importante é feita nos valores de chave intermediários de k1 e k2 (etapa 442), para verificar se estes dois valores não são 0, 1 ou ordem (G) - 1; caso contrário, isto poderia significar que há um ataque de segurança sendo tentado (etapa 442). Se, contudo, o valor de k1 ou k2 cair realmente em um destes pequenos grupos de subconjunto, a negociação para uma chave pode ser abortada (etapa 444).

Se um ataque de subconjunto não for detectado, a nova chave mestra 'k' pode ser usada para se testar o valor de confirmação de chave enviado pela oferta de serviço (provedor de serviços), conforme mostrado na etapa 446. Um método para a geração de um valor de confirmação de chave é aplicar um hash à chave com uma cadeia conhecida como os bytes na chave pública de "A". A abordagem para o cálculo de um valor de confirmação de chave pode ser a mesma conforme descrito pref. Se o valor de confirmação de chave não combinar com o que foi recebido (etapa 448), a chave será assumida como estando em erro (etapa 450). Um valor de confirmação de chave incorreto significaria que um ataque *man-in-the-middle* (homem no meio) ou algum outro ataque está sendo tentado. Caso contrário, o usuário gera um valor de confirmação de chave final usando a chave mestra 'k' (etapa 452). O valor de confirmação de chave é enviado para o provedor de serviços (etapa 454) como uma confirmação final; conforme mostrado no ponto (F) na Figura 8. Então, após uma pausa curta, a nova chave de encriptação é usada no software de usuário (etapa 456). Durante um período de tempo curto, também haverá uma janela em que as mensagens que foram previamente transmitidas poderiam chegar. Durante este período de vários minutos, a chave antiga é mantida e tentada, se um erro de descriptação ocorrer (etapa 456).

Voltando-nos, agora, para a Figura 9, esta representa um fluxograma de dados de etapas de exemplo no provedor de serviços para uma seqüência de rechaveamento quando da nova geração de uma outra chave no ambiente ilustrado nas Figuras 1, 2 e 3. Este procedimento mostra a utilidade de usar a chave de encriptação de longa duração para a

implementação do sigilo futuro perfeito. Nesta modalidade, nós assumimos que o usuário começou o processo e já criou um novo par de chaves de encriptação (ou de autenticação) de curta duração, conforme mostrado na Figura 8. A chegada da chave de encriptação pública de curta duração 'X' é mostrada como a entrada (D). A chave pública é recebida e a informação de confirmação de usuário é lembrada e checada (etapa 460). A oferta de serviço então gera um novo par de chaves de encriptação de curta duração pelo próximo segmento de tempo (etapa 462). O cálculo matemático de exemplo para a criação de uma nova chave de encriptação de curta duração é similar àquele que foi mostrado antes, exceto pelo fato de o segredo compartilhado 's' não ser usado.

15 Capturar um Novo Par de Chaves de Longa Duração (por exemplo, por um Provedor de Serviços)

Capturar y randômico, $1 < y < q-1$;

Calcular $Y = g^y$;

Se $Y = 1$, continuar escolhendo y 's diferentes até $Y \neq 1$

20 1.

A seleção de 'y' está entre 1 e o número primo $q - 1$. O valor 'Y' eventualmente será enviado para o usuário para a geração de uma chave mestra (etapa 472).

Após capturar um novo par de chaves de encriptação de curta duração, uma chave mestra é gerada pelo provedor de serviços usando o valor 'X' que foi recém recebido do usuário e o valor recém gerado 'y'. Pelo uso de 'A' e 'X' em conjunto para a geração da chave, o método de encriptação provê um sigilo futuro perfeito. Um cálculo de exemplo de chave mestra é como se segue:

25

30

Calcular Chave Mestra (por exemplo, por Provedor de serviços)

$k1 = X^y;$

$k2 = A^b;$

5 verificar que $k1, k2 \neq 0, 1$ ou ordem $(G) - 1$;

$k = \text{hash}(k1 || k2).$

Aqui, 'y' é a nova chave de encriptação privada de curta duração de provedor de serviço e 'X' é a nova chave de encriptação pública de curta duração recebida gerada pelo usuário. O valor 'b' é a chave privada de longa duração existente de provedor de serviços e 'A' é a chave de encriptação pública de longa duração existente.

O valor 'k' representa a chave mestra para a oferta de serviço (etapa 464). Isto será usado para a encriptação de todos os dados entre a oferta de serviço e o usuário. O valor 'k' é a combinação das chaves intermediárias 'k1' (com base nas novas chaves de autenticação de curta duração) e 'k2' (com base nas chaves de encriptação de longa duração). O cálculo de 'k' não é diretamente dependente do segredo compartilhado original 's', mas os valores 'A' e 'b' portam parte da autenticação originalmente provida por 's'. Uma verificação pode ser feita sobre os valores intermediários de k1 e k2 (etapa 466), para verificar se estes dois valores não são 0, 1 ou ordem $(G) - 1$; caso contrário, isto poderia significar que há um ataque de segurança sendo tentado. Se, contudo, k1 ou k2 cair realmente em um destes pequenos grupos de subconjunto, a negociação para uma chave pode ser abortada (etapa 468).

30 Se um ataque de subconjunto não for detectado, a chave

mestra 'k' poderá ser usada para se testar o valor de confirmação de chave enviado pela oferta de serviço (etapa 470). Um método para a geração de um valor de confirmação de chave é aplicar um hash à chave com uma cadeia conhecida, tais como os bytes na chave pública "B" (etapa 470). Este cálculo pode ser similar àqueles já descritos. A oferta de serviço então transmitiria uma nova chave de encriptação pública de curta duração 'Y', e o valor de confirmação de chave h_B para o usuário (etapa 472). Esta transferência dos valores de chave e do valor de confirmação de chave é mostrada na caixa de transferência (E) na Figura 9.

Uma vez que o usuário tenha gerado sua própria chave mestra 'k', ele envia um valor de confirmação de chave final para garantir que a oferta de serviço saiba que tudo funcionou corretamente (etapa 454 da Figura 8), conforme mostrado em (F). Esta etapa final em (F) é mostrada na Figura 9 como uma entrada para a oferta de serviço (etapa 474). Se o valor de confirmação de chave foi calculado para 'A' e enviado para a oferta de serviço (etapa 474), então, isto é o que o teste procura (etapa 476). Se o valor de confirmação de chave não combinar com o valor esperado, a operação será abortada (etapa 478). Se o valor de confirmação de chave for verificado, então, é assumido que existe um percurso de comunicação de dados pleno de duas vias encriptado e seguro (etapa 480). O servidor mantém a chave prévia por vários minutos, somente como garantia no caso de pacotes estarem a caminho durante este estágio de geração de nova chave (etapa 480).

De acordo com um outro aspecto, qualquer forma de

portador legível em computador pode conter as instruções de processamento adaptadas para fazerem com que uma unidade de processamento execute os métodos descritos aqui. O portador legível em computador pode ser qualquer tipo adequado de portador, tal como uma memória de estado sólido (por exemplo, uma memória apenas de leitura (ROM), uma memória de acesso randômico (RAM), etc.), uma memória magnética, uma memória ótica, um outro tipo de memória, ou ondas / sinais modulados (tais como ondas / sinais modulados com frequência de rádio, frequência de áudio ou frequência ótica) contendo um conjunto apropriado de instruções de computador que fariam com que uma unidade de processamento realizasse as técnicas descritas aqui.

Tendo descrito em detalhes as modalidades de exemplo da presente invenção, incluindo os métodos de operação de exemplo, é para ser compreendido que as operações descritas aqui são apresentadas apenas a título de exemplo e não têm por significado limitarem o escopo da presente invenção, o qual é definido pelas reivindicações a seguir.

REIVINDICAÇÕES

1. Método realizado por um primeiro sistema (32) para estabelecer um percurso de comunicação bidirecional (24, 36) entre o primeiro sistema (32) e um segundo sistema (22) para um troca de uma ou mais mensagens, o método **caracterizado** por compreender:

a geração de um primeiro par de chaves tendo uma primeira chave pública e uma primeira chave privada;

a geração de um segundo par de chaves tendo uma segunda chave pública e uma segunda chave privada, a segunda chave pública sendo gerada com base em um segredo conhecido compartilhado conhecido pelo primeiro sistema (32) e pelo segundo sistema (22);

em que o segredo compartilhado é comunicado através de um canal seguro fora de banda (34);

o envio da segunda chave pública e da primeira chave pública para o segundo sistema (22);

a recepção de uma terceira chave pública e de uma quarta chave pública geradas pelo segundo sistema (22), a quarta chave pública sendo gerada com base no segredo compartilhado; e

o cálculo de uma chave mestra com base na primeira chave privada, na segunda chave privada, na terceira chave pública e na quarta chave pública, em que a chave mestra é configurada para ser usada na criptografia de uma ou mais mensagens.

2. Método, de acordo com a reivindicação 1, **caracterizado** pelo fato de ainda compreender:

gerar uma cadeia de teste;

enviar uma primeira cadeia de teste ao segundo sistema

(22)

receber uma segunda cadeia de teste gerada pelo segundo sistema (22); e

autenticar o segundo sistema (22) com a segunda cadeia de teste e a chave mestra.

3. Método, de acordo com a reivindicação 2, **caracterizado** pelo fato de ainda compreender uma etapa de receber uma carga útil de dados tendo uma entrada de serviço de Descrição, Descoberta e Integração Universais (UDDI), antes da etapa de receber uma segunda cadeia de teste gerada pelo segundo sistema (22).

4. Método, de acordo com a reivindicação 1, **caracterizado** pelo fato de que o primeiro sistema compreende um dispositivo móvel sem fio (32).

5. Método, de acordo com a reivindicação 1, **caracterizado** pelo fato de que o segundo sistema compreende um sistema hospedeiro (22) oferecendo serviços.

6. Método, de acordo com a reivindicação 5, **caracterizado** pelo fato de que o segredo compartilhado compreende um número de identificação pessoal (PIN) gerado automaticamente pelo sistema hospedeiro (22).

7. Método, de acordo com a reivindicação 4, **caracterizado** pelo fato de que o segredo compartilhado é recebido do segundo sistema (22) através de uma interface web seguindo uma solicitação pelo primeiro sistema (32).

8. Método, de acordo com a reivindicação 5, **caracterizado** pelo fato de que a troca de uma ou mais mensagens compreende uma troca de mensagens de e-mail, mensagens XML baseadas em http ou mensagens WML baseadas em http.

9. Método, de acordo com a reivindicação 5, **caracterizado** pelo fato de que o dispositivo móvel sem fio (32) e o sistema hospedeiro (22) são endereçados com endereços de e-mail ou endereços IP.

5 10. Método, de acordo com a reivindicação 5, **caracterizado** pelo fato de que o método SPEKE (Simple Password Exponential Key Exchange) modificado é utilizado no cálculo da chave mestra.

10 11. Método, de acordo com a reivindicação 1, **caracterizado** pelo fato de que o primeiro sistema compreende um sistema hospedeiro oferecendo serviços (46), e em que o segundo sistema compreende um dispositivo sem fio móvel (48).

15 12. Método, de acordo com a reivindicação 1, **caracterizado** pelo fato de ainda compreender a criptografia de uma ou mais mensagens usando a chave mestra.

13. Sinal digital **caracterizado** pelo fato de conter uma ou mais mensagens que são criptografadas de acordo com o método conforme definido na reivindicação 12.

20 14. Portadora que pode ser lida em computador, **caracterizada** pelo fato de conter instruções de processamento adaptadas para fazerem com que uma unidade de processamento execute o método conforme definido na reivindicação 1.

25 15. Primeiro sistema (32) para estabelecer um percurso de comunicação bidirecional (24, 36) para um segundo sistema (22) para um troca de uma ou mais mensagens, o sistema **caracterizado** por compreender:

30 um meio para a geração de um primeiro par de chaves que tem uma primeira chave pública e uma primeira chave

privada;

um meio para a geração de um segundo par de chaves tendo uma segunda chave pública e uma segunda chave privada, a segunda chave pública sendo gerada com base em
5 um segredo compartilhado conhecido pelo primeiro sistema (32) e pelo segundo sistema (22);

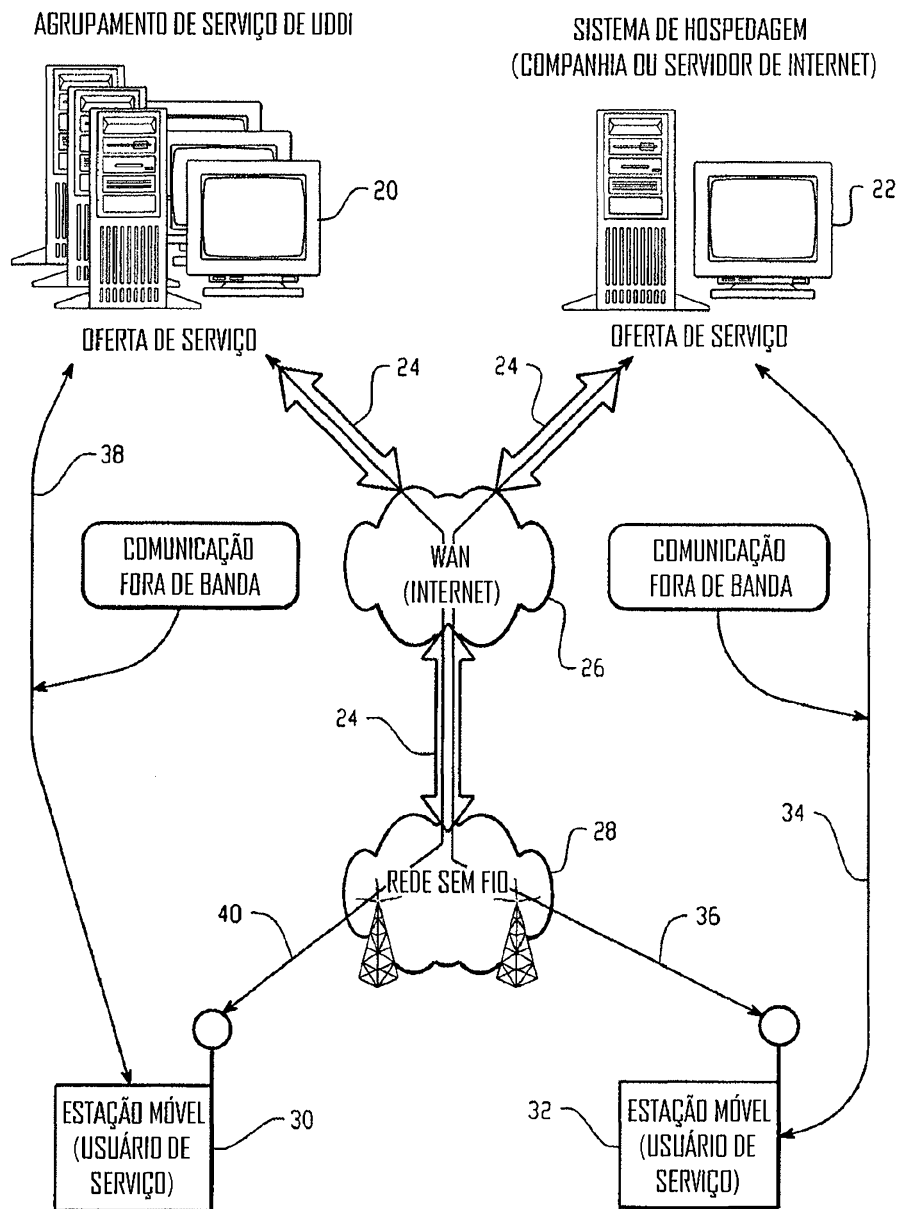
em que o segredo compartilhado é comunicado através de um canal seguro fora de banda (34);

um meio para o envio da segunda chave pública e da
10 primeira chave pública para o segundo sistema (22);

um meio para a recepção de uma terceira chave pública e de uma quarta chave pública geradas pelo segundo sistema (22), a quarta chave pública sendo gerada com base no segredo compartilhado; e

15 um meio para o cálculo de uma chave mestra com base na primeira chave privada, na segunda chave privada, na terceira chave pública e na quarta chave pública, em que a chave mestra é configurada para ser usada na criptografia de uma ou mais mensagens.

20

*Fig. 1*

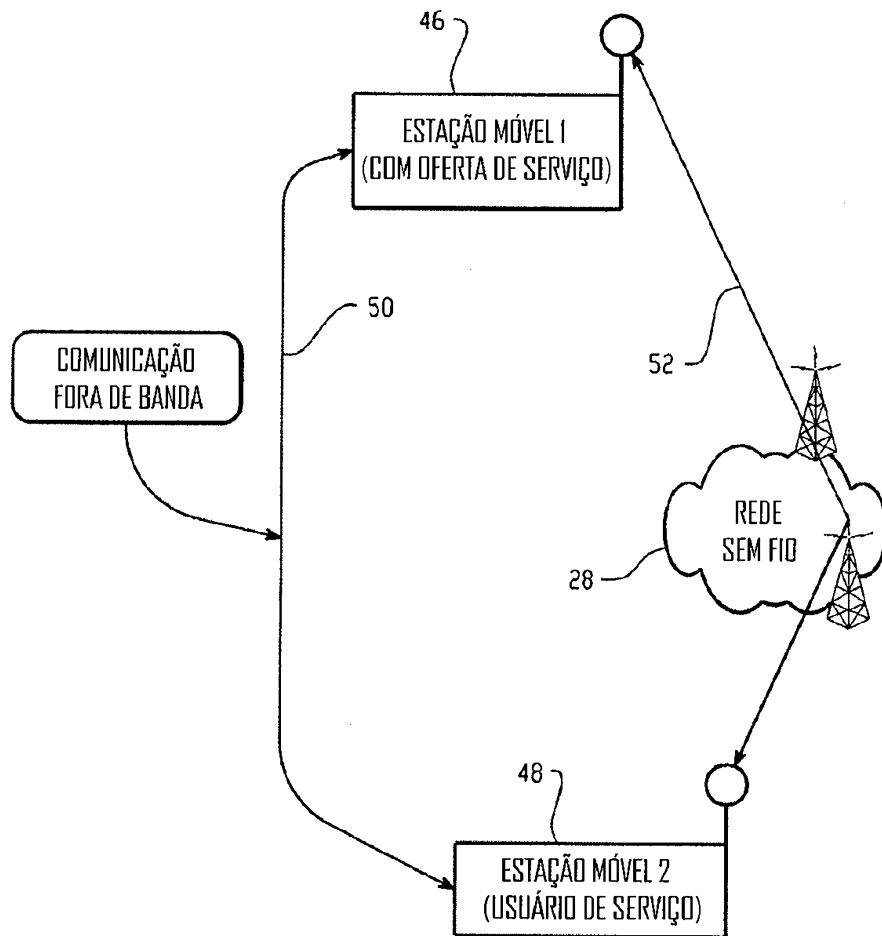


Fig. 2

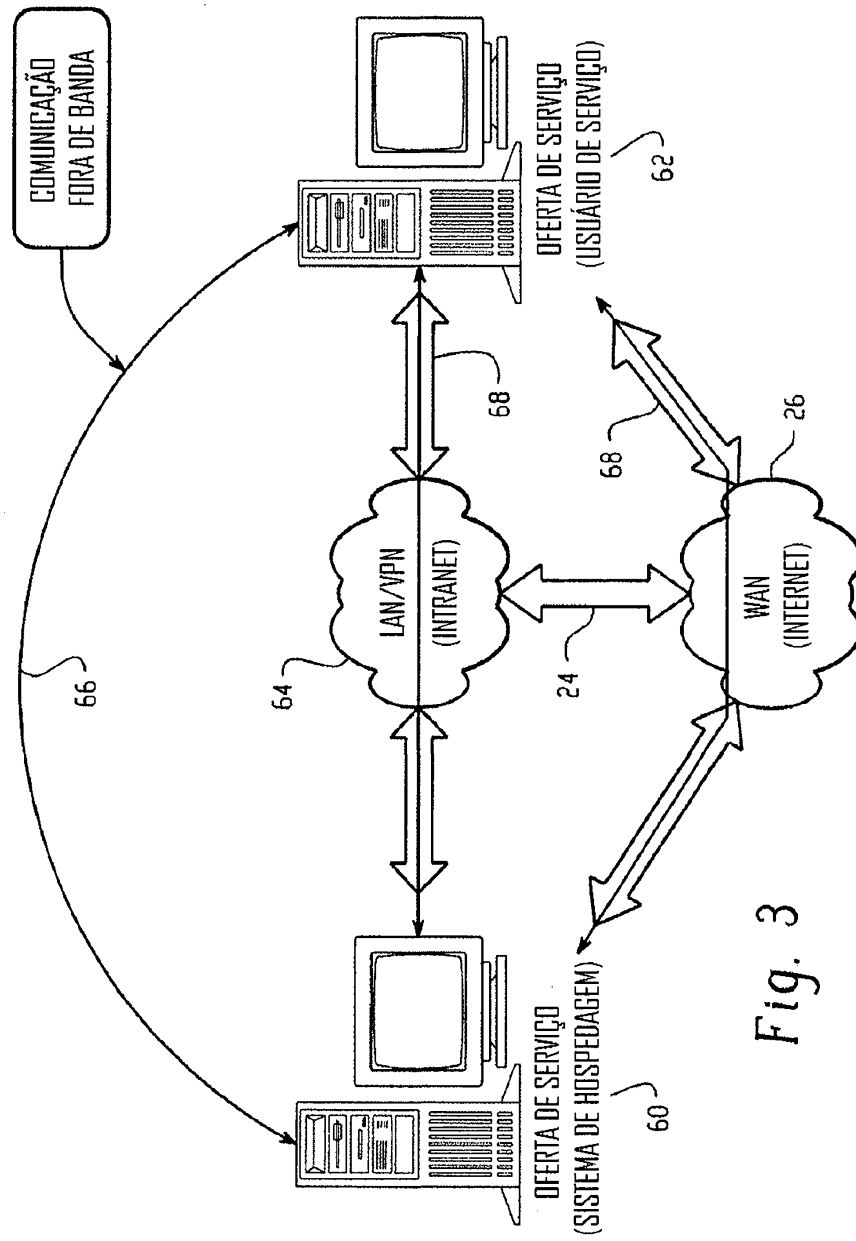


Fig. 3

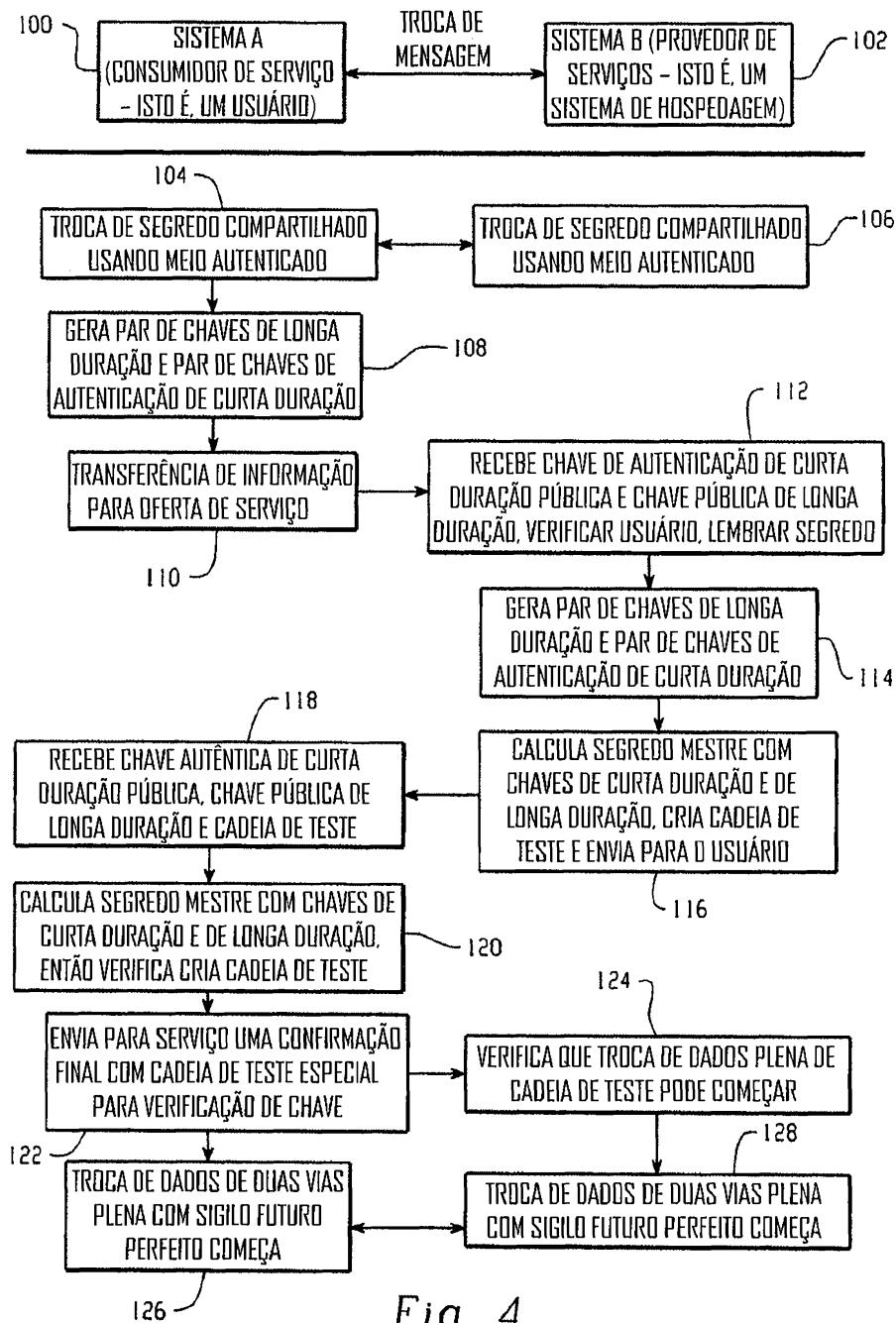


Fig. 4

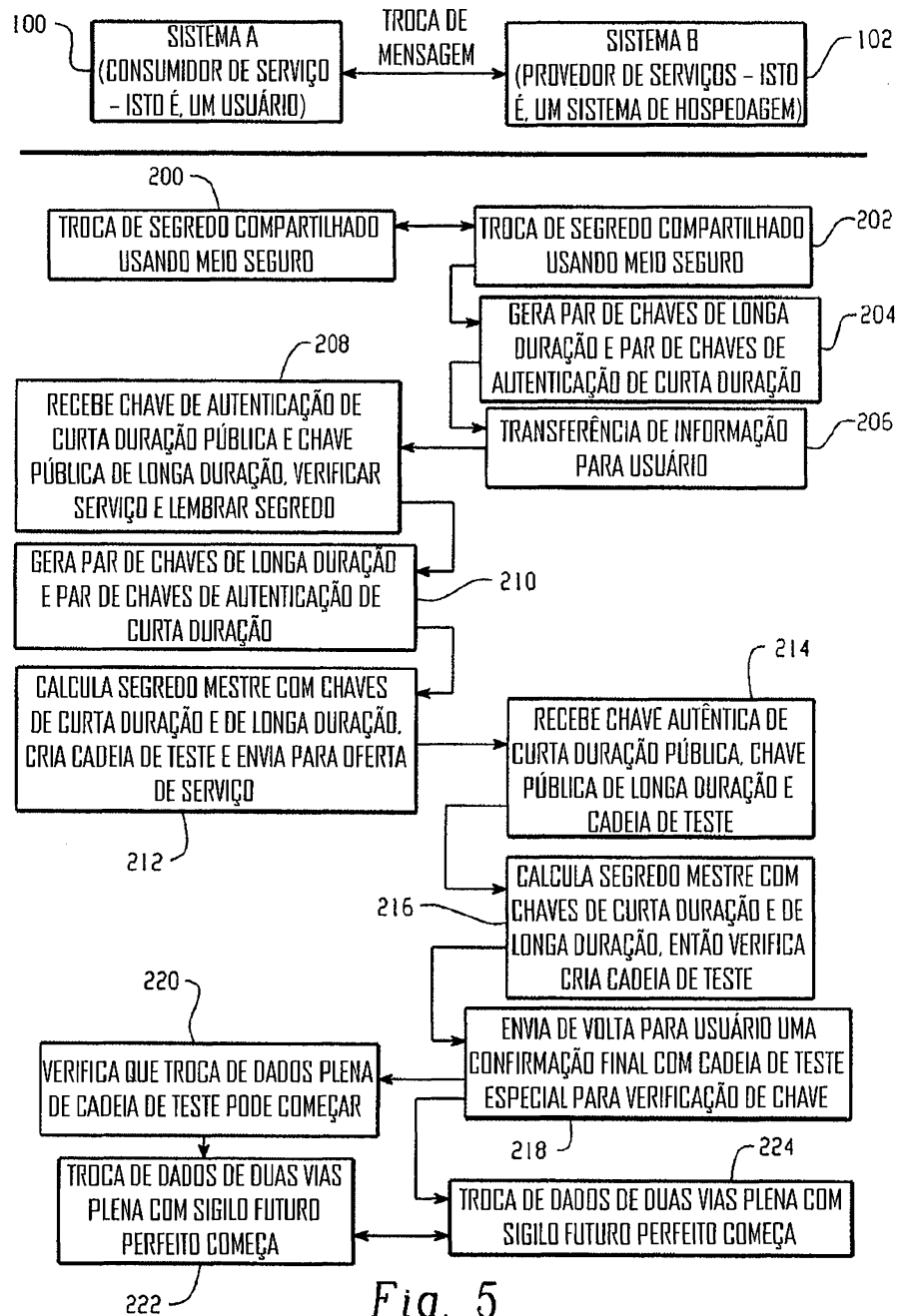


Fig. 5

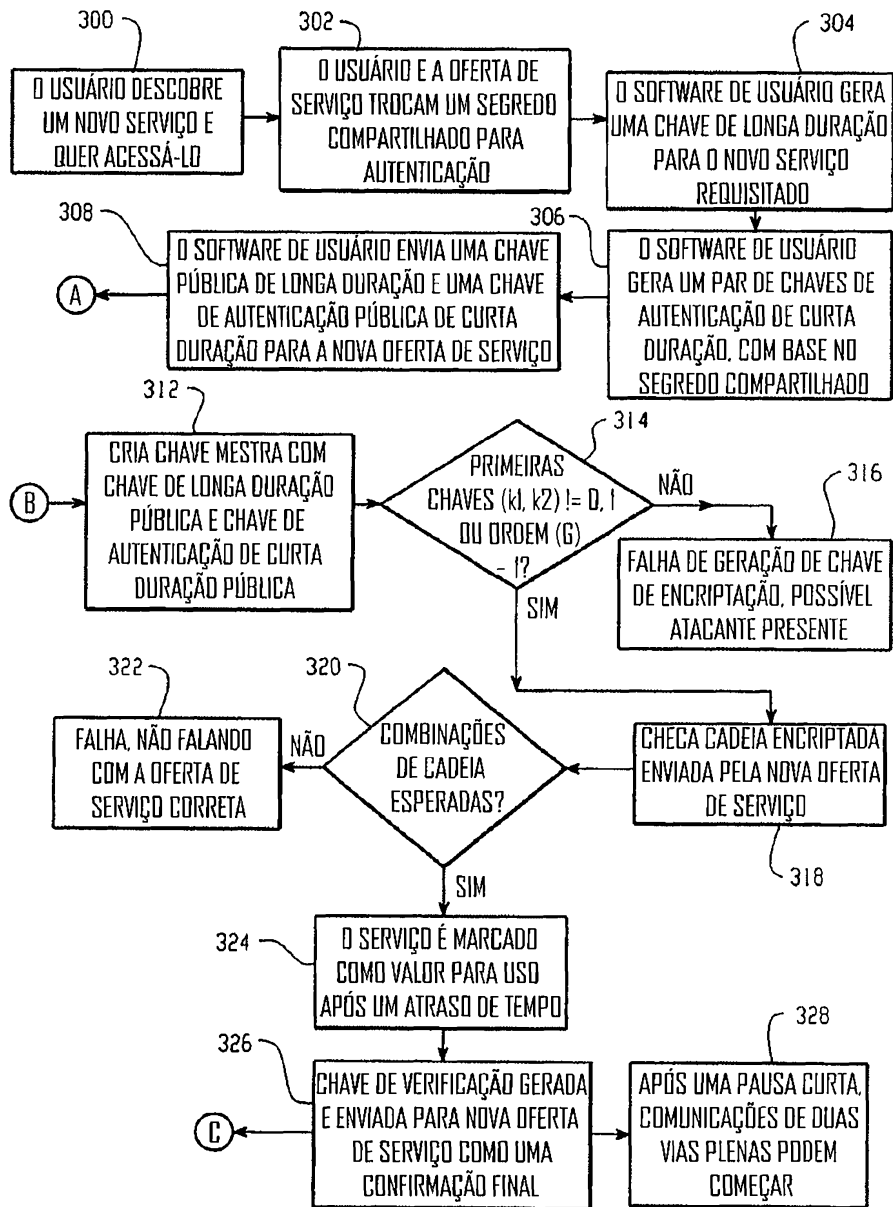


Fig. 6

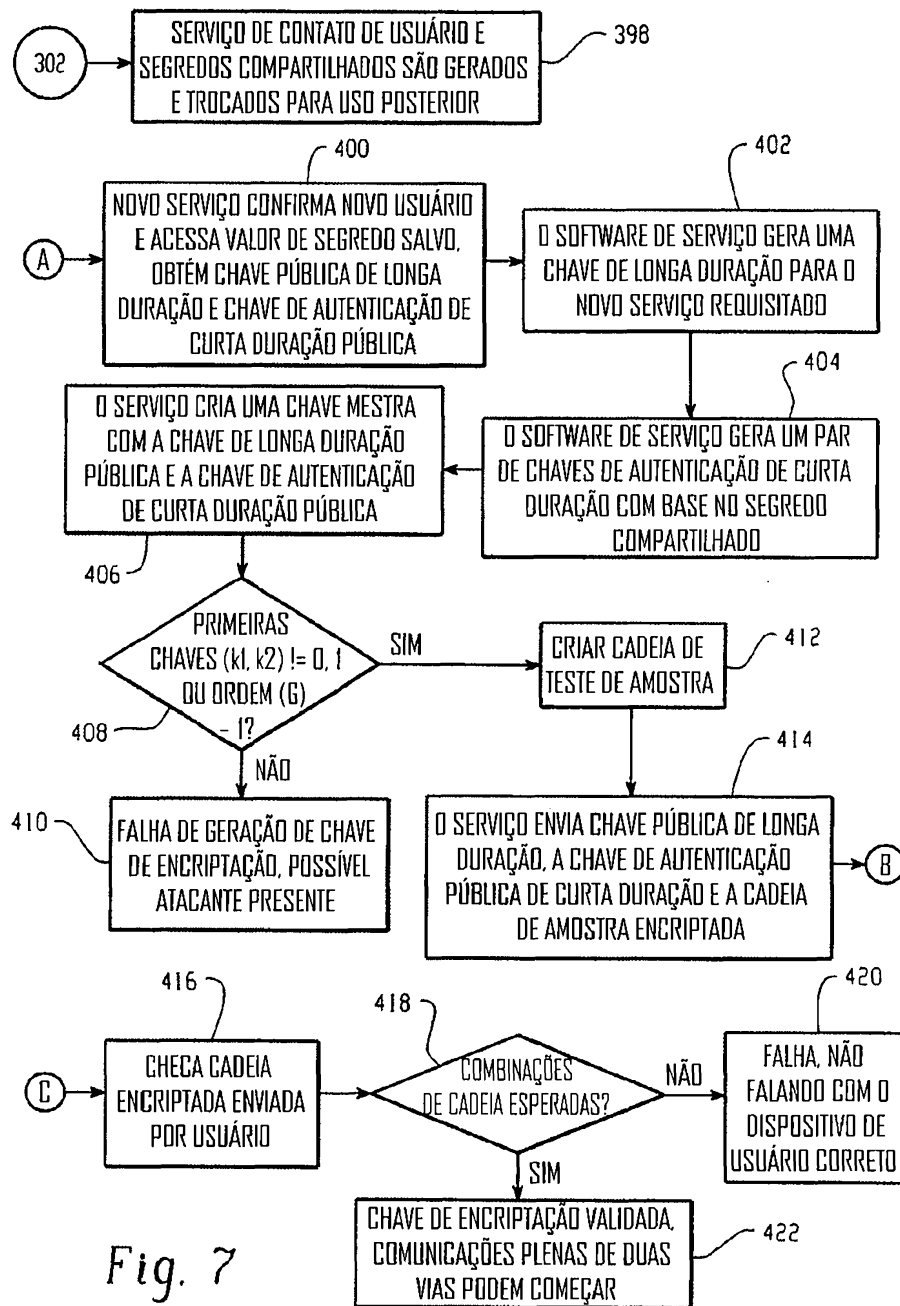


Fig. 7

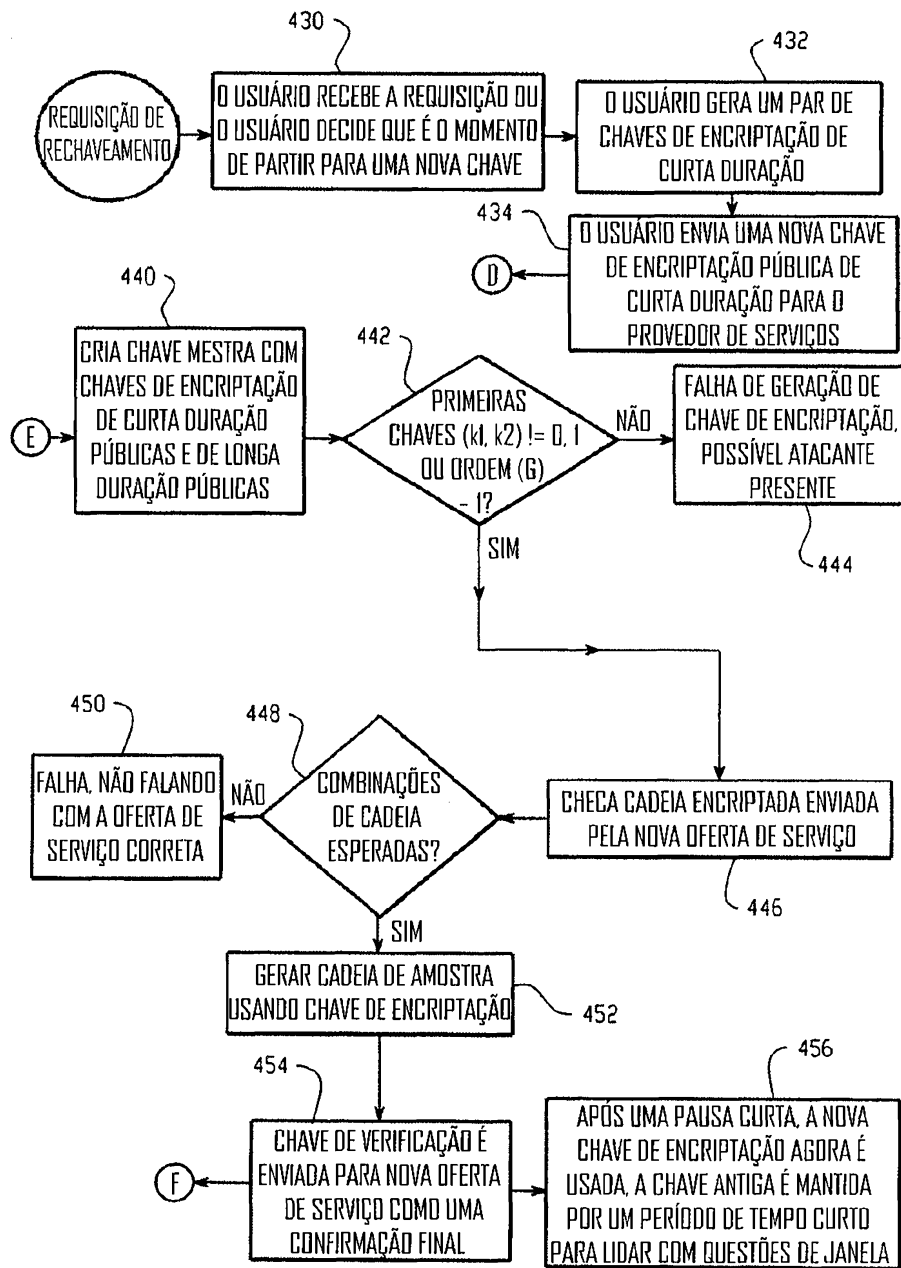


Fig. 8

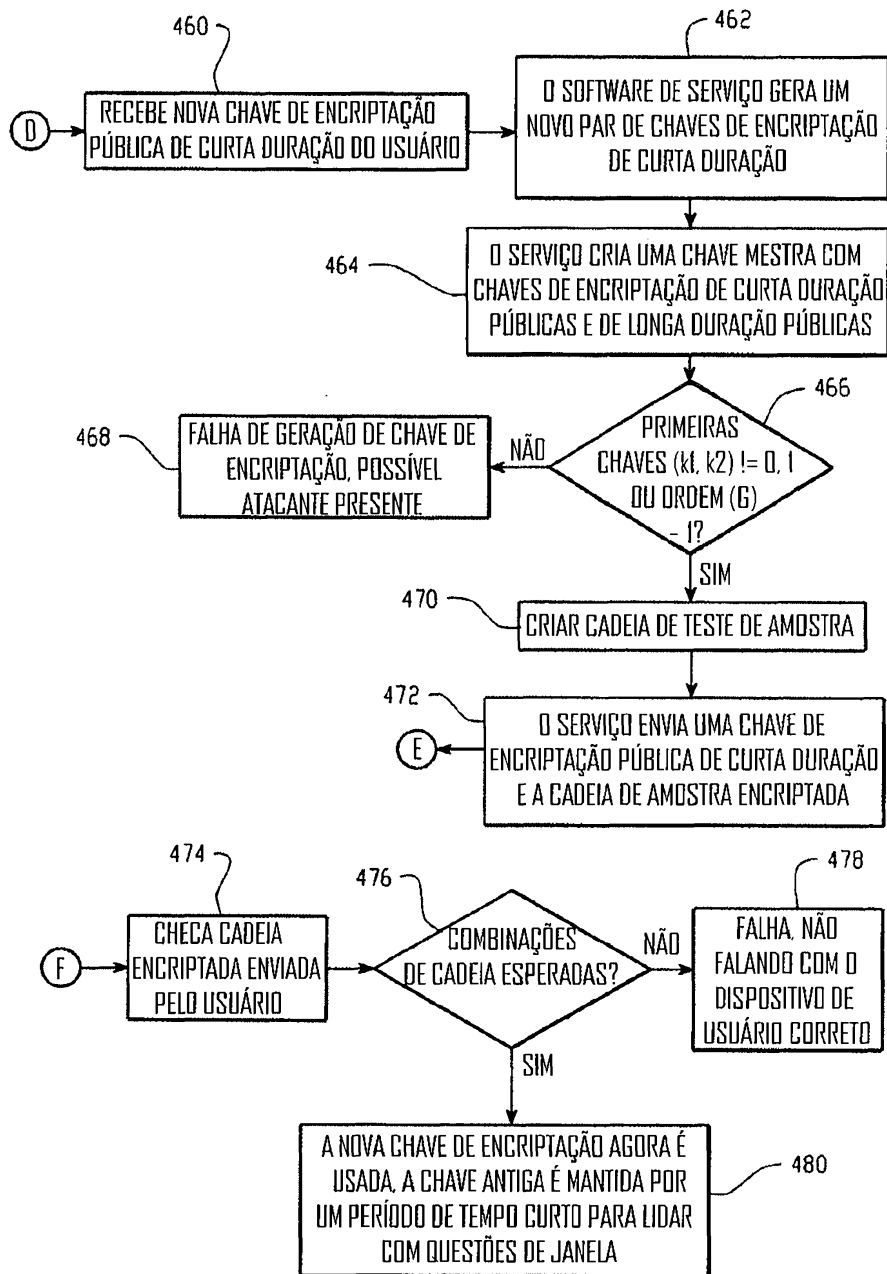


Fig. 9