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

(11) BR 112014007665-0 B1

(22) Data do Depósito: 28/09/2012

(45) Data de Concessão: 13/07/2021

(54) Título: MÉTODO, MEIO DE ARMAZENAMENTO E SISTEMA DE COMPUTAÇÃO DE DERIVAÇÃO CHAVE BASEADA EM PARÂMETROS

(51) Int.Cl.: G06F 15/16.

(30) Prioridade Unionista: 29/09/2011 US 13/248.962; 29/09/2011 US 13/248.953; 29/09/2011 US 13/248.973.

(73) Titular(es): AMAZON TECHNOLOGIES, INC..

(72) Inventor(es): GREGORY B. ROTH; BRADLEY JEFFERY BEHM; ERIC D. CRAHEN; CRISTIAN M. ILAC; NATHAN R. FITCH; ERIC JASON BRANDWINE; KEVIN ROSS O'NEILL.

(86) Pedido PCT: PCT US2012058083 de 28/09/2012

(87) Publicação PCT: WO 2013/049689 de 04/04/2013

(85) Data do Início da Fase Nacional: 28/03/2014

(57) Resumo: DERIVAÇÃO CHAVE BASEADA EM PARÂMETROS. Sistemas e métodos para chaves que geram autenticação a partir de credenciais secretas compartilhadas entre partes de autenticação e autenticadores. A geração das chaves pode envolver utilizar informações especializadas que, como resultado de serem usadas para gerar as chaves, geram as chaves geradas utilizáveis para um escopo menor de usos do que a credencial secreta. Ainda, a geração de chave pode envolver várias invocações de uma função onde cada um pelo me-nos um subgrupo de invocações da função resulta em uma chave que tem um escopo menor de uso permissível do que uma chave produzida a partir de várias invocações anteriores da função. As chaves geradas podem ser usadas como chaves de assinatura para assinar as mensagens. Uma ou mais ações podem ser tomadas dependendo de se uma mensagem e/ou o modo no qual a mensagem foi submetida cumpre com as restrições de uso da chave.

“MÉTODO, MEIO DE ARMAZENAMENTO E SISTEMA DE COMPUTAÇÃO DE DERIVAÇÃO CHAVE BASEADA EM PARÂMETROS”

REFERÊNCIA CRUZADA A PEDIDOS RELACIONADOS

[001] Este pedido reivindica prioridade do pedido de patente US 13/248.962, depositado em 29 de setembro de 2011, intitulado “PARAMETER BASED KEY DERIVATION” (Arquivo do Procurador N.º 90204-813889 (029400PC)); 13/248.953, depositado em 29 setembro de 2011, intitulado “TECHNIQUES FOR CLIENT CONSTRUCTED SESSIONS” (Arquivo do Procurador N.º 90204-818478 (032300US)) e 13/248.973, depositado em 29 de setembro de 2011, intitulado “KEY DERIVATION TECHNIQUES” (Arquivo do Procurador N.º 90204-813890 (029500US)), as divulgações completas são aqui incorporadas por referência.

FUNDAMENTOS

[002] Ambientes de computação assumem muitas formas. Como exemplo, as organizações geralmente utilizam redes de dispositivos de computação para fornecer um conjunto robusto de serviços aos seus usuários. Redes frequentemente incluem várias fronteiras geográficas e muitas vezes se conectam com outras redes. Uma organização, por exemplo, pode apoiar suas operações usando ambas as redes internas de recursos de computação e de recursos de computação gerenciados por outros. Computadores da organização, por exemplo, podem se comunicar com computadores de outras organizações para acessar e/ou fornecer dados enquanto usando serviços de outra organização. Em muitos casos, as organizações configuram e operam redes remotas usando hardware gerenciado por outras organizações, reduzindo, assim, os custos de infraestrutura e alcançando outras vantagens.

[003] Embora diversos ambientes de computação provaram ser úteis para uma ampla variedade de aplicativos, tais ambientes apresentam muitos desafios. Por exemplo, configurar os recursos do computador em prol de um objetivo organi-

zacional pode afetar adversamente em prol de outro objetivo organizacional. Por exemplo, a gestão eficaz da segurança de recursos de computação muitas vezes pode vir à custa do acesso eficiente aos dados e serviços. Equilibrar os objetivos de segurança e eficiência pode ser bastante desafiador, muitas vezes exigindo esforço e recursos significativos.

BREVE DESCRIÇÃO DOS DESENHOS

[004] A Figura 1 mostra um exemplo ilustrativo de um ambiente de computação que pode ser utilizado para implementar vários aspectos da presente divulgação, de acordo com pelo menos uma modalidade;

[005] A Figura 2 mostra um exemplo ilustrativo de um ambiente que inclui um provedor de recursos de computação que gera múltiplas zonas de falha de acordo com pelo menos uma modalidade;

[006] A Figura 3 mostra um exemplo ilustrativo de um ambiente no interior de uma zona de falha da Figura 2, de acordo com pelo menos uma modalidade;

[007] A Figura 4 mostra um exemplo ilustrativo de uma configuração de recursos de computação que pode ser usada para suportar um ambiente como o ambiente mostrado na Figura 3, de acordo com pelo menos uma modalidade;

[008] A Figura 5 é um diagrama que ilustra um exemplo da forma com que vários elementos que participam em um ambiente de computação podem ser escopos diferentes alocados de acordo com pelo menos uma modalidade;

[009] A Figura 6 é um diagrama que ilustra um exemplo da forma com que a informação pode ser comunicada entre os participantes de um processo de verificação de assinatura da mensagem de acordo com pelo menos uma modalidade;

[010] A Figura 7 é um fluxograma que mostra um exemplo ilustrativo de um processo para assinatura de mensagens, de acordo com uma modalidade;

[011] A Figura 8 é um fluxograma que mostra um exemplo ilustrativo de um processo de verificação de assinatura, de acordo com pelo menos uma modalidade;

[012] A Figura 9 é um diagrama que ilustra uma forma exemplar de distribuição de chaves, de acordo com pelo menos uma modalidade;

[013] A Figura 10 é um diagrama que ilustra uma forma exemplar de distribuição de chaves de uma maneira que fornece diferentes escopos de autoridade de acordo com pelo menos uma modalidade;

[014] A Figura 11 é um fluxograma que mostra um exemplo ilustrativo de um processo de derivação de chave de acordo com pelo menos uma modalidade;

[015] A Figura 12 é um diagrama que ilustra várias derivações de chave de múltiplas restrições, de acordo com pelo menos uma modalidade;

[016] A Figura 13 é um exemplo ilustrativo de uma função para derivar uma assinatura, de acordo com pelo menos uma modalidade;

[017] A Figura 14 é um exemplo ilustrativo de como múltiplas derivações de chave podem ser realizadas e utilizadas de acordo com pelo menos uma modalidade;

[018] A Figura 15 é um diagrama que ilustra um exemplo da forma com que as chaves podem ser derivadas, de acordo com pelo menos uma modalidade;

[019] A Figura 16 é um diagrama que ilustra outro exemplo da forma com que chaves podem ser derivadas, de acordo com pelo menos uma modalidade;

[020] A Figura 17 é um diagrama que ilustra outro exemplo da forma com que as chaves podem ser derivadas, de acordo com pelo menos uma modalidade;

[021] A Figura 18 é um fluxograma que mostra um exemplo ilustrativo de um processo para iniciar uma sessão, de acordo com pelo menos uma modalidade;

[022] A Figura 19 é um fluxograma que mostra um exemplo ilustrativo de um processo para gerar uma chave de sessão, de acordo com pelo menos uma modalidade.

[023] A Figura 20 é um fluxograma que mostra um exemplo ilustrativo de um processo para obtenção de acesso a um ou mais recursos de computação durante

uma sessão de acordo com pelo menos uma modalidade;

[024] A Figura 21 é um fluxograma que mostra um exemplo ilustrativo de um processo para determinar se concede o acesso solicitado a um ou mais recursos de computação, de acordo com pelo menos uma modalidade;

[025] A Figura 22 é um fluxograma que mostra um exemplo ilustrativo de um processo de delegação de autoridade de acordo com pelo menos uma modalidade;

[026] A Figura 23 é um diagrama que representa um exemplo ilustrativo de várias delegações de autoridade de acordo com pelo menos uma modalidade; e

[027] A Figura 24 é um diagrama que representa um exemplo ilustrativo de uma forma com que as chaves podem ser derivadas utilizando as chaves de várias autoridades.

DESCRIÇÃO DETALHADA

[028] Na descrição que se segue, as várias modalidades serão descritas. Para fins de explicação, configurações e detalhes específicos são apresentados a fim de proporcionar uma compreensão completa das modalidades. No entanto, também será evidente para um especialista na técnica que as modalidades podem ser praticadas sem os detalhes específicos. Além disso, as características bem conhecidas podem ser omitidas ou simplificadas, de modo a não obscurecer a modalidade a ser descrita.

[029] As técnicas aqui descritas e sugeridas incluem sistemas e métodos para gerar chave, de acordo com várias modalidades. As chaves podem ser usadas para diversos fins, como autenticação e participação em esquemas de assinatura da mensagem. Em uma modalidade, um provedor de recursos de computação fornece serviços de computação para clientes com base pelo menos em parte em pedidos eletrônicos recebidos de dispositivos de usuários dos serviços. Os serviços podem ser qualquer serviço adequado que pode ser oferecido, incluindo, entre outros, acesso a dados, acesso aos recursos de computação para realizar operações,

acesso a serviços de armazenamento de dados, e semelhantes.

[030] Para garantir que os serviços são prestados de maneira segura, várias modalidades da presente divulgação utilizam técnicas para autenticar solicitações (também conhecido como “mensagens”) para garantir que os pedidos são legítimos. Em uma modalidade, os pedidos são autenticados usando um algoritmo Código de Autenticação de Mensagem Hash (HMAC) ou outro algoritmo apropriado, como discutido em mais detalhe abaixo.

[031] Em uma modalidade, tanto a parte de autenticação (por exemplo, o usuário dos serviços ou parte agindo em nome do usuário) e o autenticador (por exemplo, provedor de serviços ou pessoa agindo em nome do prestador) compartilham uma credencial secreta, que pode ser referida como uma chave. Um autenticador pode armazenar credenciais secretas compartilhadas para vários usuários. Como parte de uma transação, a parte de autenticação pode assinar pedidos usando a credencial secreta compartilhada formando assim uma assinatura. A assinatura pode ser fornecida para o autenticador com as solicitações. O autenticador pode usar sua própria cópia da credencial secreta compartilhada para gerar uma assinatura para as solicitações recebidas e, por comparação, se a assinatura gerada corresponde à assinatura recebida (por exemplo, por ser idêntica à assinatura recebida), determinar se as solicitações foram assinadas usando a credencial secreta compartilhada. Se determinado que as solicitações foram assinadas utilizando a credencial secreta compartilhada, as solicitações podem ser consideradas autênticas e, por conseguinte, pode determinar-se que as solicitações devem ser cumpridas.

[032] Uma vez que a interação acima é simétrica (isto é, ambos utilizam informação comum no desempenho das suas funções), as credenciais secretas compartilhadas que um autenticador mantém podem ser usadas tanto para autenticar as partes de autenticação quanto para agir em seus nomes. Como resultado, um elevado grau de segurança é desejável para proteger estas credenciais. A manutenção

de elevados graus de segurança pode ter desempenho negativo e consequências de disponibilidade. Por exemplo, manter um elevado grau de segurança pode incluir a manutenção de um sistema centralizado de armazenamento de chave. Tais sistemas centralizados, no entanto, podem causar um gargalo de escalonamento uma vez que a adição de usuários e/ou serviços causa uma carga maior ao sistema centralizado. Se um sistema centralizado falhar, pode ser difícil ou impossível de autenticar as solicitações. Assim, a centralização oferece vantagens para a segurança e desvantagens para o escalonamento e disponibilidade dos serviços.

[033] Em uma modalidade, os impactos negativos de tais sistemas (e outros sistemas) são reduzidos pela utilização de um protocolo de assinatura que deriva de artefatos de credenciais secretas partilhadas que podem ser usadas para provar que uma parte de autenticação tem uma credencial secreta compartilhada e, portanto, é provável autorizada para obter acesso especificado em solicitações assinadas com os artefatos. Em uma modalidade, tais artefatos são obtidos por meio da configuração de sistemas de computação autenticadores para aceitar como uma assinatura um valor que é com base pelo menos em parte em uma derivação de uma credencial compartilhada, em vez de a própria credencial partilhada. A derivação da credencial partilhada pode ser de tal modo que, como descrito mais completamente a seguir, o método não permite uma determinação concreta da credencial compartilhada.

[034] Por exemplo, em uma modalidade, as partes de autenticação são capazes de assinar com assinaturas com

HMAC (M, HMAC(X, credencial)),

em que M é uma mensagem, e HMAC(X, credencial) é um artefato derivado de uma credencial secreta compartilhada. O valor de X pode ser algum valor que é conhecido por ambas a parte de autenticação e o autenticador, e podem estar disponíveis ao público. Por exemplo, X pode ser uma data atual, codificada de uma maneira predeterminada para garantir que HMAC(X, credencial) é calculado consis-

tentemente pela parte de autenticação e o autenticador. Como outro exemplo, X pode ser um identificador de um serviço com o qual o artefato é utilizável. Como mais um exemplo, X pode codificar vários significados semânticos e ser fornecido de forma tal que ambas a parte de autenticação e o autenticador consistentemente calculam o artefato. O significado semântico pode ser uma limitação para a utilização da chave, incluindo o significado que indica que não há outras formas de derivações que a chave deve ser usada. Combinando exemplos anteriores do presente parágrafo, X pode ser codificado como “20110825/DDS” onde a cadeia à esquerda da barra representa uma data e a cadeia à direita da barra representa o nome de um serviço com o qual um artefato calculado com X é utilizável. Geralmente, X pode ser qualquer valor ou um conjunto de valores codificados de forma consistente, tanto para a parte de autenticação quanto para o autenticador. Deve-se notar que outras funções, exceto funções HMAC adequadas podem ser usadas, como discutido abaixo.

[035] Voltando ao exemplo utilizando HMACs, em uma modalidade, os valores para X são escolhidos para proporcionar vantagens adicionais. Como notado, X pode (mas não necessariamente) corresponder a um ou mais significados semânticos. Significados semânticos tais como selos de tempo, nome de serviço, nomes regionais, e semelhantes são utilizados, em uma modalidade, para proporcionar um sistema onde artefatos criados de acordo com técnicas da presente divulgação fornecem correspondentes restrições na utilização de chaves derivadas X. Desta forma, apesar de comprometimento de chaves geradas poder permitir a autenticação por partes indesejadas, restrições utilizadas para codificar chaves permitem que os efeitos adversos sejam minimizados quando as chaves estão comprometidas. Como exemplo, restrições de tempo utilizadas para obter as chaves fornecem uma maneira eficiente para um sistema verificar se uma assinatura apresentada foi assinada com uma chave que era válida no momento da apresentação da assinatura. Como um exemplo concreto, se a data atual é usada para derivar uma chave e um sistema

autenticador só aceitar assinaturas apresentadas na data atual, o sistema autenticador irá determinar que as assinaturas geradas usando chaves derivadas com datas diferentes são inválidas. Da mesma forma, uma chave derivada com um identificador de um determinado serviço seria inválida para uso com outro serviço. Outros exemplos são fornecidos abaixo.

[036] Como notado, várias técnicas da presente divulgação permitem vários parâmetros a serem usados para derivar chaves. Em uma modalidade, as chaves são derivadas a partir de vários parâmetros através da utilização de uma função múltipla HMAC. Por exemplo, uma chave pode ser calculada como se segue:

K_S= HMAC (... HMAC(HMAC(HMAC(K, P_1), P_2), P_3)..., P_N),

onde K é uma credencial secreta compartilhada e o P_i são parâmetros. A chave, K_S, pode ser utilizada para gerar uma assinatura, como:

S = HMAC (K_S, M),

em que M é uma mensagem, que pode ser canônica. Deste modo, a chave é derivada de uma maneira em camadas, permitindo derivações parciais da chave a serem passadas para vários componentes de um sistema de distribuição. Por exemplo, K_{P1}=HMAC(K, P_1) pode ser calculada e transmitida para um ou mais componentes de um sistema de distribuição. Os componentes que recebem K_{P1} podem calcular K_{P2} = HMAC (K_{P1}, P_2), onde P_2 pode ser o mesmo para cada componente ou diferente para alguns ou todos os componentes. Os valores de K_{P2} calculados pelos vários componentes podem passar os cálculos para outros componentes dos sistemas de distribuição, que podem calcular o K_{P3}= HMAC (K_{P2}, P_3). Cada componente pode armazenar em cache os resultados que calculam e possíveis resultados computados e calculados por outros componentes. Desta forma, mais segurança pode ser fornecida em torno de um armazenamento de dados que armazena chaves secretas compartilhadas porque cálculos de chaves derivadas podem ser realizados por outros componentes do sistema de distribuição.

[037] Técnicas da presente divulgação também preveem o início das sessões. Por exemplo, como discutido, uma credencial secreta compartilhada e um ou mais parâmetros podem ser utilizados para derivar uma chave. Deste modo, os parâmetros para uma sessão podem ser usados para gerar uma credencial que pode ser utilizada durante a sessão. A credencial pode ser utilizada pelo usuário que solicitou ou, em algumas modalidades, por um usuário a quem a credencial foi passada e ao qual o acesso a um ou mais recursos de computação foi delegado. Em tais casos, porque um dito delegado de acesso utiliza uma chave derivada a partir de uma credencial secreta compartilhada, mas não a própria credencial secreta compartilhada, um nível mais alto de segurança é mantido e não há necessidade de rodar a credencial secreta compartilhada para evitar o uso futuro pelo delegado. Como discutido em mais detalhes abaixo, delegados podem também tornar-se delegantes utilizando técnicas da presente divulgação, muitas das quais estão descritas em mais detalhes abaixo.

[038] A Figura 1 ilustra aspectos de um ambiente de exemplo 100 para implementar aspectos da presente divulgação, de acordo com várias modalidades. Como será apreciado, embora em um ambiente com base na Web seja usado para fins de explanação, podem ser utilizados ambientes diferentes, como apropriado, para implementar várias modalidades. O ambiente inclui um dispositivo eletrônico do cliente 102, que pode incluir qualquer dispositivo adequado operável para enviar e receber solicitações, mensagens ou informações através de uma rede apropriada 104 e transmitir a informação de volta para um usuário do dispositivo. Exemplos de tais dispositivos clientes incluem computadores pessoais, telefones celulares, dispositivos de mensagens portáteis, computadores portáteis, set-top boxes, assistentes de dados pessoais, leitores de livros eletrônicos, e semelhantes. A rede pode incluir qualquer rede apropriada, incluindo uma intranet, a Internet, uma rede celular, uma rede de área local, ou qualquer outro tipo de rede ou uma combinação destas. Os

componentes utilizados para dito um sistema pode depender pelo menos em parte do tipo de rede e/ou do ambiente selecionado. Protocolos e componentes para comunicar através de uma rede deste tipo são bem conhecidos e não serão aqui discutidos em detalhe. Comunicação sobre a rede pode ser ativada por meio de conexões com ou sem fio, e combinações das mesmas. Neste exemplo, a rede inclui a Internet, como o ambiente inclui um servidor Web 106 para receber as solicitações e servir o conteúdo em resposta a isso, embora para outras redes um dispositivo alternativo que serve a um propósito semelhante poderia ser usado como seria aparente para um especialista na técnica.

[039] O ambiente ilustrativo inclui pelo menos um servidor de aplicativo 108 e um armazenamento de dados 110. Deve entender-se que pode haver vários servidores de aplicativos, camadas, ou outros elementos, processos, ou componentes, que podem ser conectados ou configurados de outra forma, que podem interagir para realizar tarefas, como a obtenção de dados a partir de um armazenamento de dados apropriado. Como aqui utilizado, o termo “armazenamento de dados” refere-se a qualquer dispositivo ou combinação de dispositivos com capacidade de armazenar, acessar e recuperar dados, que podem incluir qualquer combinação e número de servidores de dados, bases de dados, dispositivos de armazenamento de dados, e meios de armazenamento de dados, em qualquer ambiente padrão, distribuído ou agrupado. O servidor de aplicativos pode incluir qualquer hardware e software adequado para integrar com o armazenamento de dados, conforme necessário, para executar os aspectos de um ou mais aplicativos para o dispositivo cliente, manipulando uma maioria do acesso aos dados e à lógica de negócios para um aplicativo. O servidor de aplicativos fornece serviços de controle de acesso em cooperação com o armazenamento de dados, e é capaz de gerar conteúdo, como texto, gráficos, áudio e/ou vídeo para ser transferidos ao usuário, que pode ser servido ao usuário pelo servidor Web na forma de HTML, XML, ou outra linguagem estruturada apropri-

ado neste exemplo. O manuseio de todas as solicitações e respostas, bem como a entrega de conteúdo entre o dispositivo cliente 102 e o servidor de aplicativos 108, pode ser manipulado pelo servidor Web. Deve ser entendido que os servidores Web e de aplicativos não são necessários e são apenas exemplos de componentes, uma vez que o código estruturado discutido aqui pode ser executado em qualquer dispositivo apropriado ou máquina hospedeira como discutido neste documento.

[040] O armazenamento de dados 110 pode incluir várias tabelas separadas de dados, bases de dados, ou outros mecanismos de armazenamento de dados e meios para armazenar dados relativos a um aspecto particular. Por exemplo, o armazenamento de dados ilustrado inclui mecanismos para armazenar os dados de produção 112 e informação do usuário 116, que podem ser usados para servir o conteúdo para o lado da produção. O armazenamento de dados também é mostrado para incluir um mecanismo para armazenar dados de registro 114, o qual pode ser usado para gerar relatórios, análise, ou outros tais fins. Deve entender-se que pode haver vários outros aspectos que podem requere que sejam armazenados no armazenamento de dados, como para a informação de imagem principal e acessar a informação para a direita, que pode ser armazenada em qualquer um dos mecanismos acima mencionados, conforme apropriado, ou em mecanismos adicionais no armazenamento de dados 110. O armazenamento de dados 110 é operável, através da lógica que está associada a este, para receber instruções do servidor de aplicativo 108 e obter, atualizar ou de outra forma processar os dados em resposta ao mesmo. Em um exemplo, um usuário pode enviar uma solicitação de busca para um determinado tipo de item. Neste caso, o armazenamento de dados pode acessar as informações do usuário para verificar a identidade do usuário, e pode acessar as informações detalhadas no catálogo para obter informações sobre os itens desse tipo. A informação pode então ser devolvida ao usuário, como em uma lista de resultados em uma página da Web que o usuário é capaz de ver através de um navega-

dor no dispositivo do usuário 102. As informações para um determinado item de interesse podem ser visualizadas em uma página dedicada ou janela do navegador.

[041] Cada servidor normalmente inclui um sistema operacional que fornece instruções de programas executáveis para a administração geral e funcionamento desse servidor, e normalmente inclui um meio de armazenamento legível por computador (por exemplo, um disco rígido, memória de acesso aleatório, memória apenas para leitura, etc.) armazenando instruções que, quando executadas por um processador do servidor, permitem que o servidor execute suas funções pretendidas. Implementações adequadas para o sistema operacional e funcionalidade geral dos servidores são conhecidas ou estão disponíveis comercialmente, e são facilmente implementadas por pessoas com conhecimentos correntes na técnica, particularmente à luz da presente divulgação.

[042] O ambiente em uma modalidade é um ambiente de computação distribuída, utilizando vários sistemas de computador e componentes que estão interligados por meio de ligações de comunicação, utilizando uma ou mais redes de computadores ou ligações diretas. No entanto, será apreciado por especialistas na técnica que dito um sistema poderia funcionar igualmente bem em um sistema que tem menos ou mais componentes que estão ilustrados na Figura 1. Assim, a descrição do sistema 100 na Figura 1 deve ser considerada como sendo de natureza ilustrativa, e não limitando o escopo da revelação.

[043] A Figura 2 mostra um exemplo ilustrativo de um ambiente 200 que inclui um fornecedor de recursos de computação 202 que controla várias zonas de falha 204, de acordo com pelo menos uma modalidade. Um fornecedor de recursos de computação, em uma modalidade, é uma organização que opera hardware de computador em nome de um ou mais clientes 206. O provedor de recursos de computação pode fornecer recursos de computação de várias maneiras. Por exemplo, em uma modalidade, o fornecedor de recursos de computação 202 gera o hardware

que está configurado para ser utilizado por clientes 206. O provedor de recursos de computação 202 fornece uma interface que permite que os clientes 206 configurem recursos de computação por meio de programação usando o hardware. Por exemplo, o fornecedor de recursos de computação pode manter servidores de hardware que executam sistemas de computação virtuais que são controlados por meio de programação pelo cliente. Como outro exemplo, o provedor de recursos de computação 202 pode gerenciar vários armazenamentos de dados para fornecer soluções de armazenamento de dados remotos, como o armazenamento de dados de alta durabilidade e armazenamento de dados em nível de bloco.

[044] Uma zona de falha, em uma modalidade, é um conjunto de recursos de computação que são separados por um ou mais limites de falha de modo que cada zona de falha é tolerante a uma falha de outra zona de falha. Como um exemplo, cada zona de falha 204 pode ser um centro de dados separado. Assim, se um centro de dados deixa de ser operacional, talvez devido a uma queda de energia ou outro evento perturbador, outros centros de dados podem continuar a funcionar. As zonas de falhas podem ser, cada uma localizada em diferentes localizações geográficas e algumas ou todas as zonas de falhas podem ser separados por fronteiras geopolíticas. Por exemplo, duas ou mais das zonas de falhas podem ser em diferentes países. Deve-se notar que, para o propósito de ilustração, a presente divulgação fornece numerosos exemplos em que zonas de falhas são centros de dados. No entanto, as zonas de falha podem ser definidas de várias outras maneiras. Por exemplo, salas separadas no mesmo centro de dados podem ser consideradas zonas de falhas separadas de acordo com várias modalidades. Como outro exemplo, recursos de computação no mesmo local, mas suportados por diferentes geradores de energia de backup e/ou suportados por diferentes recursos de rede, podem ser considerados diferentes zonas de falhas. Como ainda outro exemplo, os centros de dados podem ser agrupados de modo que cada conjunto de centros de dados pode ser

considerado uma zona de falha. Além disso, pode haver muitas razões pelas quais uma zona de falha pode falhar, incluindo razões relacionadas com o funcionamento da rede de energia, operação de rede pública, afirmações políticas de poder, e outras razões.

[045] Em uma modalidade, os clientes 206 se comunicam com o fornecedor de recursos de computação 202 através de uma rede 208, como a Internet. Os clientes 206 podem ter recursos configurados em uma ou mais das zonas de falha 204 e podem se comunicar com os recursos através do envio de mensagens eletrônicas, como mensagens invocando uma interface de programação de aplicativo de serviço da web (API) do provedor de recursos de computação, a fim de configurar e operar os recursos. Os clientes podem utilizar os recursos em várias zonas de falhas, a fim de diminuir os efeitos de possíveis falhas que afetam os recursos dos clientes. Um cliente que utiliza os recursos do provedor de recursos de computação 202 para operar um site acessível ao público pode, por exemplo, manter a web e outros servidores em zonas de falhas separadas, de modo que, se os servidores em uma zona de falha falharem, o público pode ainda acessar o site acessando servidores em outra zona de falha.

[046] A Figura 3 mostra um exemplo ilustrativo de um ambiente 300 dentro de uma zona de falha 302, que pode ser uma zona de falha de um fornecedor de recursos de computação, como ilustrado na Figura 2. A zona de falha 302, em uma modalidade, inclui recursos de computação que são usados para fornecer vários serviços em nome de clientes. Por exemplo, como ilustrado na Figura 3, a zona de falha 302 inclui os recursos de computação que são utilizados para fornecer um serviço de armazenamento de dados durável que pode armazenar, de modo mais barato e redundante, quantidades relativamente grandes de dados, em nome dos clientes. Esse serviço pode ser utilizado quando grandes quantidades de armazenamento e/ou segurança do armazenamento de dados de dados é necessária, mas quando

o desempenho de entrada/saída não é alta prioridade. A zona de falha 302 pode também incluir um serviço de armazenamento de dados em bloco 306, que proporciona a utilização de dispositivos de armazenamento em nível de bloco, dispositivos físicos e/ou virtuais, para os clientes. Os clientes podem, por exemplo, conectar dispositivos de armazenamento em nível de bloco para sistemas de computadores também utilizados pelos clientes. Também é ilustrado um serviço de sistema de computador virtual 308 que pode prestar serviços de computação para os clientes. Em uma modalidade, o serviço de sistema de computador virtual 308 fornece serviços de computação através da implementação de sistemas de computadores virtuais para os clientes em servidores físicos mantidos pelo provedor de recursos de computação, embora as variações sejam possíveis, tais como onde sistemas de computadores físicos são alocados para clientes para uso do cliente. Em uma modalidade relacionada aos sistemas de computadores virtuais, os clientes podem gerenciar programaticamente os sistemas de computadores virtuais de acordo com suas necessidades. Por exemplo, como ilustrado na Figura 3, os clientes podem configurar sistemas computacionais virtuais do serviço do sistema de computador virtual 308 para servir os clientes dos clientes do fornecedor de serviços de computação virtual. Os sistemas de computadores virtuais podem ser, por exemplo, configurados para operar um site acessível ao público. Ambos os clientes do provedor de recursos de computação virtual e os clientes dos clientes podem, em várias modalidades, acessar vários serviços operados na zona de falha 302, comunicando com os serviços através de uma rede 310, que pode ser a rede 208 descrita acima em conexão com a Figura 2.

[047] Deve-se notar que as diversas modalidades ilustradas na Figura 3, como acontece com todas as modalidades ilustrativas mostradas nas Figuras e aqui descritas, são de natureza ilustrativa e que as variações são consideradas como estando dentro do escopo da presente divulgação. Por exemplo, outros serviços dife-

rentes dos ilustrados podem ser fornecidos na zona de falha 302 além de ou em vez dos serviços ilustrados. Como ilustrado pelas elipses na Figura 3, por exemplo, serviços adicionais podem ser operados na zona de falha 302. Além disso, alguns dispositivos podem utilizar outros serviços. Por exemplo, vários serviços (como um serviço de armazenamento de dados em nível de bloco 306 e um serviço de sistema de computador virtual 308) podem ser utilizados em conjunto para oferecer outros serviços, como um serviço de banco de dados relacional, um serviço de correio eletrônico, e, em geral, qualquer tipo de serviço de computação que pode ser fornecido usando recursos de um provedor de recursos de computação.

[048] Como ilustrado na Figura 3, cada um dos serviços do provedor de recursos de computação pode incluir um verificador separado 312. O verificador pode ser um dispositivo de computação, coleção de dispositivos de computação, módulo de aplicação, ou outro recurso que verifica vários atestados feitos por clientes e, possivelmente, por outros sistemas de computador. Em uma modalidade, cada um dos verificadores 312 verifica as assinaturas de mensagens que são produzidas de acordo com as várias modalidades aqui descritas e, em seguida, fornecidas pelos clientes em ligação com as solicitações de acesso aos recursos de computação, como descrito em mais detalhes abaixo. Chaves e outras informações relevantes podem ser propagadas para os verificadores de uma autoridade de chave central para permitir que os verificadores verifiquem as informações. Deve-se notar que cada serviço tendo um verificador é um exemplo ilustrativo de uma modalidade particular, mas que outros arranjos estão dentro do escopo da presente divulgação. Por exemplo, um único verificador pode suportar vários serviços, inclusive todos os serviços e pode até suportar múltiplas zonas de falhas.

[049] A Figura 4 mostra um exemplo ilustrativo de uma configuração de recursos de computação que pode ser usada para suportar um ambiente como o ambiente mostrado na Figura 3, de acordo com pelo menos uma modalidade. A Figura

4 mostra especialmente um exemplo específico, onde a zona de falha na Figura 3 é um centro de dados. Deste modo, voltando à figura 4, um centro de dados 402 pode incluir vários racks 404-406. O centro de dados 402 é um exemplo de um ou mais centros de dados que podem ser utilizados em várias modalidades da presente divulgação, como centros de dados mostrados na Figura 4. A elipse entre o rack de servidor 404 e o rack de servidor 406 indica que o centro de dados 402 pode incluir qualquer número apropriado de racks de servidor, embora, por motivos de clareza, apenas dois sejam mostrados na Figura 4. Cada rack de servidor 404-406 pode participar na manutenção de serviços como energia elétrica e comunicações de dados para vários computadores servidores 408-414 e 416-422. Mais uma vez, as elipses indicam que os racks de servidor 404-406 podem incluir qualquer número adequado de computadores servidores. Por exemplo, os computadores de servidor 408-422 podem incluir um ou mais servidores virtuais do sistema de computador (VCS) e/ou um ou mais servidores de armazenamento de dados. Cada servidor 408-422 pode corresponder a uma implementação da unidade dedicação de recursos.

[050] Na Figura 4, cada rack de servidor 404-406 é descrito como incluindo um switch de rack 424-426. Os switches de rack 424 e 426 podem ser responsáveis por pacotes de comutação de dados digitais e aos seus respectivos conjuntos de computadores de servidor 408-414 e 416-422. Os racks switches 424-426 podem ser comunicativamente ligados a um centro de dados de matriz de comutação 428 e, em seguida, a um conjunto de roteadores de borda 430 que liga o centro de dados 402 a uma ou mais outras redes de computadores, incluindo a Internet. A matriz de comutação pode incluir qualquer conjunto adequado de componentes de rede incluindo vários switches interconectados 432-438 (para maior clareza, apenas quatro são mostrados na Figura 4) de um ou mais tipos de switch dispostos em uma ou mais camadas de comutação, bem como roteadores, gateways, pontes, hubs, repetidores, firewalls, computadores, e combinações adequadas dos mesmos. Em pelo

menos uma modalidade, os switches de rack 424-426 e os roteadores de borda 430 são considerados como parte da matriz de comutação 428. Os racks switches 424-426, os roteadores de borda 430, e os componentes da matriz de comutação 428 são exemplos de equipamento de rede 224 da Figura 2.

[051] Como notado acima, várias modalidades da presente divulgação permitem os vários níveis de autoridade a serem concedidos por razões diferentes. A Figura 5 é um diagrama que ilustra uma forma exemplar de uma maneira em que os vários elementos que participam em um ambiente de computação podem ser alocados diferentes escopos de autoridade de acordo com pelo menos uma modalidade. Na Figura 5, um fornecedor de recursos de computação 502 é ilustrado. Em uma modalidade, o provedor de recursos de computação 502 tem autoridade sobre seus recursos e, como ilustrado na Figura 5, é capaz de repartir essa autoridade entre os vários participantes no uso dos recursos. Deve-se notar que, para o propósito de ilustração consistente com outras ilustrações e descrições das mesmas, a Figura 5 mostra um provedor de recursos de computação 502 tendo autoridade sobre um domínio. No entanto, a realização da presente divulgação também é aplicável a outros másters de domínios de autoridade. Por exemplo, um máster da autoridade pode ser um governo ou uma organização governamental, uma suborganização de outra organização ou, em geral, qualquer entidade com autoridade sobre algum domínio.

[052] Voltando ao exemplo ilustrativo da Figura 5, o provedor de recursos de computação 502 gerencia sua autoridade, permitindo que diferentes subentidades tenham autoridade sobre diferentes subdomínios. Por exemplo, como mostrado na Figura, cada um de um número de zonas de falhas 504 do provedor de recursos de computação fornece um correspondente subdomínio do domínio 502 do provedor de recursos de computação. Assim, cada zona de falha pode ter autoridade sobre os seus próprios recursos, mas não os recursos de outra zona de falha (embora, em

alguns casos, a autoridade sobre alguns subdomínios pode ser compartilhada). Assim, de acordo com uma modalidade, uma zona de falha pode fornecer acesso dos usuários aos recursos de computação na zona de falha, mas não o acesso aos recursos de computação de outra zona de falha.

[053] Como mencionado acima, cada zona de falha pode incluir um ou mais serviços 506. Por conseguinte, como ilustrado na Figura 5, cada serviço pode ser responsável por um subdomínio do domínio da zona de falha correspondente 504. Assim, um serviço, em uma modalidade, pode proporcionar o acesso aos recursos acessíveis pelo serviço, mas não a outros serviços. Cada serviço pode servir um ou mais clientes 508 e, por conseguinte, cada cliente pode ser responsável por um subdomínio de autoridade de um serviço correspondente 506. Assim, em uma modalidade, um cliente pode fornecer acesso aos seus recursos próprios envolvidos com um serviço correspondente, mas não o serviço de outro cliente. Como um exemplo ilustrativo de concreto, se o serviço é um serviço de recursos de computação virtual, um cliente pode fornecer acesso (como o acesso público) aos seus próprios sistemas de computadores virtuais, mas não, sem permissão, aos sistemas de computadores virtuais de outros clientes.

[054] Como notado, a alocação particular de autoridade conforme ilustrado na Figura 5 é para o propósito de ilustração e numerosas variações são consideradas como estando dentro do escopo da presente divulgação. Como notado, as modalidades da presente divulgação são aplicáveis aos domínios de autoridade fora dos domínios gerenciados por provedores de recursos de computação e subdomínios podem ser determinados de acordo com as necessidades e circunstâncias particulares. Além disso, a Figura 5 mostra os clientes de um provedor de recurso virtual contendo os menores subdomínios de autoridade. No entanto, as técnicas da presente divulgação podem permitir que os domínios do cliente sejam divididos em um ou mais subdomínios.

[055] Diversas modalidades da presente descrição referem-se à assinatura de mensagens. A Figura 6 é um diagrama 600 que ilustra um modo exemplar no qual a informação pode ser comunicada entre os participantes em um processo de verificação de assinatura da mensagem de acordo com pelo menos uma modalidade. Em uma modalidade, uma importante chave 602 fornece uma chave para ambos o requerente da mensagem 604 e um verificador de assinatura 606. A fonte de chave pode ser um sistema de computador configurado para fornecer chaves a pelo menos um requerente da mensagem 604 e o verificador de assinatura 606. A fonte chave também pode gerar as chaves utilizando várias técnicas, incluindo as várias modalidades aqui descritas ou pode obter chaves geradas a partir de outra fonte. O requerente de mensagem 604 poderá ser um sistema de computador configurado para enviar uma mensagem e uma assinatura ao verificador de assinatura 606 ou outro componente que funciona em ligação com o verificador de assinatura 606. O sistema de computador do requerente da mensagem 604 pode ser um sistema de computador de um cliente de um provedor de recursos de computação, por exemplo. O verificador de assinaturas 606 pode ser um sistema de computador configurado para receber mensagens e assinaturas e analisar a assinatura para verificar que a mensagem é autêntica, como discutido abaixo. Resumidamente, o verificador de assinatura 606 pode analisar uma assinatura e mensagem recebidas para determinar se a assinatura foi gerada utilizando a chave correta K. Deve-se notar que, enquanto a Figura 6 mostra uma fonte chave 602 separada do requerente de mensagem 604 e verificador de assinatura 606, o requerente da mensagem ou verificador de assinatura também pode ser uma fonte chave. Por exemplo, os clientes de um provedor de recursos de computação podem fornecer suas próprias chaves. Chaves de cliente podem, então, ser fornecidas ao verificador de assinatura para a verificação das assinaturas. Além disso, o requerente da mensagem 604 e verificador de assinatura 606 pode receber cada chave diferente da fonte de chave 602. Por

exemplo, o emissor de mensagem 604 poderá receber uma chave de verificador de assinatura 606 pode receber uma chave de que é derivada, utilizando as diversas modalidades da presente divulgação, a partir da chave recebida pelo requerente da mensagem 604.

[056] Como ilustrado na Figura 6, o verificador de assinatura 606 recebe mensagens e assinaturas correspondentes do requerente da mensagem 604. As mensagens podem ser, por exemplo, solicitações eletrônicas de acesso a um serviço de computação 608. As mensagens podem, por exemplo, codificar chamadas API para um serviço web. Se análise da assinatura e mensagem indica que as mensagens são autênticas, então o verificador de assinatura notifica o serviço (ou um componente de controle de acesso ao serviço) que o requerente da mensagem pode ter o acesso solicitado. Por exemplo, o verificador de assinatura pode passar a mensagem recebida ao serviço para habilitar o serviço para atender a solicitação. Deste modo, o serviço pode ser um sistema de computador que pode funcionar para satisfazer solicitações, como, por exemplo, os vários serviços descritos acima. Deve-se notar que, enquanto várias descrições de vários componentes da Figura 6 e de outros componentes descrevem os componentes como, eventualmente, são implementadas como sistemas de computador configurados para realizar certas ações, os componentes podem também compreender vários dispositivos de computação, como redes de dispositivos de computação, que são configurados em conjunto para executar as ações.

[057] A Figura 7 é um fluxograma que mostra um exemplo ilustrativo de um processo 700 para a assinatura de mensagens, de acordo com uma modalidade. Alguns ou todos do processo 700 (ou quaisquer outros processos aqui descritos, ou variantes e/ou combinações dos mesmos) podem ser realizados sob o controle de um ou mais sistemas de computadores configurados com instruções executáveis e podem ser implementados como código (por exemplo, instruções executáveis, um

ou mais programas de computador, ou um ou mais aplicativos) executando coletivamente em um ou mais processadores, por hardware, ou combinações dos mesmos. O código pode ser armazenado em um meio de armazenamento lido por computador, por exemplo, sob a forma de um programa de computador que compreende uma pluralidade de instruções executáveis por um ou mais processadores. O meio de armazenamento lido por computador pode ser não transitório.

[058] Em uma modalidade, o processo 700 inclui obter 701 uma chave K. A chave pode ser obtida de qualquer forma adequada. Por exemplo, a chave pode ser gerada por um sistema de computador que executa o processo 700. A chave pode ser recebida eletronicamente por um sistema de computador executando o processo 700. Geralmente, obter a chave pode ser realizada de qualquer maneira adequada. A chave pode ser qualquer chave apropriada para um algoritmo de assinatura particular sendo utilizado. Por exemplo, se um esquema código de autenticação de mensagem à base de hash (HMAC) está sendo usado com uma função hash criptográfica (SHA)-256 de algoritmo hash seguro, a chave pode ser uma sequência de bytes, como uma sequência de 64 ou menos bytes. Diferentes funções criptográficas de hash, como SHA-224, SHA-384 e SHA-512 também podem ser usadas.

[059] Em uma modalidade, o processo inclui também canonicalização de uma mensagem M, para formar uma mensagem canonicalizado M_c. Canonicalizar uma mensagem pode incluir organizar informações na mensagem em um formato que permite que um verificador verifique se a assinatura da mensagem é válida. Geralmente, muitos protocolos de comunicação de informações transformam os bits que compreendem uma mensagem, deixando a mensagem semanticamente idêntica. Como resultado, duas mensagens semanticamente idênticas podem compreender diferentes grupos de bits e, portanto, pode resultar em diferentes assinaturas. Assim, canonicalização permite uma maneira simples para garantir que uma assinatura pode ser verificada. Deve-se notar, no entanto, que algumas modalidades da

presente descrição não necessitam de canonicalização de mensagem. Por exemplo, se vários protocolos sendo utilizados não resultam em mensagens semanticamente idênticas compreendendo diferentes conjuntos de bits, canonicalização pode não ser necessária e pode ser omitida. Geralmente, canonicalização pode ser omitida, em qualquer caso em que a verificação da assinatura é capaz de prosseguir com sucesso sem a manipulação de uma mensagem assinada.

[060] Em uma modalidade, a assinatura é gerada por computação HMAC (K, M_c), onde HMAC() é uma função HMAC, como descrito acima. As funções HMAC têm várias propriedades que as tornam particularmente úteis para várias modalidades da presente divulgação. Por exemplo, as funções HMAC podem ser calculadas de forma eficiente por um sistema de computador, deixando desse modo os recursos computacionais disponíveis para outras tarefas. Além disso, as funções HMAC são *preimage resistant* (não inversas). Por exemplo, dada uma assinatura S=HMAC(K, M) com uma chave K e uma mensagem M, essencialmente, nenhuma informação é obtida sobre a chave K. Por exemplo, a partir de S, seria computacionalmente impossível ou pelo menos pouco prático determinar K a partir de S. As funções de HMAC são também segundas *preimage resistant*. Em outras palavras, dados S=HMAC(K, M) e M, é impossível ou pelo menos computacionalmente inviável determinar uma mensagem M' diferente de M tal que S=HMAC (K, M'). Além disso, as funções HMAC são *forgery-resistant*. Por exemplo, dado um oráculo para S=HMAC(K, M), consultando os tempos N do oráculo (N um inteiro positivo) permite a produção de pelo a maioria dos pares de assinatura de mensagem N. Em outras palavras, dado um conjunto de assinatura-pares de mensagens, é impossível ou impraticável computacionalmente determinar a chave ou determinar uma função que irá produzir uma assinatura correta para uma mensagem não6 no conjunto.

[061] Embora as funções HMAC sejam particularmente úteis para várias modalidades, outras funções podem ser usadas. Por exemplo, pode ser usada qual-

quer função com as propriedades acima de funções HMAC. Além disso, outras funções que não têm necessariamente todas (ou qualquer) as propriedades acima podem ser usadas, como nos casos em que a segurança não é uma preocupação primordial e/ou onde a segurança é uma preocupação, mas é mantida através de outros mecanismos. Deve-se notar que várias ilustrações de várias modalidades específicas mostram entradas em funções HMAC, mas que variações são possíveis. Por exemplo, as entradas para uma função HMAC (ou outras funções) podem ser diferentes. Como descrito acima, por exemplo, uma entrada é uma chave. No entanto, essa entrada pode ser derivada a partir de uma chave ou de outra forma com base pelo menos em parte em uma chave. Como um exemplo ilustrativo, a entrada pode compreender uma chave com informação, como um identificador de esquema de assinatura (talvez um identificador de versão), que é adicionado para a chave como um sufixo, prefixo, ou outro. Como outro exemplo, a entrada pode ser uma informação que é obtida através da utilização de um mapeamento da chave para a informação, que pode ser outra chave. Da mesma forma uma entrada como uma mensagem pode ser derivada a partir de uma mensagem. Como outro exemplo a variação considerada como estando dentro do escopo da presente divulgação, a assinatura pode não ser o resultado de uma função HMAC, mas um ou mais valores que são derivados a partir da saída de uma função HMAC (ou outra função adequada). Em algumas modalidades, a chave e a mensagem podem ser transmitidas na função na ordem inversa.

[062] Voltando à descrição da Figura 7, uma vez que a assinatura é gerada por computação HMAC(K,M_c), a assinatura e mensagem M são fornecidas 708 a um receptor, que pode ser um dispositivo de computação que verifica as assinaturas ou outro dispositivo de computação envolvido em um processo de verificação de assinaturas, como um dispositivo de computação proporcionando uma interface para comunicação de mensagens e assinaturas. Como acontece com todas as modalida-

des explicitamente descritas aqui, as variações são consideradas como estando dentro do escopo da presente divulgação. Por exemplo, a mensagem canonicalizada M_c pode ser fornecida ao receptor, em vez de ou em adição à mensagem M. Além disso, fornecer a mensagem M e a assinatura para o receptor pode também incluir fornecer outra informação, como um identificador de chave que pode ser usado para identificar, em um armazenamento de dados que associa chaves com identificadores de chave. Além disso, outra informação, como os parâmetros que codificam política, como discutido abaixo, pode ser fornecida com a mensagem M e assinatura.

[063] A Figura 8 é um fluxograma que mostra um exemplo ilustrativo de um processo 800 para verificação de assinatura, de acordo com pelo menos uma modalidade. O processo 800 mostrado na Figura 8 pode ser realizado por um verificador, como descrito na Figura 2. Além disso, o processo 800 pode ser realizado em resposta à recepção de uma assinatura e uma mensagem, como em resposta a outro sistema de computador tendo realizado o processo 700 da Figura 7. Em uma modalidade, o processo 800 inclui obter 802 uma chave K, como descrito acima. Obter uma chave K pode também incluir outras ações em várias modalidades. Por exemplo, se o processo 800 é usado por um sistema de computador que verifica as assinaturas geradas a partir de múltiplas chaves (como a partir de vários clientes de um provedor de recursos de computação), obter a chave K pode incluir selecionar a chave a partir de várias chaves em um armazenador de dados. O armazenamento de dados pode associar várias chaves com aqueles que apresentam assinaturas para verificação. Por exemplo, cada cliente de um provedor de recursos de computação pode ter um identificador de chave (ou vários identificadores de chave) que é usado para referenciar um armazenamento de dados e identificar uma chave apropriada. O identificador de chave pode ser submetido em conexão com a apresentação da mensagem e sua assinatura ou pode ser de outra forma determinado, como mediante a apresentação de credenciais de login. Um destinatário de um identifica-

dor de chave (por exemplo, um verificador de mensagens) pode fazer referência a um armazenamento de dados para determinar se uma chave correspondente ao identificador de chave está no armazenamento de dados e, se não, pode, então, gerar a própria chave, por exemplo, usando as técnicas aqui descritas, para derivar a chave diretamente ou indiretamente a partir de uma credencial secreta compartilhada. Para permitir isso, o destinatário pode ter acesso a um caminho de derivação de chave que, em uma modalidade, é a informação que codifica a informação necessária para derivar a chave a partir das informações que o destinatário já tem (por exemplo, uma chave derivada de uma credencial secreta compartilhada). Esta informação pode ser fornecida ao destinatário de um apresentador de uma mensagem com uma assinatura ou de outra forma pode ser disponibilizada para o destinatário. Por exemplo, o destinatário pode ser programado para gerar automaticamente as chaves usando sua região atribuída e um código para a data atual. Geralmente, qualquer método para obter a chave que foi utilizada para gerar a assinatura (ou outra chave, que pode ser utilizada para verificar a assinatura, em algumas modalidades) pode ser utilizado. O receptor também pode aplicar a política sobre os caminhos de derivação de chave admissíveis e inadmissíveis no que diz respeito ao pedido em mãos ou alguma outra propriedade conhecida para o receptor.

[064] Em uma modalidade, uma assinatura S e mensagem M são recebidas 804. A assinatura S e mensagem M podem ser recebidas por via eletrônica de um apresentador, como um dispositivo de computação que realizou o processo 700 da Figura 7. A mensagem M é então canonicalizada 806 para determinar M_c, de acordo com uma modalidade. Canonicalização da mensagem M, em várias modalidades, garante que a assinatura S pode ser verificada. Deste modo, em uma modalidade, o 800 processo inclui gerar 808 uma assinatura S' calculando HMAC(K, M_c). Em uma modalidade, S' é igual a HMAC(K, M_c), embora S' possa ser derivada a partir de HMAC(K,Mc), em várias modalidades. Para a finalidade de ilustração, a parte restan-

te do processo 800 será descrito com o pressuposto de que o S'=HMAC(K, M_c), mas que numerosas variações estão dentro do escopo da presente divulgação.

[065] Assim, em uma modalidade, é feita uma determinação 810 se S' é igual à assinatura recebida S. Em outras palavras, é feita uma determinação se a assinatura recebida é suficiente, por exemplo, porque esta é uma assinatura que foi gerada usando a chave K. Assim, em uma modalidade, se for determinado 810 que S' e S não são iguais, então a assinatura é 812 não verificada. No entanto, se o S' é igual a S, então a assinatura é 814 verificada. Dependendo se a assinatura é verificada, podem ser tomadas medidas apropriadas. Por exemplo, se a mensagem foi uma solicitação para acesso a um recurso de computação, o acesso solicitado pode ser negado (pelo menos temporariamente). Da mesma forma, se a mensagem foi uma solicitação para acesso ao recurso de computação e a assinatura foi verificada, o acesso solicitado pode ser concedido. Deve-se notar, no entanto, que a ação apropriada a ser realizada pode variar amplamente em várias modalidades, dependendo dos motivos de assinaturas serem recebidos e verificados.

[066] Como acima referido, várias modalidades da presente divulgação aplicam-se aos vários ambientes. Em muitos ambientes, é útil ter gerenciamento centralizado de vários aspectos da manutenção da segurança. A Figura 9, por exemplo, é um diagrama que ilustra um modo exemplar 900 de distribuição de chaves, de acordo com pelo menos uma modalidade. Na figura 9, uma autoridade central de chave mantém um ou mais armazenamentos de dados (coletivamente referidos como "armazenamento de dados") que contêm várias chaves utilizadas por uma organização. As chaves podem corresponder, por exemplo, aos usuários de dispositivos de computação da organização. Cada usuário de um conjunto de usuários pode, por exemplo, ser atribuída uma ou mais chaves. Em uma modalidade, pelo menos algumas chaves correspondem a clientes (e/ou os usuários dos clientes) da organização. Por exemplo, em uma modalidade, a organização é um provedor de recursos de compu-

tação e cada cliente do provedor de recursos de computação corresponde a uma ou mais chaves que permitem aos usuários dos clientes acessar recursos de computação mantidos pelo provedor de recursos de computação. Outras adaptações do processo 800 da Figura 8, de acordo com as variações descritas acima com a Figura 7 estão também dentro do escopo da presente divulgação.

[067] Como ilustrado na Figura 9, a autoridade de chave 902 propaga chaves para uma pluralidade de zonas de chave 904. Uma zona chave pode ser um domínio da organização na qual uma chave recebida é válida. Por exemplo, referindo-se a Figura 2, cada zona chave 904 pode corresponder a uma zona de falha, como um centro de dados. Zonas de chave podem ser, mas não são necessariamente, geograficamente definidas. Por exemplo, cada uma das zonas chave pode corresponder a um país, região ou outra região geográfica definida. Zonas chave também podem ser definidas de outras maneiras. Por exemplo, cada uma das zonas chave pode corresponder a um serviço fornecido por um provedor de recursos de computação, a um cliente de uma organização, e assim por diante. Embora não ilustrado, como tal, zonas chaves podem ter subzonas. Por exemplo, uma zona chave pode corresponder a um país. No interior do país pode haver várias regiões, cada uma correspondendo a subzonas da zona chave. As chaves podem ser propagadas a subzonas, em tais modalidades.

[068] Como ilustrado na Figura 9, as zonas chaves 904 podem propagar chaves a um ou mais verificadores 906 para a zona chave. Por exemplo, se uma zona chave corresponde a um centro de dados, um dispositivo de computação do centro de dados pode propagar chaves para verificadores para cada um de uma pluralidade de serviços suportados por recursos de computação no centro de dados. Desta maneira, os verificadores podem ser usados para verificar as assinaturas apresentadas em conexão com várias solicitações. Isto alivia os recursos de computação da própria autoridade chave de verificar assinaturas e ainda reduzir latência e

requisitos de largura de banda, especialmente nos casos em que a autoridade chave 902 está geograficamente distante dos serviços nos quais as solicitações são feitas.

[069] A propagação da chave pode ser feita de várias maneiras. Em uma modalidade, as chaves são distribuídas ao longo de canais seguros para vários beneficiários. Em algumas modalidades, a entidade de chave propaga as mesmas chaves para cada zona chave. Além disso, algumas chaves podem ser utilizáveis em várias zonas chave. A autoridade de chave 902 pode propagar chaves utilizáveis em várias zonas chave para essas várias zonas chave enquanto abstendo-se de propagar essas chaves para zonas chave onde as chaves não podem ser usadas. Assim, no exemplo de um provedor de recursos de computação, a autoridade de chave 902 pode propagar uma chave para um cliente somente para aquelas zonas chaves onde o cliente é capaz de usar a chave, como centros de dados usados para manter os recursos de computação do cliente.

[070] Diversas modalidades da presente divulgação também fornecem propagação chave de maneiras prevendo numerosas vantagens. A Figura 10 é um diagrama 1000 ilustrando uma forma exemplar de distribuição de chaves de uma maneira que fornece diferentes escopos de autoridade de acordo com pelo menos uma modalidade. Como na Figura 10, o diagrama 1000 inclui uma autoridade chave 1002 com uma chave K, que propaga chaves, diretamente ou indiretamente, com várias zonas chaves 1004 e verificadores 1006, como de acordo com a descrição acima, em relação à Figura 9. Embora, para finalidade de ilustração, o diagrama 1000 é descrito em ligação com uma única chave K, e as chaves derivadas de K, as modalidades aqui descritas, aplicam-se quando a autoridade chave executa essas ações de numerosas chaves.

[071] Como ilustrado na Figura 10, a chave K é usada como uma base para as outras chaves derivadas de K. Por exemplo, a partir de K, uma chave K_1 é derivada e propagada para uma primeira zona chave (Zona chave$_1$). Como tal, a chave

K_1 (ou chaves derivadas a partir da chave K_1) é utilizável na primeira zona chave, mas não em outras zonas principais que não têm K_1 (ou uma chave derivada a partir da chave K_1). Da mesma forma, cada um de um número de outras zonas chave correspondente recebem diferentes chaves derivadas a partir da chave K. Deve-se notar que, enquanto a Figura 10 mostra as chaves derivadas da chave K sendo propagadas a partir da autoridade chave 1002 para zonas principais correspondentes, as variações são possíveis. Por exemplo, a chave K pode ser propagada para as zonas chaves e cada zona chave que recebe a chave K pode usar a chave K para derivar uma ou mais chaves correspondentes. Por exemplo, a zona chave 1004 chamada "Zona chave$_1$" pode receber a chave K e derivar K_1. Geralmente, as várias tarefas envolvidas na derivação de chave e propagação podem ser realizadas de modo diferente do que ilustrado nas várias modalidades.

[072] Como mostrado no exemplo ilustrativo da Figura 10, as chaves recebidas pelas zonas principais 1004 são utilizadas para derivar chaves que são propagadas ainda mais. Por exemplo, referindo-se à zona chave 1004 chamada "Zona chave$_2$", uma chave K_2 que é derivada a partir da chave K é usada para derivar chaves adicionais K_2' e K_2''. As chaves K_2' e K_2'' são propagadas aos verificadores correspondentes 1006 para uso pelos verificadores 1006 em verificação de assinaturas. Assim, um verificador que recebe K_2' que, em uma modalidade, é capaz de verificar uma assinatura gerada utilizando K_2', enquanto que um verificador que não recebeu K_2' não seria capaz de verificar a assinatura. Ao propagar as chaves da maneira ilustrada nas Figuras 9 e 10 (ou suas variações) vantagens são alcançadas. Por exemplo, por propagação das chaves para vários verificadores em vários locais, em vez de um ou mais verificadores centralizados, menor latência é alcançada. Além disso, referindo a Figura 10, ao propagar chaves derivadas para outros dispositivos que, por sua vez, derivam chaves adicionais, é possível espalhar cálculos sobre vários dispositivos sobre diversos locais, permitindo assim, a derivação chave mais rápida

e aumentando a tolerância a falhas.

[073] Derivações de chaves podem ser realizadas de várias maneiras. A Figura 11 é um fluxograma que mostra um exemplo ilustrativo de um processo 1100 de derivação de chave, de acordo com pelo menos uma modalidade. Em uma modalidade, o processo 1100 inclui a obtenção 1002de uma chave K_i, como de um modo descrito acima. A chave K_i pode ser qualquer chave apropriada, como descrito acima. Além disso, a chave K_i pode ser, mas não é necessariamente, derivada de outra chave, como pelo desempenho do processo 1100 ou outro processo. Após a obtenção da chave K_i, uma nova chave é derivada de K_i. No exemplo ilustrativo da Figura 11, uma nova chave K K_{i+1} é calculada como (ou com base, pelo menos em parte em) HMAC(K_i, R_{i+1}), em que R_{i+1} é a informação que identifica uma ou mais restrições sobre a chave K_{i+1}. R_{i+1} pode ser, por exemplo, uma sequência de bits que codifica a informação que indica onde a chave K_{i+1} é utilizável. Por exemplo, R_{i+1} pode codificar uma zona chave onde a chave K_{i+1} pode ser usada. As restrições podem ser com bases, pelo menos em parte sobre a geografia, tempo, identidade de usuário, serviço, e assim por diante. Exemplos de restrições são fornecidos na descrição abaixo.

[074] Além disso, como discutido mais abaixo, o processo 1100 pode ser utilizado várias vezes, para derivar uma chave. Por exemplo, uma chave gerada usando o processo 1100 (ou uma variação da mesma) pode ser utilizada para gerar outra chave, utilizando a mesma ou outra restrição. Usando a terminologia na figura, R_{i+1} pode ser, por exemplo, uma sequência de bits que codifica a informação que indica onde a chave K_{i+1} poderia ser utilizada. K_{i+1} poderia se tornar a chave K_i para a próxima iteração do processo. Por exemplo, se o processo 1100 foi utilizado para gerar uma chave com base em uma restrição geográfica, a chave gerada pode ser usada para gerar uma chave com uma restrição com base em data. Dito um processo pode ser utilizado várias vezes para usar várias restrições para derivar uma chave. Como

discutido mais detalhadamente abaixo, usando várias restrições para derivar uma chave, um ou mais verificadores podem aplicar a política enquanto verificam-se as assinaturas. Como um breve exemplo ilustrativo, como parte de um processo de verificação de assinatura, um verificador pode determinar uma assinatura esperada utilizando uma restrição, como uma codificação de uma data atual. Se uma assinatura foi fornecida que foi gerada em uma data diferente, então a verificação da assinatura falharia, de acordo com uma modalidade. Geralmente, se o uso de uma assinatura não cumpre com uma restrição utilizada para obter uma chave, a verificação da assinatura pode falhar, de acordo com várias modalidades.

[075] A Figura 12 é um diagrama 1200 mostrando um exemplo ilustrativo de uma derivação de uma chave usando várias restrições, de acordo com pelo menos uma modalidade. Na Figura 12, uma chave é derivada utilizando várias restrições. Neste exemplo, uma chave e uma data de restrição são utilizadas para determinar uma chave de data (Kdate, na figura). Na figura, a data é codificada como 20110715, correspondendo a 15 de Julho de 2011, apesar de datas poderem ser codificadas de forma diferente e, geralmente, a informação pode ser codificada de forma diferente do ilustrado nas figuras. A data chave data é usada com uma restrição regional para derivar uma chave regional, Kregion. Neste exemplo, a região é codificada com um identificador regional “USA-zone-1”, que pode corresponder uma das várias regiões nos Estados Unidos. A chave Kregion é usada com uma restrição de serviço para derivar uma chave de serviço, KService. Neste exemplo, o serviço é um serviço de sistema de computador virtual, codificado por sua sigla VCS. A chave KService é utilizada com um identificador de solicitação para derivar uma chave de assinatura, isto é, uma chave utilizada para assinar as solicitações para um serviço. Neste exemplo, o identificador do pedido é “vcs_request”, que pode corresponder a um determinado tipo de solicitação que pode ser apresentada ao serviço VCS. Por exemplo, “vcs_request” pode corresponder a uma solicitação de provisão, interrom-

per ou modificar um sistema de computador virtual. A chave de assinatura é utilizada para gerar uma assinatura que pode ser apresentada com as solicitações. A assinatura pode ser gerada de qualquer forma adequada, como descrito acima.

[076] Como ilustrado na Figura 12, o pedido pode ser canonicalizado para formar uma mensagem M_c, que é como entrada para uma função HMAC para gerar a assinatura. É claro que, as variações, incluindo variações, onde a canonicalização não é necessária e onde outras funções além de funções HMAC são utilizadas, podem ser utilizadas de acordo com as várias modalidades. Além disso, a Figura 12 mostra um exemplo particular de uma derivação de assinatura de acordo com uma modalidade. No entanto, mais ou menos restrições podem ser utilizadas para derivar a assinatura e restrições podem ser usadas em uma ordem diferente da ilustrada. Além disso, enquanto a Figura 12 mostra a derivação de uma assinatura, as técnicas podem ser aplicadas para derivar outros objetos que não podem ser considerados assinaturas em todos os aplicativos. Por exemplo, as técnicas ilustradas na Figura 12 (e outras) podem ser utilizadas geralmente para derivar chaves.

[077] A Figura 13 é um exemplo ilustrativo de uma função 1300 para derivar uma assinatura, de acordo com pelo menos uma modalidade. Como ilustrado na Figura 13, a assinatura é calculada como:

HMAC(HMAC(HMAC(HMAC(HMAC(K,data),região),serviço)protocolo),Mc).

Neste exemplo, K é uma chave, “data” é uma codificação de uma data, “região” é uma codificação de um identificador de uma região, “serviço” é uma codificação de um identificador de um serviço, “protocolo” corresponde a um protocolo de codificação de mensagem em particular, e M_c é uma mensagem canonicalizada. Assim, como ilustrado na Figura 13, a assinatura é calculada através do cálculo da mesma função HMAC várias vezes, cada vez com uma restrição diferente como uma entrada para a função HMAC. A chave de assinatura, neste exemplo, é a seguinte:

HMAC(HMAC(HMAC(HMAC(K,data),região),serviço),protocolo)

que por si só é derivado através da utilização da função HMAC várias vezes, cada vez com uma restrição diferente.

[078] No exemplo da Figura 13, cada uma das várias restrições define um domínio e a intersecção dos domínios definidos e define a maneira pela qual a assinatura gerada com a chave de assinatura seria válida. Neste exemplo específico, a assinatura gerada com a chave de assinatura ilustrada na Figura 13 seria válida na data especificada, na região especificada, e para o serviço especificado usando o protocolo especificado. Assim, se uma solicitação for assinada usando a chave de assinatura, mas em uma data diferente da especificada pela entrada para a chave de assinatura, a assinatura para a solicitação pode ser considerada não verificada, mesmo que a solicitação tenha sido feita para o serviço especificado e na região especificada.

[079] Como com outras modalidades aqui descritas, variações são consideradas como estando dentro do escopo da presente divulgação. Por exemplo, a Figura 13 mostra o uso repetido de uma função HMAC. Várias funções podem ser usadas para derivar uma assinatura e, em algumas modalidades, as funções de HMAC não são usadas em cada parte da derivação. Além disso, como se referiu, diferentes restrições e diferentes números de restrição pode também ser utilizados em várias modalidades.

[080] Chave de derivação pode ser realizada de várias maneiras, de acordo com várias modalidades. Por exemplo, um único dispositivo de computação pode calcular uma chave de assinatura, de acordo com algumas modalidades. De acordo com outras modalidades, vários dispositivos de computação podem calcular coletivamente uma chave de assinatura. Como um exemplo ilustrativo específico, referindo-se à Figura 13, um computador pode calcular

Kregion = HMAC (HMAC(K, data), região)

e um outro computador pode calcular

Chave de assinatura=HMAC(Kregion, Service).

[081] Como outro exemplo, um sistema de computador separado pode executar uma camada diferente no cálculo da chave de assinatura. Referindo-se ao exemplo no parágrafo anterior, em vez de um único computador computação Kregion, um computador pode calcular

Kdate = HMAC(K, data)

e um outro computador pode calcular

Kregion = HMAC(Kdata, região).

[082] A Figura 14 é um exemplo ilustrativo de como a derivação de chave múltipla pode ser realizada e utilizada de acordo com pelo menos uma modalidade. Em particular, a Figura 14 mostra um exemplo de diagrama 1400 ilustrando os membros de um conjunto distribuído de sistemas de computador coletivamente calculando uma chave de assinatura (ou outra chave, em diversas outras modalidades). Como mostrado na Figura 14, cada membro do conjunto é um sistema de computador do provedor de chave 1402 que gera uma chave e fornece a chave gerada para outro sistema de computador. Por exemplo, um fornecedor de chave chamado Key $Provider_1$ obtém uma chave K (de outra fonte, ou por meio da geração da própria chave), e utiliza a chave e uma restrição, chamada R_1 para gerar uma chave K_1. Key $Provider_1$ passa a chave K_1 para $KeyProvider_2$, que utiliza K_2 e uma outra restrição, R_2, para gerar outra chave K_2. $KeyProvider_2$ passa a chave K_2 a $KeyProvider_3$, que usa K_3 e outra restrição, R_3, para gerar outra chave K_3. Dependendo de quantos provedores de chave existem em uma modalidade particular, esse processo pode continuar até $KeyProvider_{N-1}$ passa uma chave K_{N-1} ao $KeyProvider_N$, que usa K_{N-1} e outra restrição, R_N, para gerar outra chave de assinatura, K_N. A chave K_N é, então, passada para um sistema de computador verificador 1404. A chave K ou quaisquer chaves derivadas de K (geralmente referidas como K_i na figura) também pode ser transmitidas para um sistema de computador do assinante 1406, como por meio de

um algoritmo de troca de chaves seguro.

[083] O sistema de computador signatário 1406 pode também, em várias modalidades, gerar K_N por conta própria se, por exemplo, as restrições R_1-R_N são disponibilizadas para o assinante e/ou disponibilizadas publicamente. Além disso, o sistema de computador de assinante 1406 pode executar apenas uma parte do processo para derivar K_N por si só, em várias modalidades. Por exemplo, o assinante poderá obter (talvez a partir de um sistema de computador provedor de chave apropriado) K_i, para algum inteiro i, que é menos do que N e restrições R_{i+1} através R_N. O assinante pode então usar K_i e restrições R_{i+1} através de R_N para gerar a chave de assinatura, K_N. Outras variações também são consideradas como estando dentro do escopo da presente divulgação.

[084] O sistema de computador signatário 1406 pode usar a tecla K_N para assinar as mensagens a serem verificados pelo verificador 1404. Por exemplo, como ilustrado, o assinante 1406 calcula a assinatura $S=HMAC(K_N, M_C)$, em que M_C é uma versão canonicalizada de uma mensagem M, também enviada para o verificador. Uma vez que o verificador tem K_N, o verificador pode canonicalizar independentemente a mensagem M e calcular $HMAC(K_N, M_C)$ para determinar se o resultado do cálculo corresponde à assinatura recebida S.

[085] Deve-se notar que as variações do processo ilustrado na Figura 14, e outros processos aqui descritos, enquanto mostrados como envolvendo o uso de múltiplas funções HMAC, várias funções diferentes podem ser utilizadas para derivar chaves. Por exemplo, diferentes tipos de funções de código de autenticação de mensagem (MAC) podem ser usados em diferentes momentos em derivar uma chave. Por exemplo, a saída de um tipo de função MAC pode ser usada como a base para entrada em outro tipo de função MAC. Geralmente, outros tipos de funções podem ser usados em vez de e/ou em além das funções HMAC em um processo de derivação chave e, em várias modalidades, não é necessário utilizar o mesmo tipo

de função várias vezes para derivar uma chave, mas diferentes funções podem ser usadas cada vez que uma função é necessária.

[086] A Figura 15 é um diagrama 1500 ilustrando uma forma exemplar em que as chaves podem ser derivadas usando várias restrições, de acordo com pelo menos uma modalidade. O exemplo mostrado na Figura 15 refere-se aos clientes, como clientes de um provedor de recursos de computação. No entanto, como notado, as técnicas aqui descritas, incluindo as técnicas descritas em relação à Figura 15, podem ser utilizadas em vários outros contextos.

[087] Como mostrado, uma chave cliente, K_{cust}, é parte de um conjunto de chaves de termos longos do cliente, cada um dos quais pode ser chaves utilizadas por um cliente por um período de tempo, como até que o cliente atualize a chave, é atribuída uma nova chave, ou de outra forma altera a chave. As chaves também podem ser usadas indefinidamente por um ou mais clientes. A chave do cliente, K_{cust}, é utilizada para derivar uma ou mais chaves de região como, por exemplo, de uma forma ilustrada acima. Por exemplo, como ilustrado na Figura 15, duas chaves de região podem ser geradas, como calculando HMAC(K_{cust}, USA-E-1) e HMAC(K_{cust}, USA-N-1), onde USA-E-1 e USA-N-1 são identificadores das respectivas regiões. De modo semelhante, as chaves região podem ser utilizadas para derivar chaves de data cuja validade pode ser restringida pela data utilizada para codificar as chaves de data. Cada uma das chaves de data pode ser utilizada para derivar chaves de serviço como, por exemplo, de um modo descrito acima.

[088] Deste modo, em várias modalidades, as chaves de serviço podem ser utilizadas com os respectivos serviços apenas na data e nas regiões utilizadas para codificar as chaves. Novas chaves de data podem ser geradas para cada dia, enquanto que as chaves da região e as chaves de termo longo do cliente podem ser geradas com menos frequência. Várias derivações de chave de restrição como ilustrado na Figura 15 e em outras partes da presente divulgação fornecem inúmeras

vantagens. Por exemplo, ao derivar a chave no modo descrito em relação à Figura 15, se uma chave de assinatura está comprometida (por exemplo, maliciosamente obtida por um terceiro), a violação de segurança é limitada a uma determinada região, em um determinado dia, e em conexão com um serviço particular. Outros serviços permaneceriam inalterados. Vantagens semelhantes são aplicáveis em outras maneiras que as chaves podem ser derivadas.

[089] A Figura 16, por exemplo, é um diagrama 1600 ilustrando outro modo exemplar pelo qual as chaves podem ser derivadas, de acordo com pelo menos uma modalidade. A Figura 16 ilustra os conceitos de uma forma semelhante ao da Figura 16. Na Figura 16, no entanto, as chaves de termo longo do cliente são utilizadas para derivar chaves data. As chaves de data são usadas para derivar chaves da região. As chaves da região são usadas para derivar chaves de serviço. Derivação pode ser realizada de acordo com as várias modalidades aqui descritas.

[090] A Figura 17 é um diagrama 1700 ilustrando ainda outra forma exemplar em que as chaves podem ser derivadas, de acordo com pelo menos uma modalidade. Na Figura 17, as chaves de termo longo de clientes são usadas para derivar chaves de meses. As chaves meses são usadas para derivar chaves regionais. As chaves regionais são usadas para derivar chaves de data. As chaves de data são usadas para definir as chaves de serviço. A derivação das várias chaves pode ser feita de uma maneira consistente com a descrição acima.

[091] Como discutido, várias técnicas da presente divulgação permitem uma nova maneira de gerar sessões. Uma sessão pode ser um período de tempo pelo qual uma ou mais ações são permitidas, onde expiração (ou outra terminação) da sessão faz com que a uma ou mais ações a serem desautorizadas. A Figura 18 é um fluxograma que mostra um exemplo ilustrativo de um processo 1800 para iniciar uma sessão, em conformidade com pelo menos uma modalidade. O processo 1800 pode ser realizado por qualquer dispositivo de computação adequado ou coletiva-

mente por qualquer coleção apropriada de dispositivos de computação. Por exemplo, o processo 1800 pode ser realizado por um dispositivo de cliente de um cliente de um provedor de recursos computacionais. Como outro exemplo, em outra modalidade, referindo-se à Figura 3, um dos serviços de uma zona de falha pode ser uma sessão de serviço e um ou mais dispositivos de computação que participam no fornecimento do serviço podem realizar o processo 1800.

[092] Voltando à Figura 18, em uma modalidade, o processo 1800 inclui obter 1802 uma chave, K. A chave K pode ser qualquer chave apropriada, como uma chave derivada usando outras chaves, como de uma maneira descrita acima. Por exemplo, a chave K podem ter sido propagadas para um dispositivo de computação que participam na realização do processo 1800. Em algum ponto (como mediante a obtenção da chave K, como ilustrado na figura), em uma modalidade, uma solicitação de início de sessão pode ser recebida 1804. A solicitação pode ser uma solicitação eletrônica, como descrito acima. Além disso, a solicitação, em uma modalidade, é assinada e verificada através de várias técnicas da presente divulgação. Além disso, a solicitação pode ser uma solicitação diferente dependendo de um determinado ambiente utilizado para implementar o processo 1800. Por exemplo, se o processo 1800 é realizado por um dispositivo cliente (como um dispositivo do cliente de um cliente de um provedor de recursos computacionais) para gerar uma sessão, a solicitação de início de sessão pode ser recebida por um módulo do dispositivo de cliente.

[093] Em uma modalidade, os parâmetros da sessão são determinados 1806. Os parâmetros de sessão podem ser uma informação que indica uma ou mais restrições sobre a sessão que está sendo gerada. Parâmetros de exemplo incluem, entre outros, duração, identificadores dos usuários aceitáveis de uma chave de sessão a ser gerada, um ou mais serviços com os quais a chave de sessão a ser gerada é utilizável, as restrições sobre as ações que podem ser executadas usando a chave de sessão, qualquer uma das restrições descritas acima, e outros. Os parâ-

metros podem ser codificados eletronicamente de acordo com exigências de formatação predefinidas para assegurar que os cálculos que envolvem uma chave de sessão que é gerada são consistentes. Por exemplo, as datas podem ser requeridas a serem codificadas no formato YYYYMMDD. Outros parâmetros podem ter seus próprios requisitos de formatação. Além disso, a determinação dos parâmetros de sessão pode ser realizada de várias maneiras. Por exemplo, os parâmetros podem ser parâmetros predefinidos para uma sessão, de tal modo que uma chave de sessão é utilizável apenas para uma gama de ações permitidas para o solicitante do início da sessão e durante um período de tempo predefinido (por exemplo, um período de 24 horas). Como outro exemplo, os parâmetros podem ser fornecidos como parte de ou em conexão com a solicitação recebida. Por exemplo, os parâmetros podem ser gerados de acordo com a entrada de usuário a partir do solicitante e codificados de acordo com um esquema predefinido.

[094] Em uma modalidade, uma vez que os parâmetros são determinados, os parâmetros são utilizados para calcular uma chave de sessão 1808, K_S. Calculando a chave de sessão K_S pode ser realizada de várias maneiras. Por exemplo, em uma modalidade, a chave de sessão K_S pode ser calculada como (ou de outro modo com base pelo menos em parte em)

HMAC(K, Session_Parameters)

em que Session_Parameters é uma codificação dos parâmetros que foram determinados 1806. Session_Parameters podem ser codificados de forma predefinida, que garante a consistência computacional. A chave de sessão K_S pode igualmente ser calculada por outros meios, como por exemplo de uma maneira descrita abaixo em relação à Figura 19.

[095] Uma vez que a chave de sessão K_S é calculada 1808, em uma modalidade, a chave de sessão K_S é fornecida para utilização. Fornecer a chave de sessão pode ser realizado de várias maneiras, em várias modalidades. Por exemplo, a

chave de sessão pode ser fornecida para um módulo do solicitante para permitir que o solicitante assine mensagens com a chave de sessão. A chave de sessão pode também ser fornecida através de uma rede para outro dispositivo para permitir que o outro dispositivo assine mensagens com a chave de sessão. Por exemplo, a chave de sessão, também pode ser fornecida a um delegado para que a sessão seja iniciada. Por exemplo, o solicitante pode ter especificado um delegado em ou em conexão com a solicitação para iniciar a sessão. A chave de sessão pode ser fornecida eletronicamente de acordo com a informação fornecida pelo solicitante (ou seja, delegante), como um correio eletrônico ou outro endereço eletrônico.

[096] Como referido, a Figura 19 mostra um exemplo ilustrativo de um processo 1900 que pode ser utilizado para gerar uma assinatura, de acordo com uma modalidade. O processo 1900 pode ser realizado por um ou mais dispositivos de computação, como um ou mais dispositivos de computação que executam o processo 1800 descrito acima em relação à Figura 18. O processo 1900, como ilustrado na Figura 19, inclui receber parâmetros de sessão, como descrito acima. Com os parâmetros de sessão tendo sido obtidos, em uma modalidade, uma chave intermediária, K_{i+1} é calculado 1904 como:

$K_{i+1}=HMAC(K_i, P_i)$

em que K_i, pode ser a chave K na descrição da Figura 18 para o primeiro cálculo de K_{i+1}, e P_i é o iº parâmetro dos parâmetros da sessão. Os parâmetros de sessão podem ser ordenados de acordo com uma ordem predeterminada para garantir a consistência computacional da armadura de chave.

[097] Em uma modalidade, uma determinação é realizada 1906 se há parâmetros adicionais a serem utilizados na geração de chave de sessão. Se há parâmetros adicionais, em uma modalidade, o índice i é aumentado 1908 em um e K_{i+1} é novamente calculado 1904. Se, no entanto, é determinado que não há parâmetros adicionais, em seguida, K_S é definido 1910 ao valor de K_{i+1}.

[098] A Figura 20 é um fluxograma que mostra um exemplo ilustrativo de um processo 2000 para obter acesso a um ou mais recursos de computação durante uma sessão de acordo com pelo menos uma modalidade. Deve-se notar que, enquanto a Figura 20 apresenta um processo 2000 para obter acesso a um ou mais recursos de computação, como com outros processos aqui descritos, o processo 2000 pode ser modificado para qualquer situação em que são utilizados processos de assinatura. O processo 2000 pode ser realizado por um sistema de computador de um usuário solicitando o acesso a um ou mais recursos de computação, como um sistema de computador de cliente ilustrado na Figura 1 e/ou um sistema de computador de cliente descrito em outro ponto aqui. Em uma modalidade, o processo 2000 inclui obter uma chave de sessão K_S. A chave de sessão pode ser obtida de qualquer forma adequada, como em uma mensagem eletrônica. A chave de sessão pode ser obtida a partir de um sistema de computador de um delegante de acesso a um ou mais recursos de computação ou outro sistema de computador, como um sistema de computador que opera em ligação com um ou mais sistemas de computadores que realizaram um processo para a geração de K_S.

[099] Em uma modalidade, uma solicitação de R é gerada 2004. A solicitação R pode ser uma mensagem, como descrito acima. A solicitação R é então canonicalizada 2006, em uma modalidade, e uma assinatura é calculada 2008 a partir da mensagem canonicalizada, como por computação da assinatura como (ou de outro modo com base pelo menos em parte na) HMAC(K_S, R_C). Após a geração da assinatura, a assinatura S e a solicitação R são fornecidos 2010. Por exemplo, como discutido acima, a assinatura S e solicitação R podem ser fornecidos eletronicamente a uma interface de um sistema de computador que participa na gestão de pedidos e verificação de assinaturas. A assinatura S e solicitação R, como com assinaturas e mensagens em geral, podem ser fornecidas em conjunto em uma única comunicação, as comunicações em separado, ou em conjunto com várias comunicações. Ou-

tra informação pode também ser fornecida em relação à assinatura S e solicitação R. Por exemplo, a informação de identificação pode ser proporcionada para permitir que um verificador selecione uma chave adequada para gerar uma assinatura com o qual se verifica a assinatura recebida. A identificação pode ser, por exemplo, um identificador de uma chave que deve ser utilizada para gerar uma assinatura para comparação. Outras informações também podem ser fornecidas e utilizadas, conforme o caso nas várias modalidades.

[0100] A Figura 21 é um fluxograma que mostra um exemplo ilustrativo de um processo 2100 para determinar se concede acesso solicitado a um ou mais recursos de computação, de acordo com pelo menos uma modalidade. Como ilustrado na Figura 12, o processo 2100 inclui obter 2102 uma chave de assinatura K_S. Como acontece com outras menções aqui sobre obter uma chave de assinatura, a chave de assinatura pode ser obtida de várias maneiras, como recebendo a chave de assinatura a partir de uma outra fonte, recuperar a chave de assinatura a partir da memória, calcular a assinatura de chave a partir da informação disponível e semelhantes.

[0101] Em uma modalidade, a solicitação R recebida é canonicalizada para formar R_C, como de um modo descrito acima. Deve-se notar que, como acontece com os outros processos descritos aqui, são possíveis variações. Por exemplo, um sistema de computador que executa uma variação do processo 2100 (ou outro processo) pode simplesmente receber a mensagem canonicalizada e canonicalização pode ser realizada por outro dispositivo de computação. Voltando à descrição da Figura 21, uma assinatura S' é calculada como (ou de outro modo com base pelo menos em parte na) HMAC(K_S, Rc). A chave de assinatura S' calculada é comparada 2110 com a assinatura recebida S para determinar se as duas assinaturas são equivalentes. Se as duas assinaturas são determinados e não são equivalentes, a sessão é determinada 2112 para ser invalidada e ações apropriadas, como negação

do pedido, podem ser tomadas. Se as duas assinaturas são consideradas equivalentes, a sessão é validada 2114 e medidas apropriadas, como a concessão de acesso a um ou mais recursos de computação, podem ser tomadas.

[0102] As técnicas da presente divulgação, como mencionadas, podem ser utilizadas para permitir a delegação de autoridade. A Figura 22 é um fluxograma que mostra um exemplo ilustrativo de um processo 2200 para a delegação de autoridade de acordo com pelo menos uma modalidade. O processo 2200 pode ser realizado por um dispositivo de computação, como um dispositivo de computação de um usuário tentando delegar o acesso a um ou mais recursos de computação, ou um dispositivo de computação de um provedor de recursos de computação, ou qualquer dispositivo de computação adequado. Como ilustrado na figura, o processo 2200 inclui obter 2202 uma chave de sessão K_{si}. A sessão chave obtida K_{si}, pode ser obtida de qualquer forma adequada, como uma forma na qual as chaves descritas acima são descritas como sendo obtidas. Além disso, a chave de sessão pode ser uma chave que foi gerada como parte de um processo para delegar o acesso a um ou mais recursos de computação. Por exemplo, a chave de sessão pode ter sido gerada pela execução do processo 2200, ou uma variação da mesma.

[0103] Em uma modalidade, os parâmetros da sessão são determinados 2204. Os parâmetros da sessão podem ser determinados de qualquer forma adequada, como descrito acima em relação à Figura 18. Com os parâmetros da sessão determinados 2204, uma nova chave de sessão $K_{S(i+1)}$ pode ser gerada, como descrito acima, incluindo como descrito acima em relação à Figura 19. Uma vez gerada, a nova chave de sessão pode ser fornecida a um delegado. Por exemplo, a chave de sessão pode ser enviada em uma mensagem eletrônica para o delegado. A chave de sessão pode ser fornecida direta ou indiretamente para o delegado. Por exemplo, a chave de sessão pode ser dada ao delegante e o delegante pode ser responsável por fornecer a chave de sessão para um ou mais delegados. Outras

informações também podem ser fornecidas ao delegado. Por exemplo, os parâmetros da sessão podem ser fornecidos ao delegado, para permitir que o delegado forneça os parâmetros da sessão com as assinaturas, permitindo assim que um destinatário (por exemplo, verificador) dos parâmetros de sessão gere assinaturas esperadas para verificar se as assinaturas fornecidas são válidas. Por exemplo, o destinatário pode usar os parâmetros para gerar uma chave de sessão a partir de uma credencial secreta ou uma chave derivada desta e usar a chave de sessão para gerar uma assinatura para uma versão canonicalizada de uma mensagem assinada correspondente. Geralmente, os parâmetros podem ser disponibilizados ao destinatário de uma assinatura de qualquer maneira adequada para permitir que o destinatário verifique as assinaturas de mensagens e o delegado não necessariamente precisa ter acesso aos parâmetros se o destinatário tem acesso aos parâmetros independentes do delegado.

[0104] A Figura 23, por exemplo, mostra um diagrama 2300 que ilustra como os privilégios podem ser delegados várias vezes. Um delegante 2302 pode querer conceder um ou mais privilégios de acesso a um delegado 2304. O delegado 2304, no entanto, neste exemplo, pode querer fornecer um ou mais privilégios para outro delegado 2306. Assim, neste exemplo, o delegado 2304 pode tornar-se um delegante. Da mesma forma, o delegado 2306 pode querer dar acesso a outro delegado e o delegado que pode desejar conceder acesso a outro delegado e assim por diante, até que finalmente um ou mais privilégios são concedidos a outro delegado 2308.

[0105] Assim, neste exemplo, o delegante original 2302 envia uma solicitação de delegação para um serviço de autenticação com base em sessão 2310 que pode ser um serviço de uma zona de falha, como descrito acima. Em resposta, em uma modalidade, o servido de autenticação com base em sessão gera e fornece uma chave de sessão para o delegante 2302, como descrito acima em relação à Figura 22. O delegante 2302, em seguida, em uma modalidade, fornece a chave de

sessão que recebeu do serviço de autenticação com base em sessão 2310 para o delegado 2304. O delegado 2304 pode fornecer a chave de sessão para outro delegado 2306. Deste modo, o delegado 2306 receberia o escopo dos privilégios recebidos pelo delegado 2304 que seria o mesmo que o escopo dos privilégios fornecidos ao delegado 2306.

[0106] No entanto, também ilustrado na Figura 23, o delegado 2304 pode apresentar uma solicitação de delegação para o serviço de autenticação com base em sessão 2310 e receber uma chave de sessão diferente que foi gerada pelo serviço de autenticação com base em sessão 2310, em resposta à solicitação de delegação. O delegado 2304 pode fornecer esta nova chave de sessão para o próximo delegado 2306. O próximo delegado 2306 pode fornecer a chave de sessão para outro delegado, ou como descrito acima, pode igualmente apresentar uma solicitação de delegação para o serviço de autenticação com base em sessão 2310, que passaria a gerar então uma chave de sessão e fornecer a chave de sessão para o delegado 2306 que apresentou a solicitação de delegação. Como indicado na Figura 23, isto pode continuar e um ou mais dos delegados pode tentar utilizar uma chave de sessão que ele ou ela tenha recebido.

[0107] Neste exemplo particular, um delegado 2308 fornece a chave de sessão para um recurso de computação 2312, em ligação com uma solicitação. Como dito acima, a solicitação pode incluir a chave de sessão, embora a chave de sessão possa ser fornecida separadamente do pedido. O recurso de computação 2312 pode ser qualquer um dos recursos computacionais descritos acima ou, em geral, qualquer recurso de computação. Um serviço de gestão de políticas 2314 pode incluir um verificador, como descrito acima, e pode, a pedido do recurso de computação, validar as solicitações. O recurso de computação 2312 e serviço de gestão de política 2314 também podem ser um único componente, embora ilustrado separadamente na Figura 23. Além disso, embora a Figura 23 mostre um único serviço de autenti-

cação com base em sessão 2310 sendo usado para gerar chaves de sessão, várias modalidades podem utilizar diferentes serviços de autenticação com bases em sessão.

[0108] Como mencionado acima, numerosas variações além dos exemplos ilustrativos aqui fornecidos são consideradas como estando dentro do escopo da presente divulgação. A Figura 24 mostra um diagrama 2400 que representa um exemplo ilustrativo de uma forma na qual as chaves podem ser derivadas utilizando as chaves de várias entidades, de acordo com uma modalidade. Na Figura 23, a chave do cliente, K_{cust}, é a partir de um conjunto de chaves de clientes mantidas por um provedor de recursos de computação. Como com modalidades descritas acima, enquanto a Figura 23 discutiu um exemplo ilustrativo em conexão com um provedor de recursos de computação, outras variações são consideradas como estando dentro do escopo da presente divulgação.

[0109] Na Figura 24, um conjunto de chaves de autoridade é mantido, onde cada chave de autoridade corresponde a um domínio diferente de autoridade. Cada chave de autoridade derivada da chave cliente K_{cust} pode ser, por exemplo, que se propague em diferentes zonas de falha, como descrito acima. As zonas de falhas podem ser, por exemplo, centros de dados em diferentes jurisdições políticas. Deve-se notar, contudo, que enquanto a Figura 24 mostra cada chave de autoridade dividida tendo sido derivada a partir de uma única chave cliente, K_{cust}, variações são possíveis. Por exemplo, as chaves de autoridade divididas podem ser derivadas de forma independente. Como outro exemplo, uma ou mais chaves de autoridade divididas podem ser derivadas a partir de uma chave comum, uma ou mais outras podem ser derivadas de outra chave comum, e outros semelhantes.

[0110] Em uma modalidade, várias autoridades são capazes de combinar autoridade para permitir o acesso a um ou mais recursos de computação. Por exemplo, como ilustrado na Figura 24, os subconjuntos de chaves de autoridade di-

vididas podem ser usados para derivar outras chaves. Por exemplo, como ilustrado na Figura 23, duas chaves de autoridade, marcadas Auth1 e Auth2, são usadas para derivar uma chave de entidade resultante da fusão. Para derivar a chave de autoridade de fusão, em uma modalidade, um valor de HMAC(f(Auth1, Auth2), R) é calculado, onde R é uma restrição, como descrito acima. Neste exemplo, f é uma função das chaves de autoridade divididas, e pode ser mais do que duas dimensões. Por exemplo, as três chaves de autoridade divididas, Auth1, Auth2, e Auth3 são utilizados, como ilustrado na Figura 23, em uma função f(Auth1, Auth2, Auth3) para calcular a chave de entidade fundida como (ou de outro modo com base pelo menos em parte na) HMAC(f(Auth1, Auth2, Auth3), R).

[0111] Numerosas variações de construção de chaves de entidades diferentes são consideradas como estando dentro do escopo da presente divulgação. Por exemplo, uma entidade pode gerar (ou geraram) uma chave (K_{spec}), utilizando diversas modalidades da presente divulgação. Cada entidade K_{spec} pode corresponder uma fonte de chave parcial, que pode ser uma codificação disponível ao público (ou codificação de outra forma disponível para uma mensagem signatária e um verificador de assinatura) de restrições utilizadas para gerar o seu K_{spec}. Por exemplo, uma semente chave parcial pode ser (K1/20110810/usa-east-1/DDS, K2/20110810/org_name/jpl/DDS), em que cada cadeia entre barras é uma restrição. Dita codificação de informação pode ser referida como um caminho chave. Como um exemplo mais geral, uma fonte de chave parcial pode ser $X_1/.../X_n$, em que cada X_i (para i entre 1 e n) corresponde a um parâmetro, como um parâmetro descrito acima. As fontes principais parciais das autoridades aplicáveis podem ser codificadas como um n-tuple, referido como uma fonte de chave. Uma n-tuple para o exemplo imediatamente acima pode ser ($spec_1$, $spec_2$, ..., $spec_n$), em que cada entrada é um caminho chave para um correspondente K_{Spec}. Deve-se notar que a fonte de chave (e/ou caminho chave) codifica o uso de chave exato (restrição total entre to-

das as chaves autorizadas) que o detentor da chave está autorizando por produção de uma assinatura/chave. Além disso, com fontes de chave parciais disponíveis para ambos os signatários de mensagens e verificadores de assinaturas, ordenação arbitrária dos parâmetros utilizados para gerar chaves e assinaturas é possível uma vez que, por exemplo, um signatário de mensagem tem informações que especificam a ordem, os parâmetros foram usados para gerar uma assinatura chave e podem, portanto, gerar uma chave de assinatura e mensagem de acordo.

[0112] Um valor para HMAC(Kspec, keu-seed) podem então ser obtidos ou calculados para cada um dos órgãos competentes, isto é, para as autoridades pelas quais uma chave deve ser gerada. Este valor pode ser calculado por um cliente obtendo uma chave de assinatura para assinar mensagens ou pode ser calculado por outro dispositivo e, posteriormente, fornecer ao cliente, em várias modalidades. Cada um desses valores pode ser referido como chaves parciais, para a finalidade da discussão seguinte. A semântica de cada uma destas chaves parciais, em uma modalidade, é que são válidas apenas quando combinadas com a construção a seguir (e certas variações da construção abaixo) e, quando combinadas, formam a intersecção das especializações codificadas nas fontes de chaves.

[0113] Para gerar uma chave de assinatura para assinar uma mensagem, um valor para

K_s= HMAC (partial_key$_1$+ ... + partial_key$_n$, key-seed)

onde “+” pode se referir a alguma operação associativa em chaves parciais que cercam o símbolo na fórmula. O sinal “+” pode ser, por exemplo, uma operação OR exclusiva (XOR) em bits compreendendo as chaves parciais. O símbolo “+” também podem se referir a alguma outra operação ou função adequada.

[0114] Para verificar uma assinatura usada para assinar uma mensagem, um verificador pode obter cada chave parcial, combinar as chaves parciais como acima para formar uma chave de assinatura, assinar uma mensagem recebida e comparar

o resultado com um resultado esperado para verificar a assinatura, como discutido acima.

[0115] Modalidades exemplares da divulgação podem ser descritas tendo em vista as seguintes cláusulas:

Cláusula 1. Um método implementado por computador para a prestação de serviços, compreendendo:

sob o controle de um ou mais sistemas de computadores configurados com instruções executáveis,

receber, a partir de uma parte de autenticação, informação eletrônica que codifica uma mensagem, a assinatura para a mensagem, e um conjunto de uma ou mais restrições nas chaves derivadas a partir de uma credencial secreta compartilhada com a parte de autenticação, a assinatura sendo determinável por aplicação de uma base de função código de autenticação de mensagem à base de hash, a credencial secreta, e o conjunto de uma ou mais restrições, mas também sendo indeterminável tendo apenas a função de código de autenticação de mensagem à base de hash, mas sem ter o conjunto de uma ou mais restrições;

obter uma chave gerada pelo menos em parte, utilizando pelo menos um subconjunto do conjunto de uma ou mais limitações;

calcular, por um ou mais sistemas de computador, um valor de uma função de código de autenticação de mensagem à base de hash por pelo menos introduzir na função de código de autenticação de mensagem à base de hash:

primeira entrada com base pelo menos em parte na chave obtida; e

segunda entrada com base pelo menos em parte no conjunto de uma ou mais limitações, determinando, por um ou mais sistemas de computadores e com base pelo menos em parte no valor calculado, se a assinatura é válida; e

fornecer acesso a um ou mais recursos de computação quando determinado que a assinatura é válida.

Cláusula 2. O método implementado por computador da cláusula 1, em que:

a mensagem compreende uma solicitação de acesso a um ou mais recursos de computação;

o método compreende ainda determinar se o conjunto de uma ou mais limitações indica que a solicitação deve ser cumprida, e

fornecer acesso a um ou mais recursos de computação depende de determinar que quais restrições indicam que a solicitação deve ser cumprida.

Cláusula 3. O método implementado por computador, de acordo com a reivindicação 2, em que a informação que codifica o conjunto de uma ou mais restrições é codificado por um documento e em que determinar se o conjunto de restrições indica que a solicitação que deveria ser cumprida inclui a avaliação do documento contra um contexto no qual a solicitação foi recebido.

Cláusula 4. O método implementado por computador da cláusula 1, em que:

a mensagem compreende uma solicitação de acesso a um recurso de computação de um ou mais recursos de computação;

a informação que codifica para o conjunto de uma ou mais restrições inclui informações especificando o recurso de computação; e

proporcionar o acesso a um ou mais recursos de computação inclui proporcionar acesso a recursos de computação quando o recurso de computação coincide com o recurso de computação especificada.

Cláusula 5. O método implementado por computador da cláusula 1, em que:

a informação que codifica o conjunto de uma ou mais restrições corresponde a um período de tempo para o qual a mensagem é válida;

determinar se a assinatura é válida é com base pelo menos em parte se mensagem foi apresentada durante o período de tempo correspondente.

Cláusula 6. O método implementado por computador da cláusula 1, em que:

a informação que codifica para o conjunto de uma ou mais restrições corres-

ponde a uma restrição com base pelo menos em parte em um local, e

determinar se a assinatura é válida é com base pelo menos em parte se uma localização de pelo menos um de um ou mais sistemas de computadores corresponde ao local correspondente.

Cláusula 7. Um método implementado por computador para a prestação de serviços, compreendendo:

sob o controle de um ou mais sistemas de computadores configurados com instruções executáveis,

obter codificação de informação eletrônica (i) uma mensagem, (ii) uma primeira assinatura para a mensagem, e (iii) um conjunto de um ou mais parâmetros, a primeira assinatura tendo sendo sido gerada com base pelo menos em parte em (i) a mensagem, (ii) uma credencial secreta, e (iii) o conjunto de um ou mais parâmetros, a primeira assinatura sendo ainda determinável tendo apenas a mensagem e a credencial secreta, mas sem o conjunto de um ou mais parâmetros;

derivar uma segunda credencial com base pelo menos em parte na credencial secreta e pelo menos um subconjunto do conjunto de um ou mais parâmetros;

gerar, com base pelo menos em parte na segunda credencial derivada, uma segunda assinatura;

determinar se a primeira assinatura corresponde à segunda assinatura, e

fornecer acesso a um ou mais recursos de computação quando a segunda assinatura gerada coincide com a primeira assinatura.

Cláusula 8. O método implementado por computador da cláusula 7, em que derivar a segunda credencial inclui introduzir, em uma função, a credencial secreta e pelo menos um subconjunto do conjunto de um ou mais parâmetros.

Cláusula 9. O método implementado por computador da cláusula 8, em que a função é uma função de autenticação de mensagem simétrica.

Cláusula 10. O método implementado por computador da cláusula 9, em que

a função de autenticação de mensagens simétrica é uma função hash.

Cláusula 11. O método implementado por computador da cláusula 9, em que introduzir, na função, a credencial secreta e pelo menos um subconjunto de um ou mais parâmetros é realizada como parte do Código de autenticação de mensagem à base de hash (HMAC).

Cláusula 12. O método implementado por computador da cláusula 8, em que a geração da segunda assinatura inclui introduzir a função de ambos uma saída da função e um parâmetro a partir do conjunto de um ou mais parâmetros.

Cláusula 13. O método implementado por computador da cláusula 7, em que a informação que codifica os um ou mais parâmetros compreende um documento eletrônico que codifica para o conjunto de um ou mais parâmetros.

Cláusula 14. O método implementado por computador da cláusula 8, em que:

gerar a segunda assinatura é com base pelo menos em parte em uma chave,

o conjunto de um ou mais parâmetros inclui uma ou mais restrições sobre a utilização da chave; e

fornecer acesso a um ou mais recursos de computação é realizado de acordo com as uma ou mais restrições.

Cláusula 15. O método implementado por computador da cláusula 14, em que a chave é com base pelo menos em parte no resultado da entrada da credencial secreta em uma função.

Cláusula 16. Um meio de armazenamento legível por computador, não transitório tendo armazenado nele instruções que, quando executadas por um computador, fazem com que o sistema de computador pelo menos:

obtenha uma chave intermediária, que é derivado a partir de pelo menos uma credencial secreta e um ou mais parâmetros de utilização do intermediário cha-

ve;

aplique, com base pelo menos em parte na chave intermediária obtida pelo menos uma porção de um processo de geração de uma assinatura que resulta em uma assinatura para uma mensagem, o processo de geração de uma assinatura configurado de tal modo que a assinatura é indeterminável, pelo processo de geração de uma assinatura, a um dispositivo de computação com a mensagem, a credencial secreta, e a assinatura, mas sem um ou mais restrições, e

fornecer a mensagem, a assinatura, e os um ou mais parâmetros para um outro sistema de computador que está configurado para analisar, com base pelo menos em parte a um ou mais parâmetros e a mensagem, a assinatura para determinar se a assinatura é válida.

Cláusula 17. O meio de armazenamento legível por computador não transitório da cláusula 16, em que os um ou mais parâmetros codificam uma ou mais restrições sobre o uso da chave intermediária que são aplicadas pelo menos em parte por dito outro sistema de computador.

Cláusula 18. O meio de armazenamento legível por computador não transitório da cláusula 16, em que a uma ou mais restrições correspondem a pelo menos um de um período de tempo dentro do qual a chave intermediária é utilizável, em uma localização em que a chave intermediária é utilizável, e um ou mais serviços para os quais a chave intermediária é utilizável para obter acesso.

Cláusula 19. O meio de armazenamento legível por computador não transitório da cláusula 16, em que as instruções, quando executadas pelo sistema de computador, permitem que o sistema de computador gere a assinatura sem o sistema de computador com acesso à credencial secreta.

Cláusula 20. O meio de armazenamento legível por computador não transitório da cláusula 19, em que, tendo o conjunto de um ou mais parâmetros, a assinatura é determinável pelo processo de geração de uma assinatura utilizando a creden-

cial secreta compartilhada, ou a chave intermediária.

Cláusula 21. O Meio de armazenamento não transitório legível por computador da cláusula 19, em que a obtenção da chave intermediária inclui a realização de um algoritmo, em que pelo menos uma saída de uma função hash é entrada, com pelo menos um dos parâmetros, na função hash.

Cláusula 22. Um sistema de computador, que compreende:

um ou mais processadores, e

memória incluindo instruções que, quando executadas por um ou mais processadores de um sistema de computador, fazem com que o sistema de computador para, pelo menos:

receba uma ou mais comunicações eletrônicas que codificam coletivamente uma mensagem, uma assinatura para a mensagem, e um ou mais parâmetros, sendo a assinatura gerada com base pelo menos em parte na credencial secreta e os um ou mais parâmetros;

analise, com base pelo menos em parte de um ou mais parâmetros, uma credencial intermediária derivada de pelo menos uma porção de um ou mais parâmetros e a credencial secreta, mas sem a credencial secreta, a mensagem e uma assinatura para determinar se a assinatura é válida, e

tenha uma ou mais ações contingentes sobre a determinação de que a assinatura é válida.

Cláusula 23. O sistema de computador da cláusula 22, em que:

a memória e um ou mais processadores são parte de um primeiro sistema de servidor em uma primeira localização geográfica;

o sistema de computador compreende um segundo sistema de servidor em uma segunda localização geográfica, o segundo sistema de servidor sendo configurado para gerar, com base pelo menos em parte na credencial secreta, uma assinatura diferente;

o primeiro sistema de servidor e o segundo sistema de servidor ambos não têm credencial secreta;

analisar a mensagem e uma assinatura inclui a introdução de uma função em que pelo menos uma porção de um ou mais parâmetros e a credencial de intermediário, e

o primeiro sistema de servidor e o segundo sistema de servidor de cada não têm informação a partir da qual uma mesma assinatura pode ser gerada, usando a função, a partir da mensagem.

Cláusula 24. O sistema de computador da cláusula 22, em que:

o sistema de computador corresponde a um serviço; e

uma ou mais ações incluem fornecer acesso ao serviço.

Cláusula 25. O sistema de computador da cláusula 24, em que o um ou mais limites de parâmetros usam a credencial intermediária para usar no acesso ao serviço.

Cláusula 26. O sistema de computador da cláusula 22, em que:

analisar a mensagem e uma assinatura inclui aplicar uma função hash para a credencial intermédia;

os um ou mais parâmetros incluem várias restrições sobre o uso da credencial intermediária, e

em que o sistema de computador está configurado para aplicar as restrições.

Cláusula 27. O sistema de computador da cláusula 22, em que:

analisar a mensagem e uma assinatura inclui aplicar uma função hash para uma chave que é derivada da credencial secreta, e

as instruções, quando executadas por um ou mais processadores do sistema de computador, fazem com que o sistema de computador, receba ainda a chave derivada a partir de um sistema de computador de autoridade chave.

Cláusula 28. O sistema de computador da cláusula 27, em que as instruções

que fazem com que o sistema de computador ainda receba a chave derivada a partir do sistema de computador de autoridade chave fazem com que o sistema de computador receba a chave derivada a partir do sistema de computador de autoridade chave antes da recepção da mensagem.

Cláusula 29. O sistema de computador da cláusula 22, em que a credencial intermédia é determinada por outro sistema de computador diferente do sistema de computador.

[0116] As várias modalidades podem ainda ser implementadas em uma ampla variedade de ambientes operacionais, o que em alguns casos pode incluir um ou mais computadores de usuário, dispositivos de computação, ou dispositivos de processamento que podem ser utilizados para operar qualquer um de uma série de aplicativos. Dispositivos de usuário ou cliente podem incluir qualquer um de uma série de computadores pessoais de uso geral, como computadores desktop ou laptop executando um sistema operacional padrão, bem como celular, sem fio, e dispositivos portáteis que executam o software móvel e são capazes de suportar um número de rede e protocolos de mensagens. Dito um sistema pode também incluir certo número de estações de trabalho com qualquer um de uma variedade de sistemas operacionais comercialmente disponíveis e outros aplicativos conhecidos para fins como desenvolvimento e gestão de base de dados. Estes dispositivos podem também incluir outros dispositivos eletrônicos, como terminais simulados, aplicativos para clientes, sistemas de jogos e outros dispositivos capazes de se comunicar através de uma rede.

[0117] A maioria das modalidades utiliza pelo menos uma rede que seria familiar para os especialistas na técnica para suportar comunicações utilizando qualquer um de uma variedade de protocolos comercialmente disponíveis, como o TCP/IP, OSI, FTP, UPnP, NFS, CIFS e AppleTalk. A rede pode ser, por exemplo, uma rede de área local, uma rede de área ampla, uma rede privada virtual, a Inter-

net, uma intranet, extranet, uma rede telefônica pública comutada, uma rede de infravermelho, uma rede sem fio e, em qualquer combinação.

[0118] Em modalidades que utilizam um servidor Web, o servidor Web pode executar qualquer um de uma variedade de aplicativos de servidor ou de médio porte, incluindo servidores HTTP, servidores FTP, servidores CGI, servidores de dados, servidores de Java e servidores de aplicativos de negócios. Os servidores também podem ser capazes de executar programas ou scripts em solicitações de resposta dos dispositivos de usuário, como pela execução de um ou mais aplicativos Web que podem ser implementados como um ou mais scripts ou programas escritos em qualquer linguagem de programação, como Java®, C, C# ou C++ ou qualquer linguagem de script, como Perl, Python ou TCL, bem como combinações dos mesmos. Os servidores podem também incluir os servidores de banco de dados, incluindo, entre outros, aqueles comercialmente disponíveis a partir de Oracle®, Microsoft®, Sybase® e IBM®.

[0119] O ambiente pode incluir uma variedade de armazenamento de dados e outros meios de memória e de armazenamento, como discutido acima. Estes podem residir em vários locais, como em um meio de armazenamento local (e/ou residente em) um ou mais computadores remotos, ou a partir de qualquer um ou todos os computadores da rede. Em um conjunto particular de modalidades, a informação pode residir em uma rede de área de armazenamento (“SAN”) familiar aos especialistas na técnica. Do mesmo modo, todos os arquivos necessários para desempenhar as funções atribuídas aos computadores, servidores ou outros dispositivos de rede podem ser armazenados localmente e/ou remotamente, como apropriado. Onde um sistema inclui dispositivos computadorizados, cada dito dispositivo pode incluir elementos de hardware que podem ser acoplados eletricamente através de um bus, os elementos, incluindo, por exemplo, pelo menos uma unidade central de processamento (CPU), pelo menos um dispositivo de entrada (por exemplo, um mouse,

teclado, touchscreen ou teclado), e pelo menos um dispositivo de saída (por exemplo, um dispositivo de vídeo, impressora, ou alto-falante). Esse sistema também pode incluir um ou mais dispositivos de armazenamento, como discos rígidos, dispositivos de armazenamento óptico e dispositivos de armazenamento de estado sólido, como a memória de acesso aleatório (“RAM”) ou uma memória somente leitura (“ROM”), bem como dispositivos de mídia removível, como, cartões de memória, cartões de memória flash, etc.

[0120] Ditos dispositivos também pode incluir um leitor de mídia de armazenamento lido por computador, um dispositivo de comunicação (por exemplo, um modem, uma placa de rede (com ou sem fios), um dispositivo de comunicação de infravermelhos, etc.), e a memória de trabalho, como descrito acima. O leitor de mídia de armazenamento lido por computador pode ser conectado com, ou configurado para receber, um meio de armazenamento legível por computador, o que dispositivos de armazenamento representa remoto, local, fixo, e/ou removível, bem como mídia de armazenamento para temporariamente e/ou de mais permanentemente contendo armazenamento, transmissão e recuperação de informações legível por computador. O sistema e vários dispositivos também normalmente incluem um número de aplicações de software, módulos, serviços ou outros elementos localizados dentro de pelo menos um dispositivo de memória de trabalho, incluindo um sistema operacional e programas de aplicativos, como um aplicativo cliente ou navegador. Deve-se notar que modalidades alternativas podem ter numerosas variações do que foi descrito acima. Por exemplo, o hardware personalizado pode também ser utilizado e/ou elementos particulares podem ser implementados em hardware, software (incluindo software portátil, como applets), ou ambos. Além disso, a ligação a outros dispositivos de computação, como os dispositivos de entrada/saída de rede pode ser empregue.

[0121] Mídia de armazenamento e mídia lida por computador contendo códi-

go, ou contendo porções de código, podem incluir quaisquer meios de comunicação apropriados conhecidos ou utilizados na técnica, incluindo mídias de armazenamento e mídias de comunicação, como, entre outros, mídias voláteis e não voláteis, removíveis e não removíveis implementadas em qualquer método ou tecnologia para o armazenamento e/ou a transmissão de informações, como instruções legíveis por computador, estruturas de dados, módulos de programas ou outros dados, incluindo RAM, ROM, EEPROM, memória flash ou outra tecnologia de memória, CD-ROM, disco digitais versáteis (DVD) ou outro armazenamento óptico, cassetes magnéticas, fita magnética, disco magnético de armazenamento ou outros dispositivos de armazenamento magnéticos, ou qualquer outra mídia que possa ser utilizada para armazenar a informação desejada e que pode ser acessada pelo dispositivo de um sistema. Com base na divulgação e nos ensinamentos aqui fornecidos, um especialista na técnica irá apreciar outras formas e/ou métodos para implementar as várias modalidades.

[0122] O relatório descritivo e os desenhos são, assim, considerados, em um exemplo ilustrativo em vez de em um sentido restritivo. Será, no entanto, evidente que várias modificações e alterações podem ser feitas para isso, sem se afastar do espírito e amplo escopo da invenção conforme definido nas reivindicações.

[0123] Outras variações estão dentro do espírito da presente divulgação. Assim, enquanto as técnicas descritas são susceptíveis a várias modificações e construções alternativas, certas modalidades ilustradas do mesmo são mostradas nos desenhos e tenham sido descritas acima em detalhe. Deve ser entendido, contudo, que não há intenção de limitar a invenção à forma ou formas específicas divulgadas, mas, pelo contrário, a intenção é cobrir todas as modificações, construções alternativas e equivalentes que estão dentro do espírito e do escopo da invenção, como definido nas reivindicações anexas.

[0124] O uso dos termos “um” e “uma” e “o/a” e semelhantes referentes no

contexto da descrição das modalidades descritas (em especial no contexto das seguintes reivindicações) deve ser interpretado como incluindo o singular e o plural, salvo se indicado aqui ou claramente contradito pelo contexto. Os termos “compreendendo”, “tendo”, “incluindo”, e “contendo” devem ser interpretados como termos abertos (isto é, que significa “incluindo, entre outros”), salvo se indicado de outra forma. O termo “ligado” deve ser interpretado como parcial ou totalmente contido em, ligado a, ou unidas entre si, mesmo que haja algo intervindo. A menção de faixas de valores aqui apresentadas destinam-se meramente a servir como a um método abreviado para referir individualmente cada valor separado dentro do intervalo, salvo se de outro modo aqui indicado, e cada valor separado incorporado na especificação como se fosse aqui descrito individualmente. Todos os métodos aqui descritos podem ser realizados em qualquer ordem adequada, salvo se de outro modo aqui indicado ou de outro modo claramente contradito pelo contexto. O uso de qualquer e todos os exemplos, ou linguagem exemplificativa (por exemplo, “como”) fornecidos aqui, pretende apenas melhor iluminar as modalidades da invenção e não constituem uma limitação no escopo da invenção salvo se de outro modo reivindicado. Nenhuma linguagem na especificação deve ser entendida como indicando qualquer elemento não reivindicado como essencial para a prática da invenção.

[0125] Modalidades preferidas da presente divulgação são aqui descritas, incluindo o melhor modo conhecido pelos inventores para realizar a invenção. Variações das modalidades preferenciais podem tornar-se evidentes para os especialistas na técnica após a leitura da descrição anterior. Os inventores esperam que especialistas na técnica empreguem ditas variações, conforme o caso, e os inventores pretendem que a invenção seja praticada de modo diferente do aqui especificamente descrito. Assim, esta invenção inclui todas as modificações e equivalentes do assunto mencionado nas reivindicações em anexo, conforme permitido pela lei aplicável. Além disso, qualquer combinação dos elementos acima descritos em todas as varia-

ções possíveis dos mesmos é incluída pela invenção salvo se de outra forma aqui indicado ou de outra forma claramente contrariado pelo contexto.

[0126] Todas as referências, incluindo as publicações, pedidos de patentes e patentes aqui citadas são aqui incorporadas por referência na mesma extensão como se cada referência fosse individual e especificamente indicada para ser incorporada por referência e fosse estabelecida na sua totalidade aqui.

REIVINDICAÇÕES

1. Método implementado por computador para determinar se deve ser concedido um acesso solicitado a um ou mais recursos de computação, **CARACTERIZADO** pelo fato de que compreende:

sob o controle de um ou mais sistemas de computação configurado com instruções executáveis,

receber (2104), a partir de uma parte autenticadora, informação eletrônica codificando uma mensagem, uma assinatura para a mensagem, e um conjunto de uma ou mais restrições sobre chaves derivadas a partir de uma credencial secreta compartilhada com a parte autenticadora, sendo a assinatura determinável pela aplicação de uma função código de autenticação de mensagem com base em hash para a mensagem, a credencial secreta, e o conjunto de uma ou mais restrições, mas também sendo indeterminável tendo apenas a função código de autenticação de mensagem com base em hash, mas sem ter o conjunto de uma ou mais restrições;

obter (2102) uma chave gerada por pelo menos aplicar a função código de autenticação de mensagem com base em hash à credencial secreta e pelo menos um subconjunto do conjunto de uma ou mais restrições;

calcular (2108), por o um ou mais sistemas de computação, uma assinatura de referência por pelo menos aplicar a função código de autenticação de mensagem à base de hash a pelo menos a chave obtida e a mensagem; e

fornecer (2114) acesso a um ou mais recursos de computação quando a assinatura de referência calculada é equivalente à assinatura recebida.

2. Método implementado por computador de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que:

a mensagem compreende uma solicitação para acesso a um ou mais recursos de computação;

o método compreende ainda determinar se o conjunto de uma ou mais restrições indica que a solicitação deve ser atendida; e

fornecer acesso ao um ou mais recursos de computação é condicionado à determinar que as restrições indicam que a solicitação deve ser atendida.

3. Método implementado por computador de acordo com a reivindicação 2, **CARACTERIZADO** pelo fato de que a informação que codifica o conjunto de uma ou mais restrições é codificada por um documento e em que determinar se o conjunto de restrições indica que a solicitação deve ser atendida inclui avaliar o documento em relação a um contexto no qual a solicitação foi recebida.

4. Método implementado por computador de acordo com qualquer uma das reivindicações 1 a 3, **CARACTERIZADO** pelo fato de que:

a mensagem compreende uma solicitação para acesso a um recurso de computação do um ou mais recursos de computação;

a informação que codifica o conjunto de uma ou mais restrições inclui informação especificando o recurso de computação; e

fornecer acesso ao um ou mais recursos de computação inclui o fornecimento de acesso ao recurso de computação quando o recurso de computação corresponde ao recurso de computação especificado.

5. Método implementado por computador de acordo com qualquer uma das reivindicações 1 a 4, **CARACTERIZADO** pelo fato de que:

a informação que codifica o conjunto de uma ou mais restrições corresponde a um período de tempo para o qual a mensagem é válida; e

determinar se a assinatura é válida, é baseado, pelo menos em parte, em se a mensagem foi enviada durante o período de tempo correspondente.

6. Método implementado por computador de acordo com qualquer uma das reivindicações 1 a 5, **CARACTERIZADO** pelo fato de que:

a informação que codifica o conjunto de uma ou mais restrições corresponde a uma restrição baseada, pelo menos em parte, em uma localização; e

determinar se a assinatura é válida, é baseado, pelo menos em parte, em se uma localização de pelo menos um do um ou mais sistemas de computação corresponde à localização correspondente.

7. Método implementado por computador de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que a função código de autenticação de mensagem com base em hash é um código de autenticação de mensagem à base de *hash* (HMAC).

8. Método implementado por computador de acordo com a reivindicação 7, **CARACTERIZADO** pelo fato de que calcular a assinatura de referência inclui a entrada para a função tanto de uma saída da função como de uma restrição a partir do conjunto de uma ou mais restrições.

9. Meio de armazenamento não transitório legível por computador **CARACTERIZADO** por ter armazenado no mesmo, instruções que quando executadas por um sistema de computação, fazem com que o sistema de computação execute o método conforme definido em qualquer uma das reivindicações 1 a 8.

10. Sistema de computação, **CARACTERIZADO** por compreender:

um ou mais processadores; e

memória incluindo instruções que, quando executadas por um ou mais processadores do sistema de computação, fazem com que o sistema de computação execute o método conforme definido em qualquer uma das reivindicações 1 a 8.

11. Sistema de computação de acordo com a reivindicação 10, **CARACTERIZADO** pelo fato de que:

a memória e um ou mais processadores são parte de um primeiro sistema de servidor em uma primeira localização geográfica;

o sistema de computação compreende um segundo sistema de servidor em uma segunda localização geográfica, o segundo sistema de servidor sendo configurado para gerar, com base pelo menos em parte na credencial secreta, uma assinatura diferente;

o primeiro sistema de servidor e o segundo sistema de servidor são desprovidos de credencial secreta; e

o primeiro sistema de servidor e o segundo sistema de servidor são, cada um, desprovidos de informações a partir das quais uma mesma assinatura poderia ser gerada, usando a função, a partir da mensagem.

12. Sistema de computação de acordo com a reivindicação 10, **CARACTERIZADO** pelo fato de que a uma ou mais restrições limitam o uso da chave para usar no acesso ao serviço.

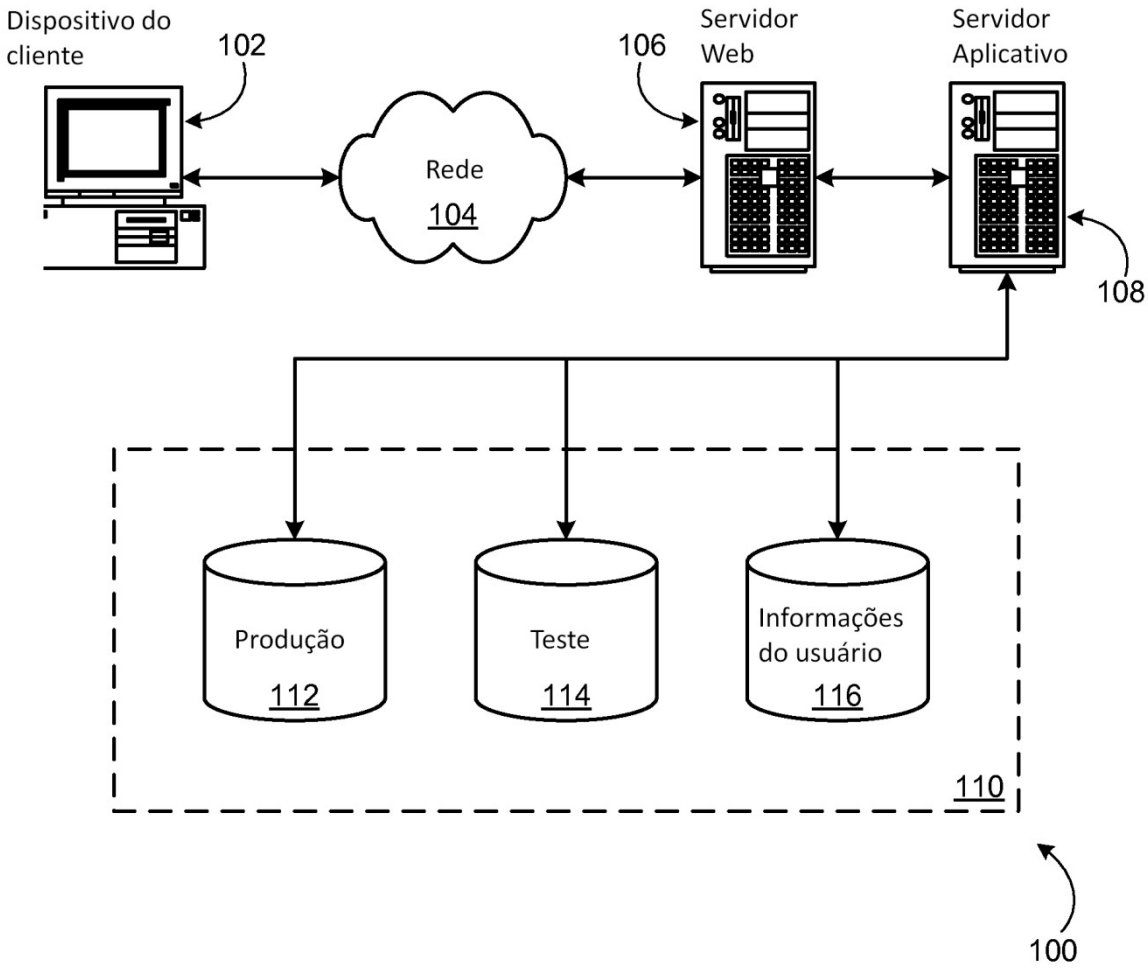

Dispositivo do cliente
102
Rede
104
106
Servidor Web
Servidor Aplicativo
108
Produção
112
Teste
114
Informações do usuário
116
110
100

Figura 1

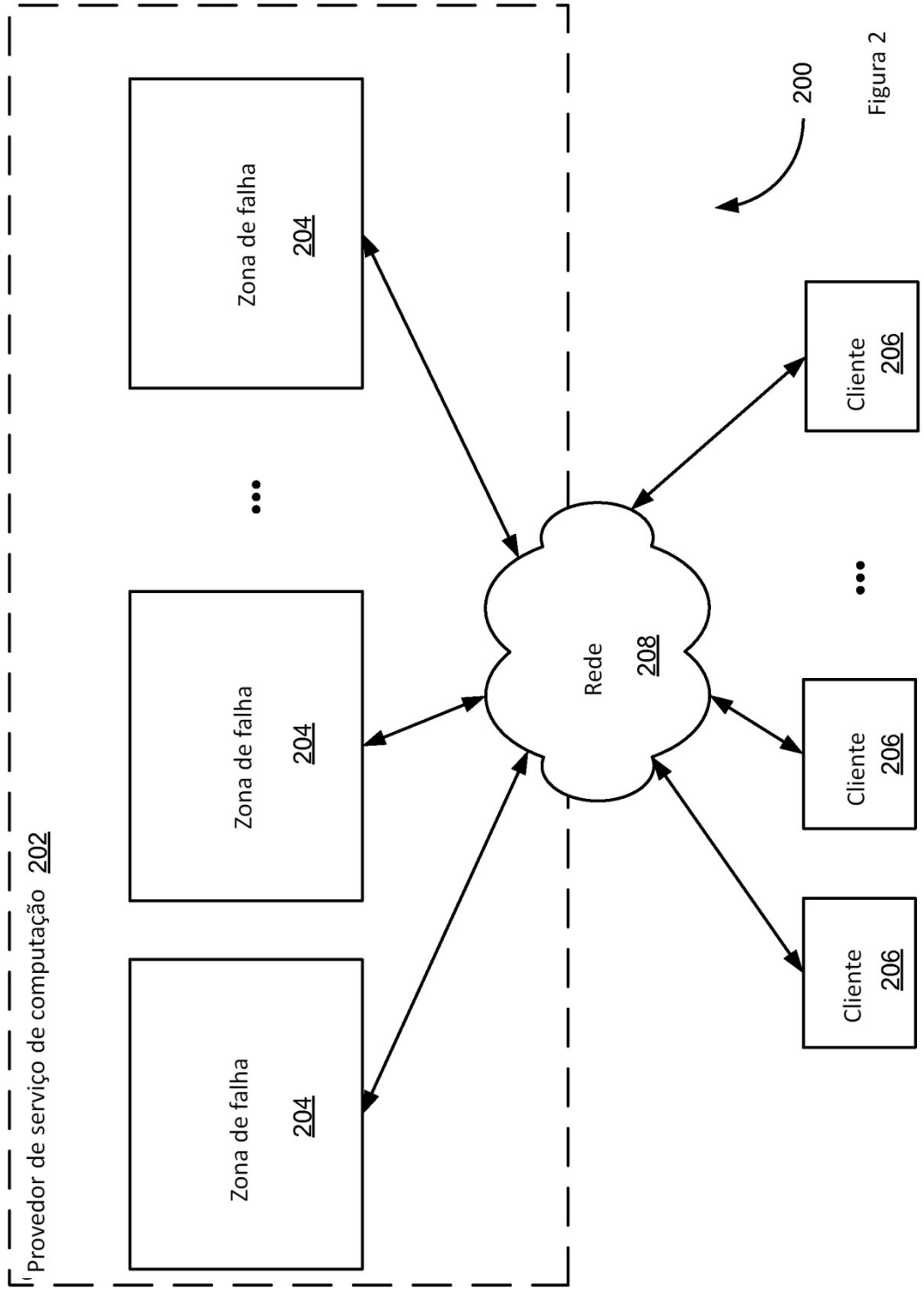

200
Provedor de serviço de computação 202
Zona de falha 204
Zona de falha 204
Zona de falha 204
Rede 208
Cliente 206
Cliente 206
Cliente 206

Figura 2

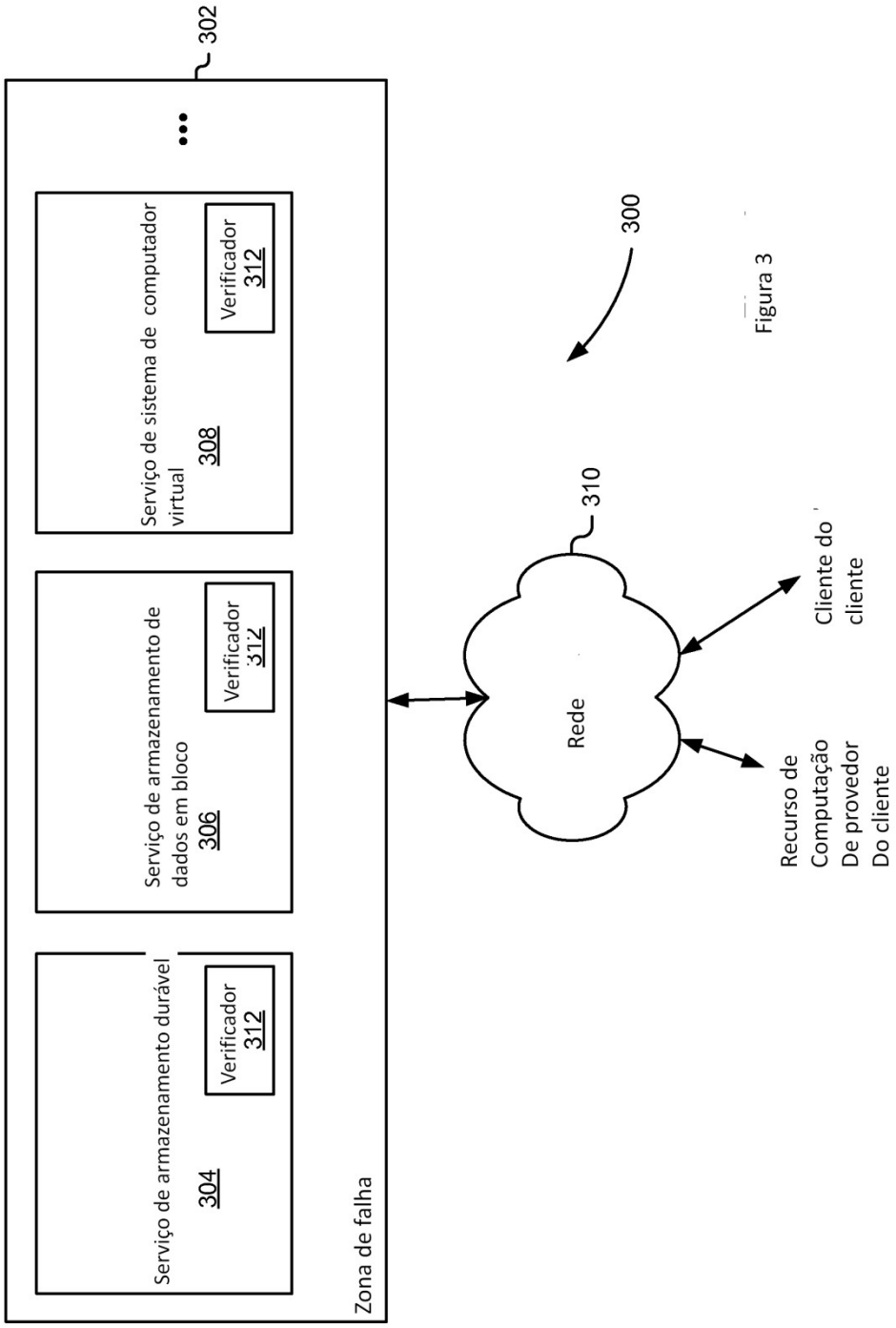

302
Serviço de sistema de computador virtual
308
Verificador
312
Serviço de armazenamento de dados em bloco
306
Verificador
312
Serviço de armazenamento durável
304
Verificador
312
Zona de falha
300
310
Rede
Cliente do cliente
Recurso de Computação De provedor Do cliente

Figura 3

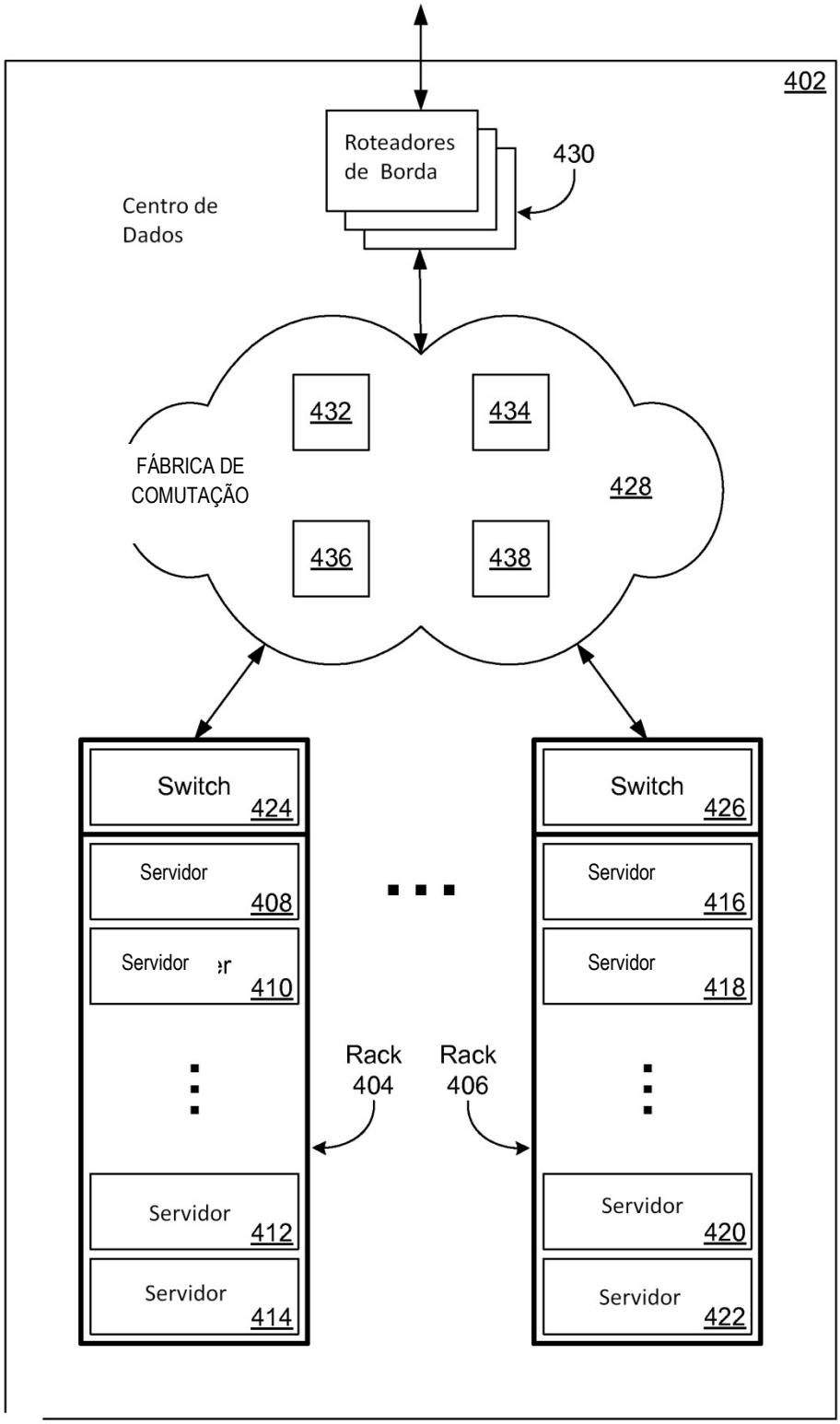

402
Roteadores de Borda
430
Centro de Dados
432
434
FÁBRICA DE COMUTAÇÃO
428
436
438
Switch 424
Servidor 408
Servidor 410
Servidor 412
Servidor 414
Switch 426
Servidor 416
Servidor 418
Servidor 420
Servidor 422
Rack 404
Rack 406

Figura 4

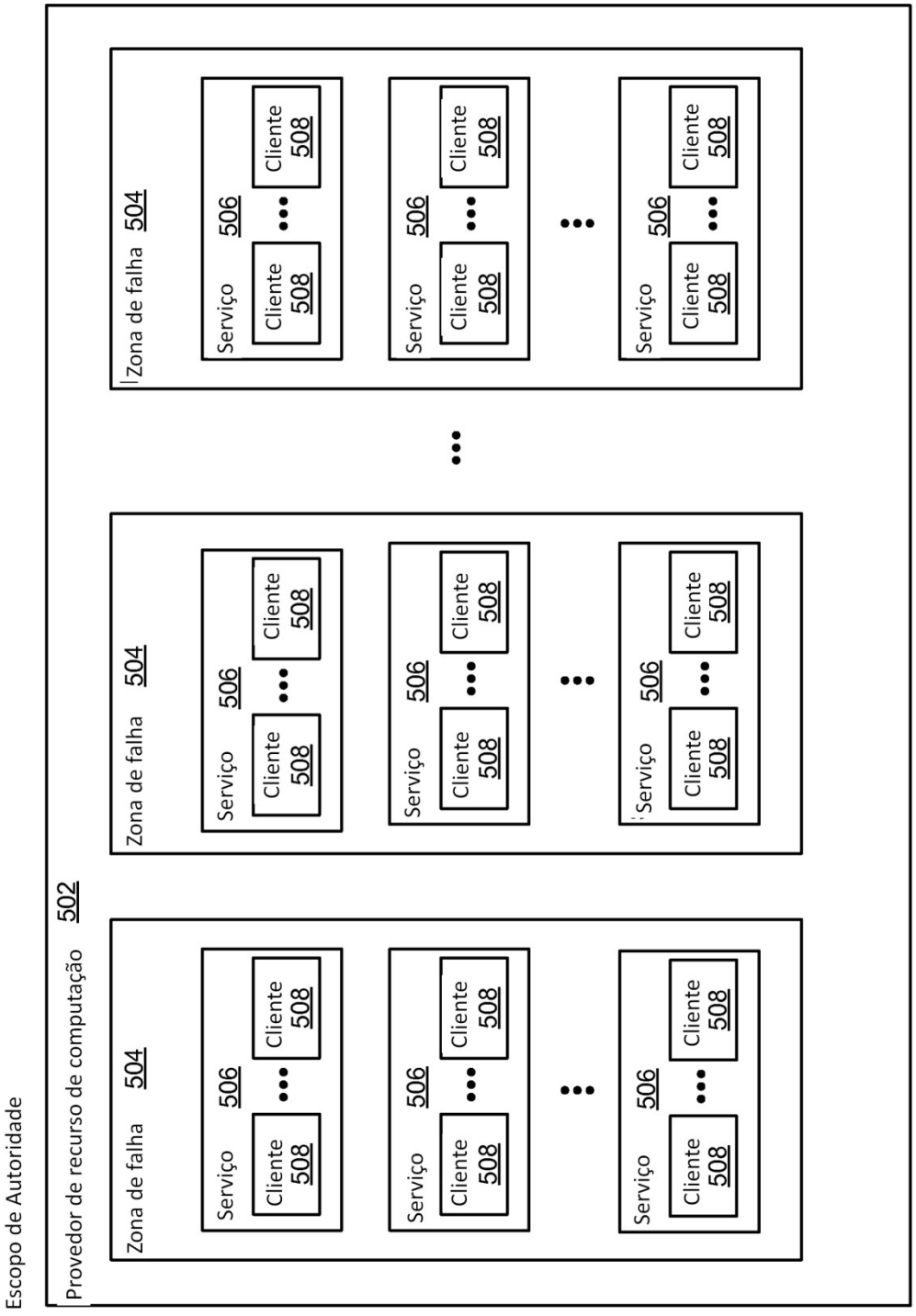

Escopo de Autoridade
Provedor de recurso de computação 502
Zona de falha 504
Serviço 506
Cliente 508

Figura 5

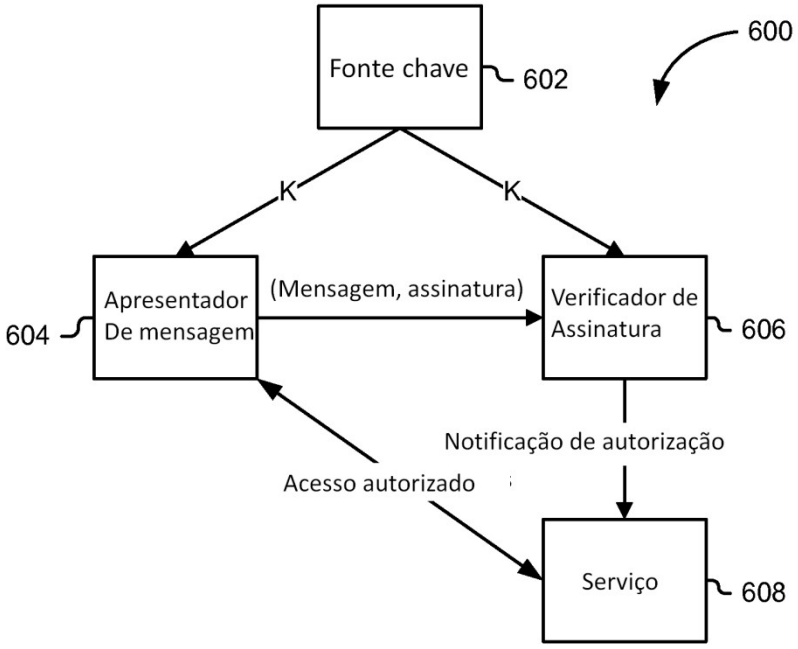

Fonte chave
602
600
K
K
Apresentador
De mensagem
604
(Mensagem, assinatura)
Verificador de
Assinatura
606
Notificação de autorização
Acesso autorizado
Serviço
608

Figura 6

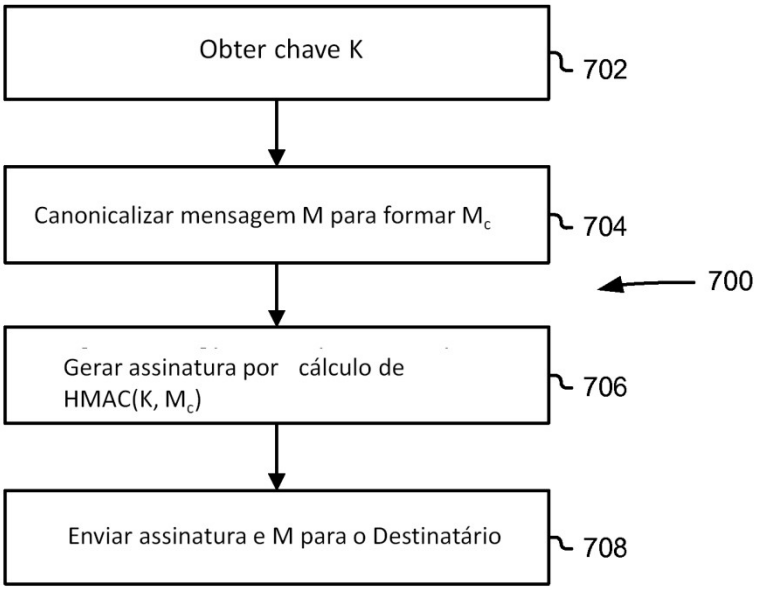

Obter chave K
702
Canonicalizar mensagem M para formar M_c
704
700
Gerar assinatura por cálculo de HMAC(K, M_c)
706
Enviar assinatura e M para o Destinatário
708

Figura 7

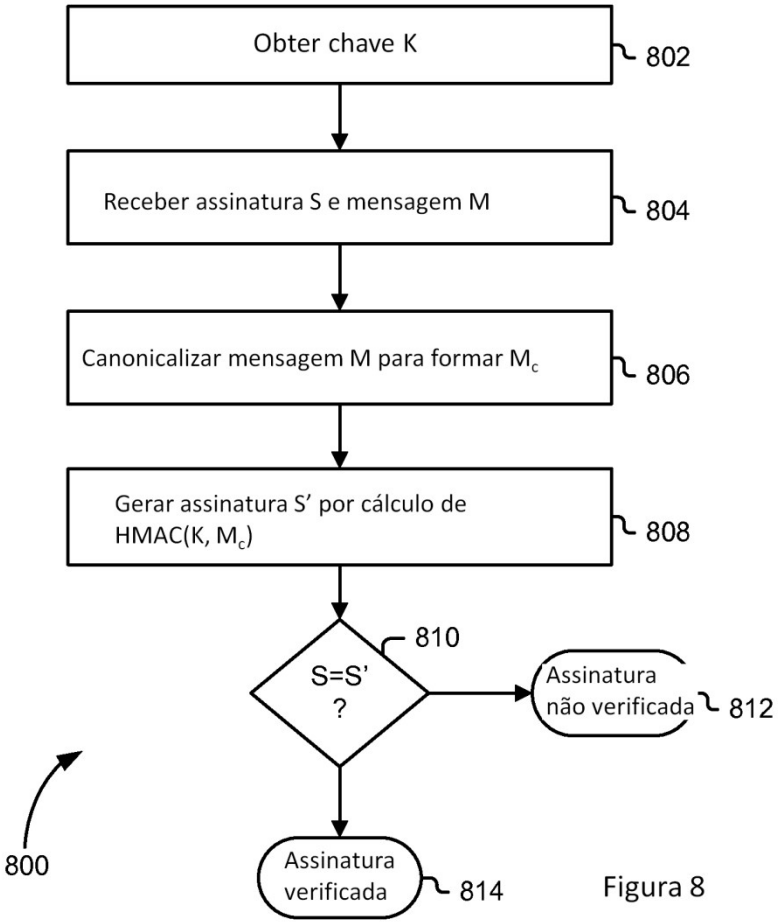

Obter chave K
802
Receber assinatura S e mensagem M
804
Canonicalizar mensagem M para formar M_c
806
Gerar assinatura S' por cálculo de HMAC(K, M_c)
808
810
S=S' ?
Assinatura não verificada
812
800
Assinatura verificada
814

Figura 8

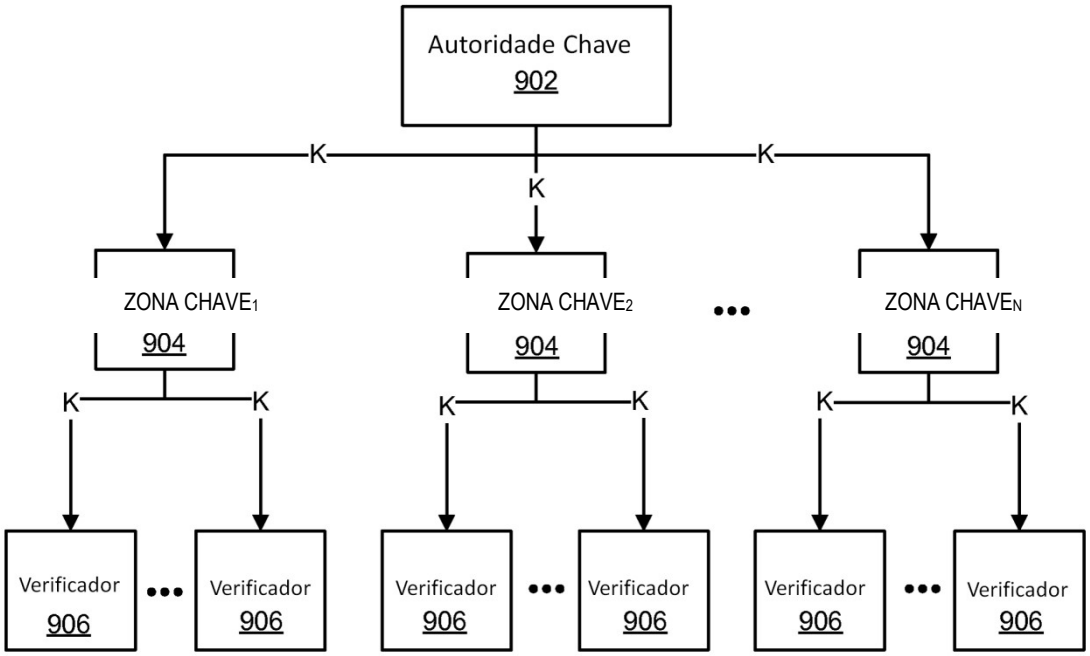

Autoridade Chave
902
K
K
K
ZONA CHAVE1
904
ZONA CHAVE2
904
ZONA CHAVEN
904
Verificador
906
Verificador
906
Verificador
906
Verificador
906
Verificador
906
Verificador
906
900

Figura 9

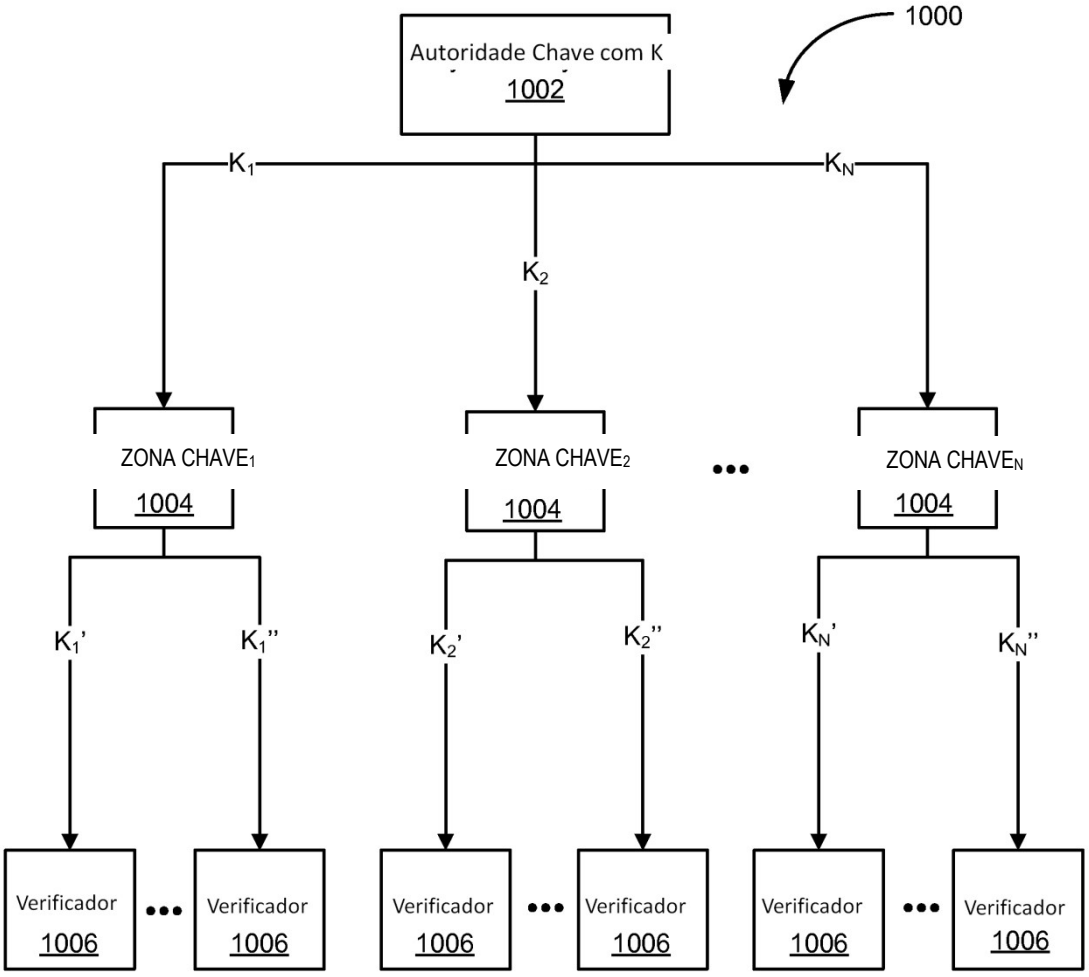

1000
Autoridade Chave com K
1002
K1
K2
KN
ZONA CHAVE1
1004
ZONA CHAVE2
1004
ZONA CHAVEN
1004
K1'
K1''
K2'
K2''
KN'
KN''
Verificador
1006
Verificador
1006
Verificador
1006
Verificador
1006
Verificador
1006
Verificador
1006

Figura 10

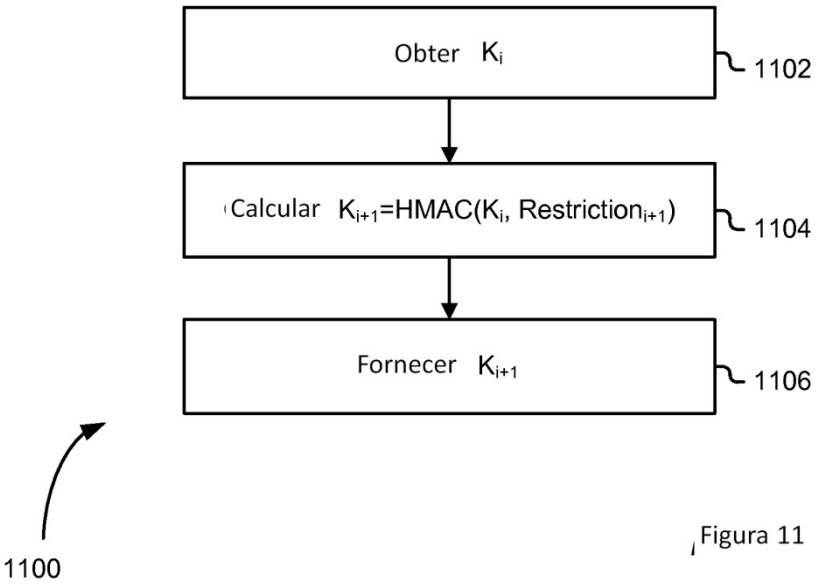

Obter K_i
1102
Calcular K_{i+1}=HMAC(K_i, Restriction$_{i+1}$)
1104
Fornecer K_{i+1}
1106
1100

Figura 11

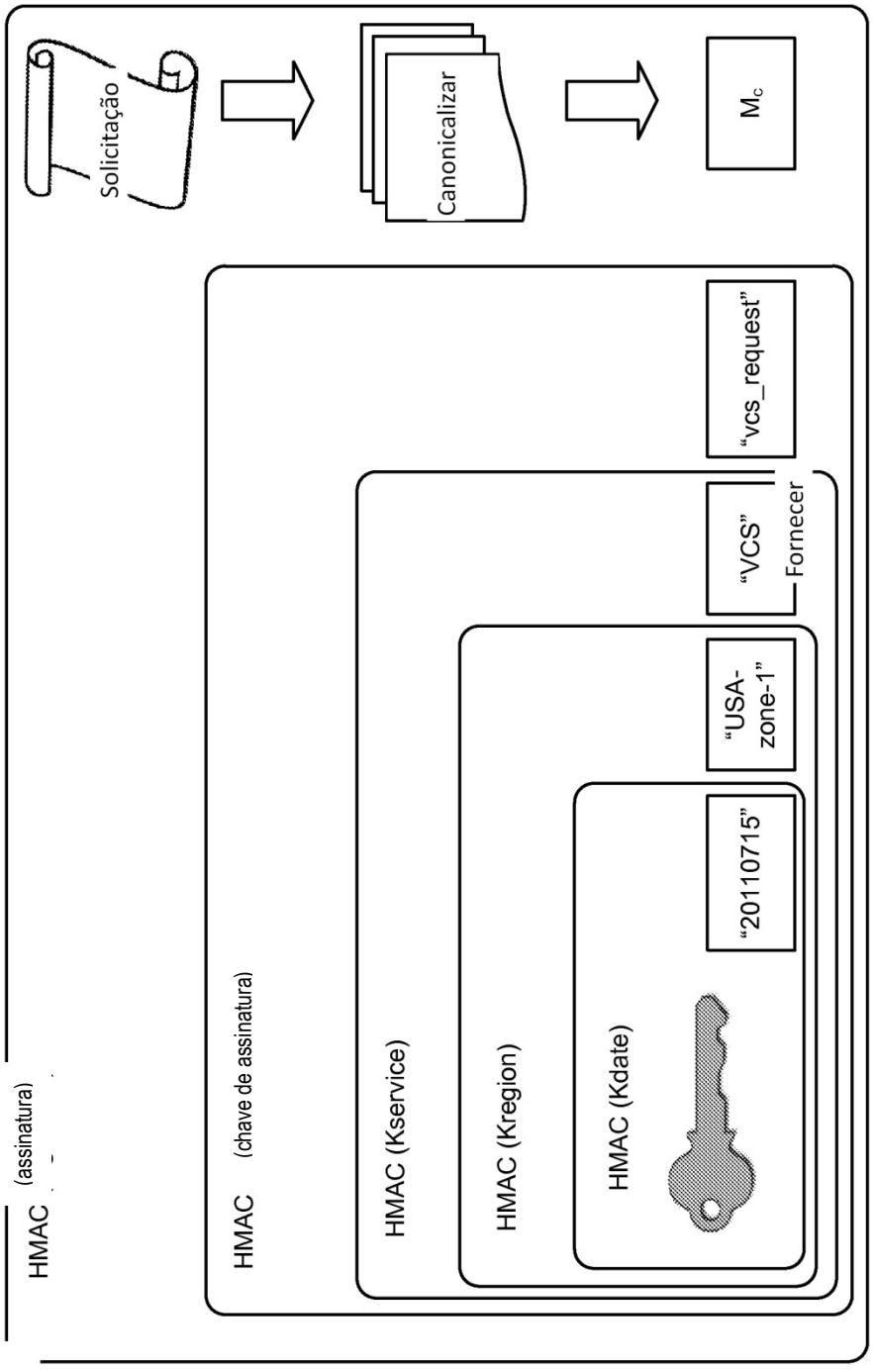

HMAC (assinatura)
Solicitação
Canonicalizar
M_C
HMAC (chave de assinatura)
HMAC (Kservice)
HMAC (Kregion)
HMAC (Kdate)
"20110715"
"USA-zone-1"
"VCS"
Fornecer
"vcs_request"
1200

Figura 12

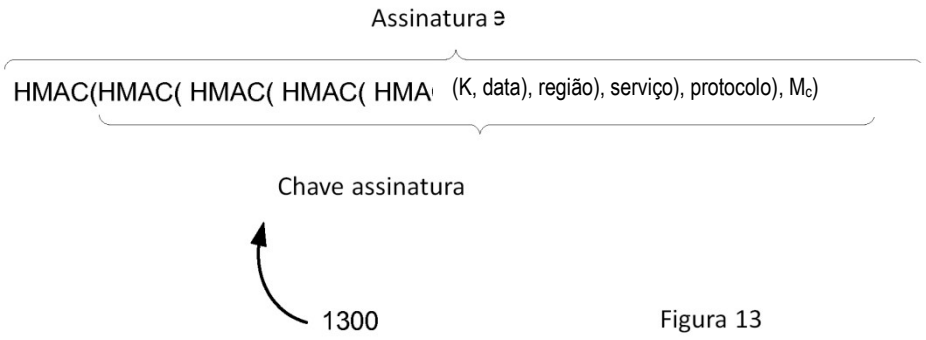
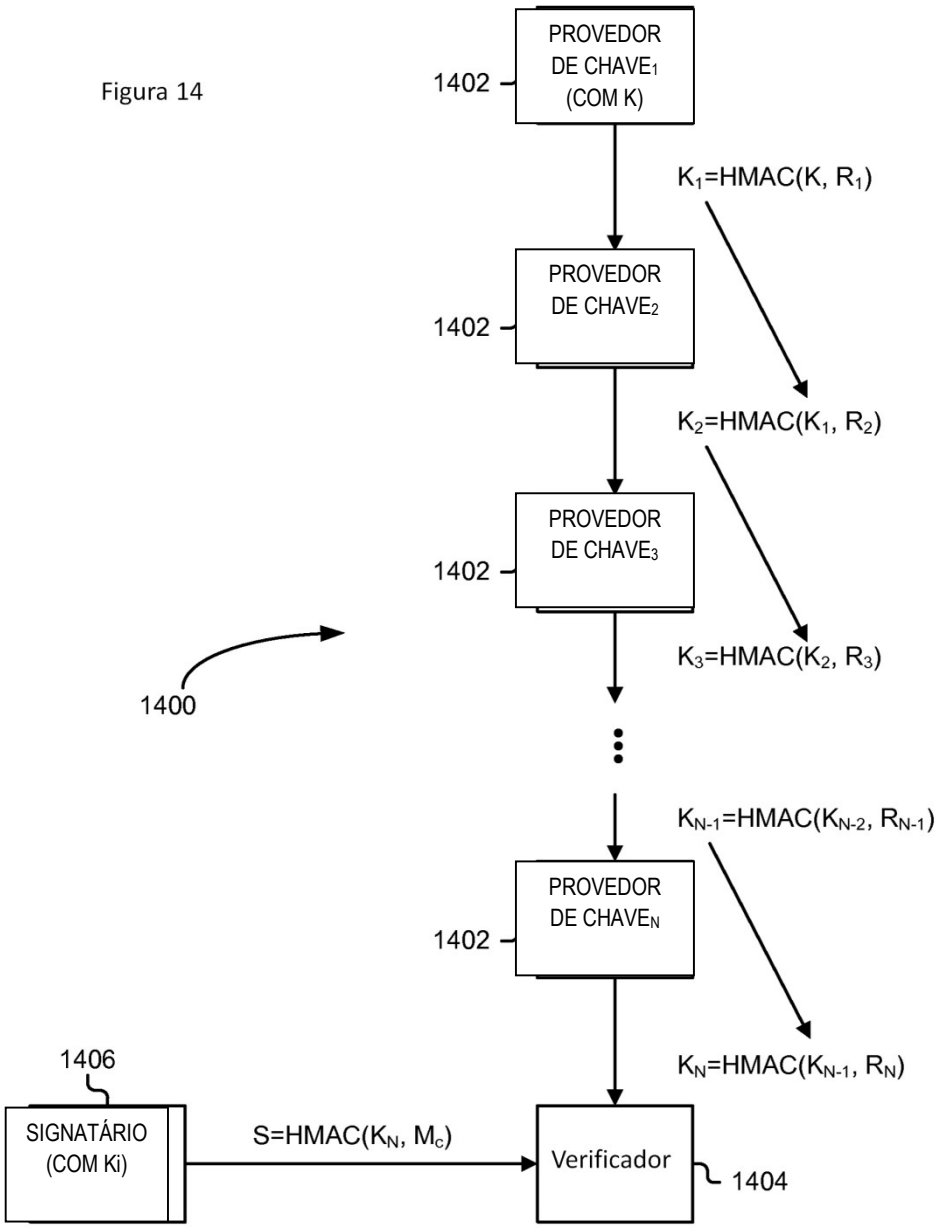

Assinatura ə
HMAC(HMAC(HMAC(HMAC(HMA (K, data), região), serviço), protocolo), Mc)
Chave assinatura
1300

Figura 13

Figura 14


PROVEDOR DE CHAVE1 (COM K)
1402
K1=HMAC(K, R1)
PROVEDOR DE CHAVE2
1402
K2=HMAC(K1, R2)
PROVEDOR DE CHAVE3
1402
K3=HMAC(K2, R3)
1400
KN-1=HMAC(KN-2, RN-1)
PROVEDOR DE CHAVEN
1402
KN=HMAC(KN-1, RN)
1406
SIGNATÁRIO (COM Ki)
S=HMAC(KN, Mc)
Verificador
1404

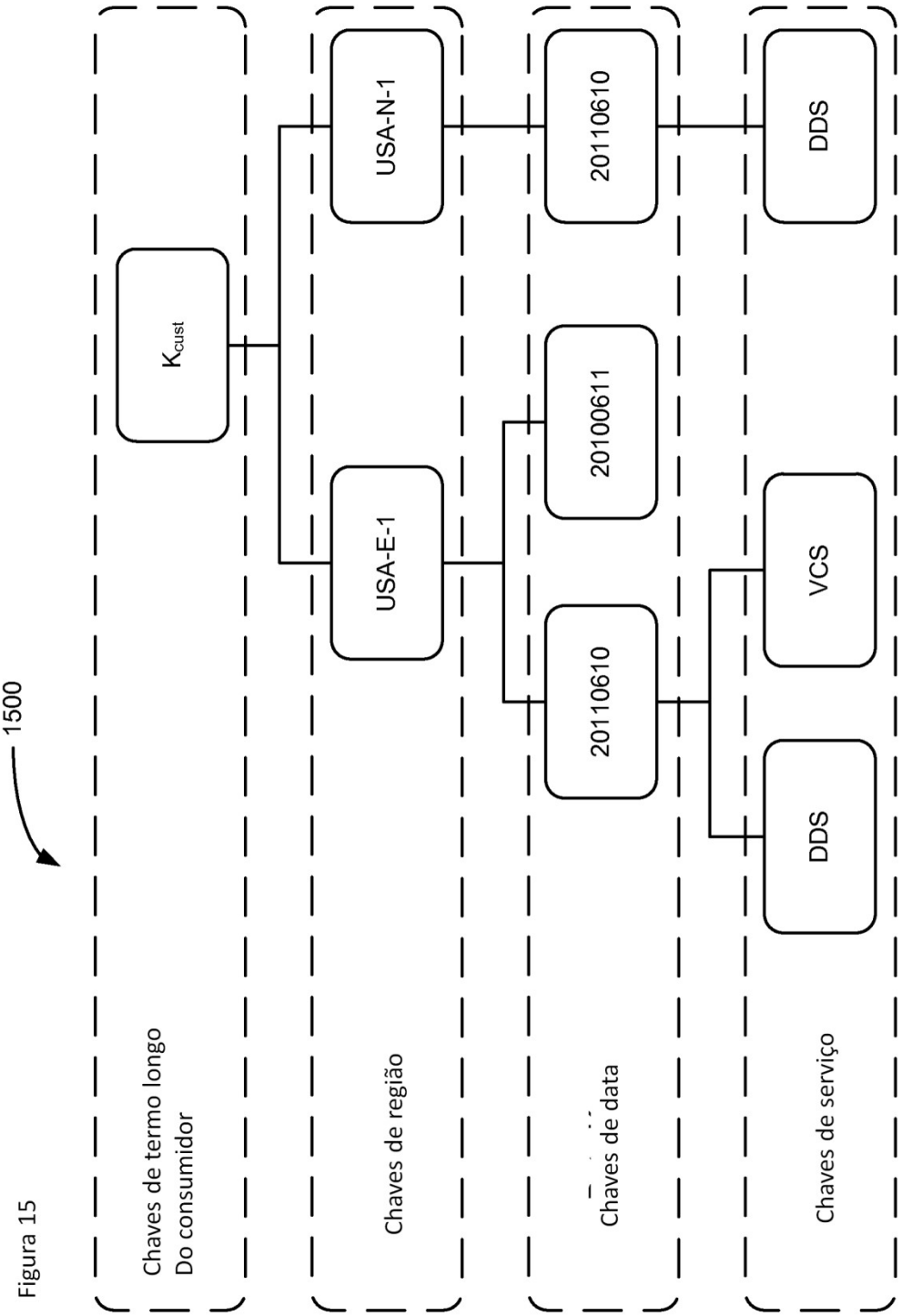

1500
Chaves de termo longo
Do consumidor
K_{cust}
Chaves de região
USA-N-1
USA-E-1
Chaves de data
20110610
20100611
20110610
Chaves de serviço
DDS
VCS
DDS

Figura 15

Figura 16

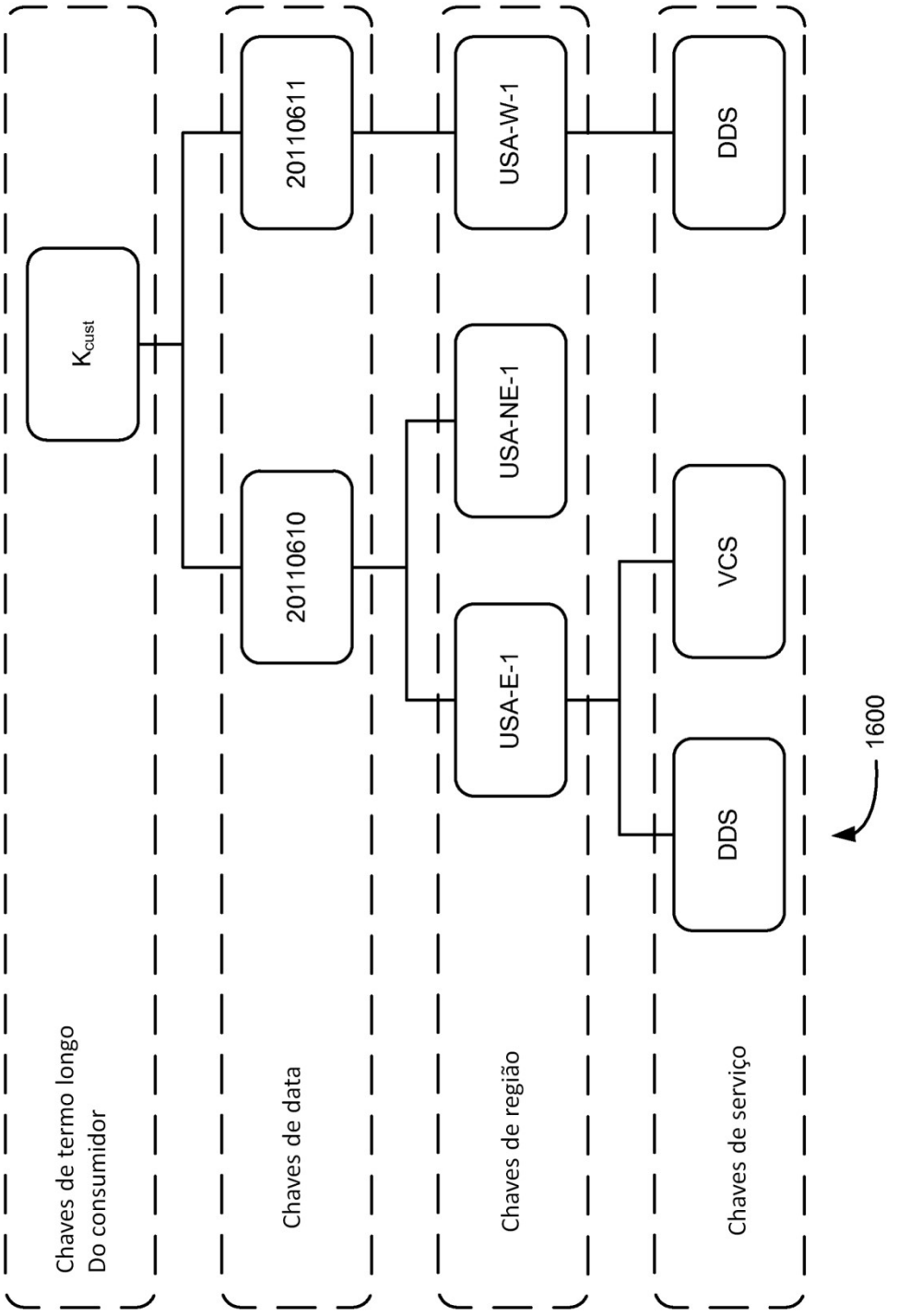
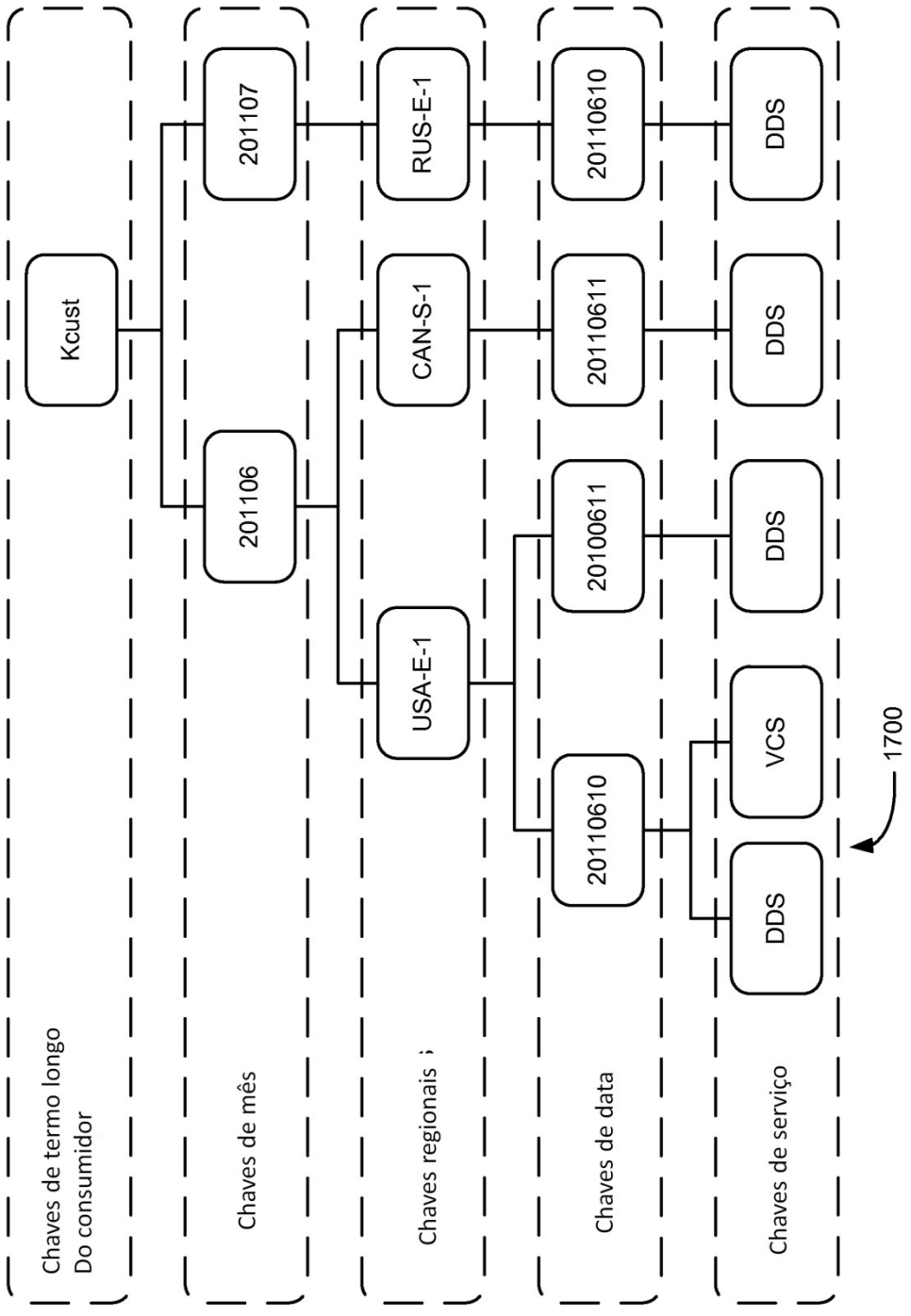

Chaves de termo longo
Do consumidor
K_{cust}
Chaves de data
20110611
20110610
Chaves de região
USA-W-1
USA-NE-1
USA-E-1
Chaves de serviço
DDS
VCS
DDS
1600

Figura 17


Chaves de termo longo
Do consumidor
Kcust
Chaves de mês
201106
201107
Chaves regionais
USA-E-1
CAN-S-1
RUS-E-1
Chaves de data
20110610
20100611
20110611
20110610
Chaves de serviço
DDS
VCS
DDS
DDS
DDS
1700

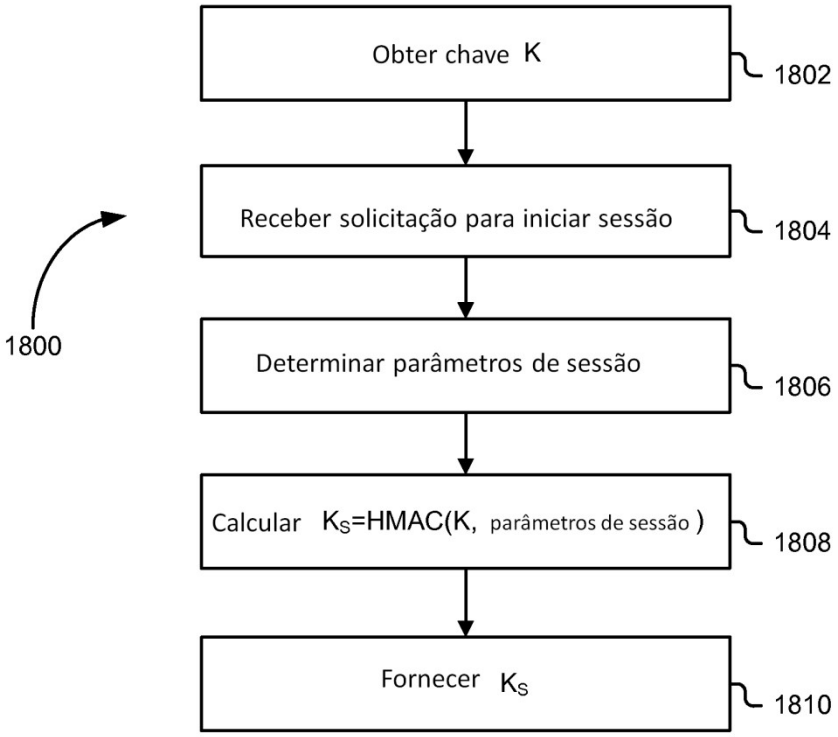

Obter chave K
1802
Receber solicitação para iniciar sessão
1804
Determinar parâmetros de sessão
1806
Calcular K_S=HMAC(K, parâmetros de sessão)
1808
Fornecer K_S
1810
1800

Figura 18

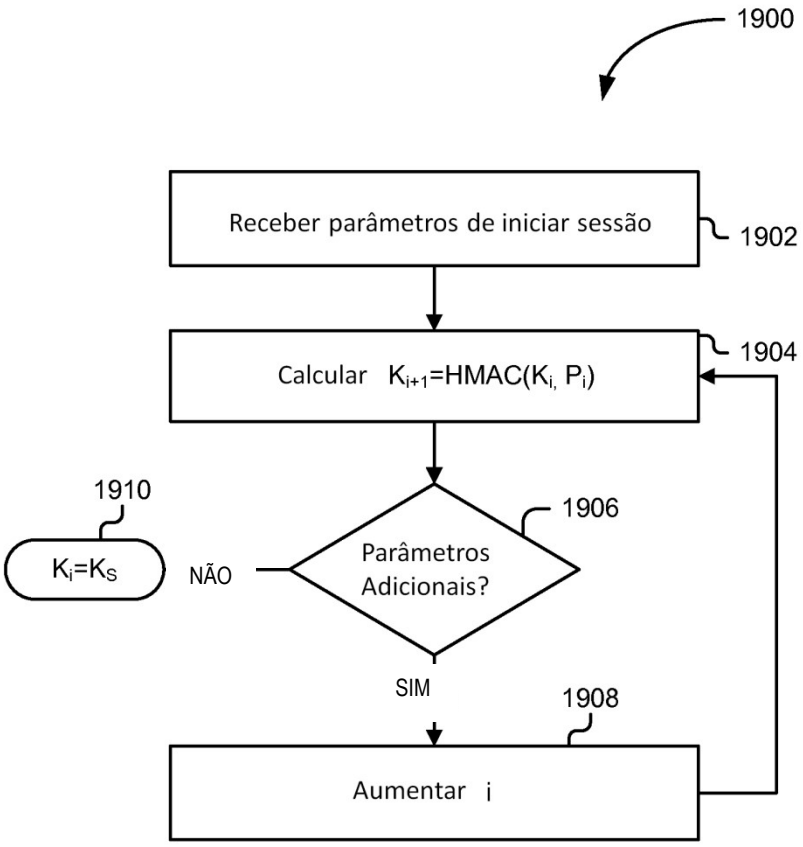

1900
Receber parâmetros de iniciar sessão
1902
Calcular K_{i+1}=HMAC(K_i, P_i)
1904
1910
K_i=K_S
NÃO
Parâmetros Adicionais?
1906
SIM
1908
Aumentar i

Figura 19

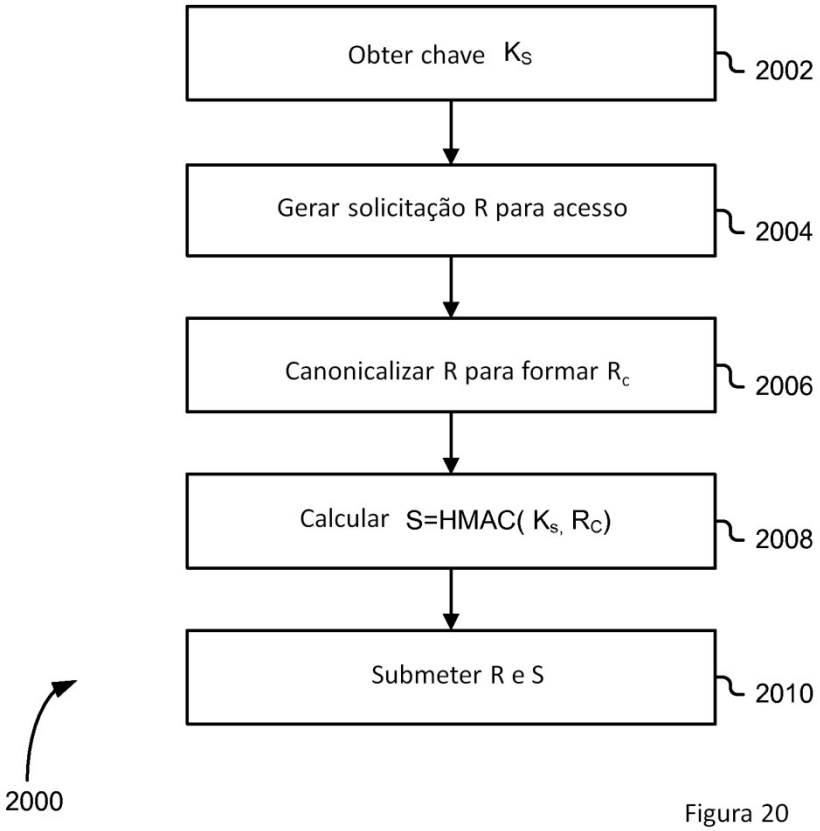

Obter chave K_S
2002
Gerar solicitação R para acesso
2004
Canonicalizar R para formar R_c
2006
Calcular $S=HMAC(K_s, R_C)$
2008
Submeter R e S
2010
2000

Figura 20

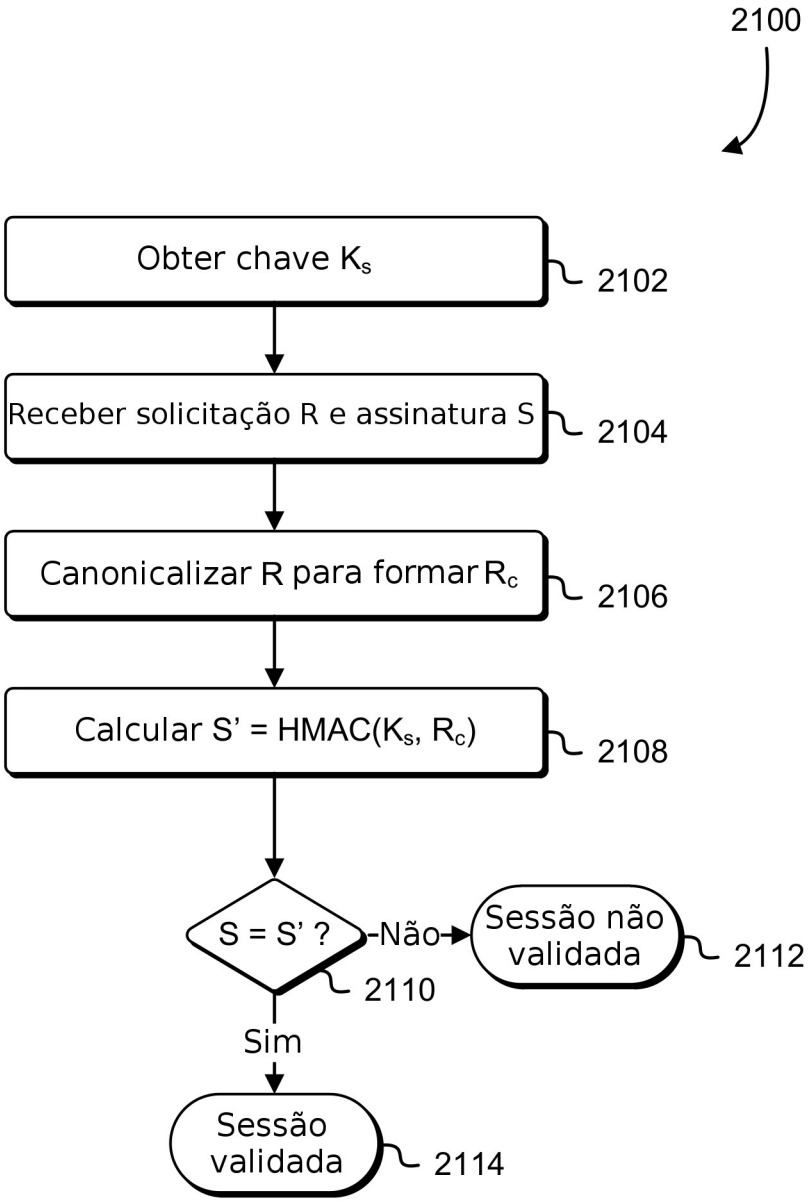

2100
Obter chave K_s
2102
Receber solicitação R e assinatura S
2104
Canonicalizar R para formar R_c
2106
Calcular S' = HMAC(K_s, R_c)
2108
S = S' ?
2110
Não
Sessão não validada
2112
Sim
Sessão validada
2114

Figura 21

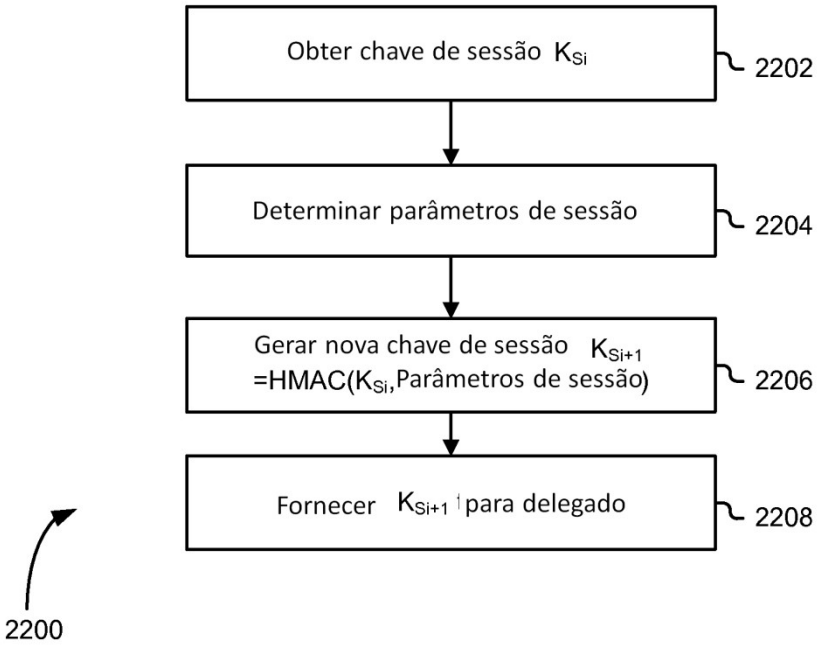

Obter chave de sessão K_{Si}
2202
Determinar parâmetros de sessão
2204
Gerar nova chave de sessão K_{Si+1} =HMAC(K_{Si},Parâmetros de sessão)
2206
Fornecer K_{Si+1} para delegado
2208
2200

Figura 22

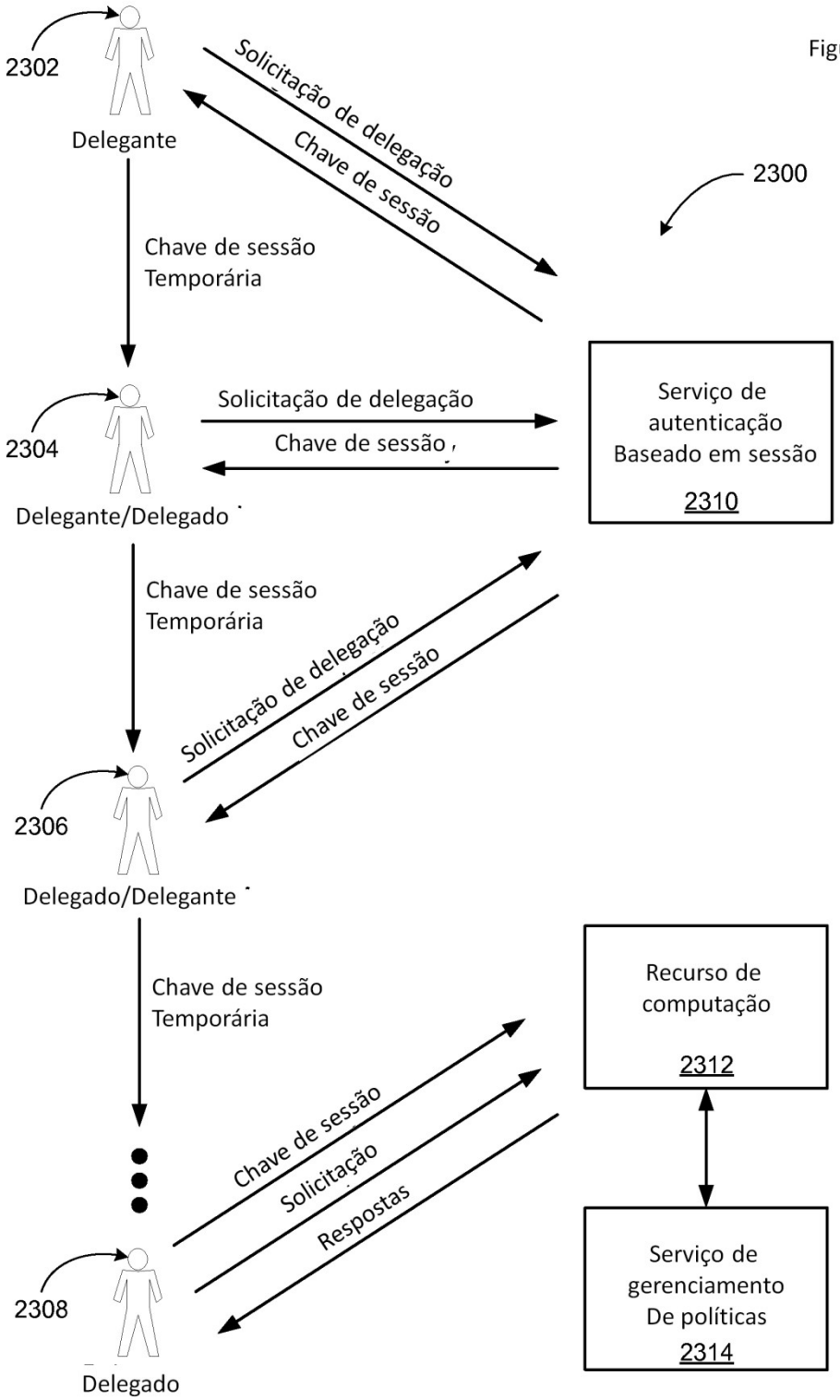

2302
Delegante
Solicitação de delegação
Chave de sessão
2300
Chave de sessão
Temporária
2304
Delegante/Delegado
Solicitação de delegação
Chave de sessão
Serviço de
autenticação
Baseado em sessão
2310
Chave de sessão
Temporária
Solicitação de delegação
Chave de sessão
2306
Delegado/Delegante
Chave de sessão
Temporária
Recurso de
computação
2312
Chave de sessão
Solicitação
Respostas
2308
Delegado
Serviço de
gerenciamento
De políticas
2314

Figura 23

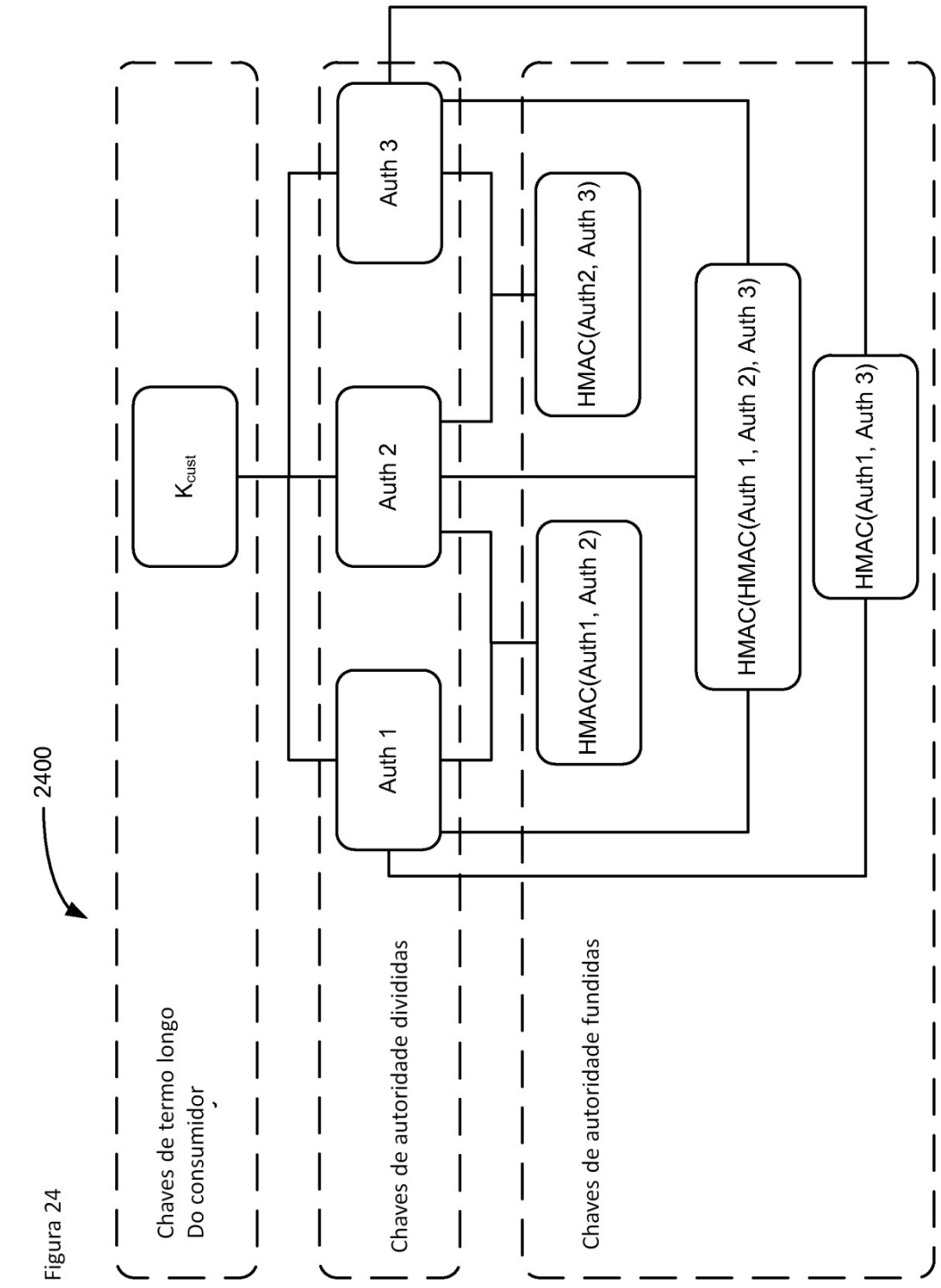

2400
Chaves de termo longo
Do consumidor
Chaves de autoridade divididas
Chaves de autoridade fundidas
K_{cust}
Auth 1
Auth 2
Auth 3
HMAC(Auth1, Auth 2)
HMAC(Auth2, Auth 3)
HMAC(HMAC(Auth 1, Auth 2), Auth 3)
HMAC(Auth1, Auth 3)

Figura 24