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

(11) BR 112019007571-2 B1

(22) Data do Depósito: 25/08/2017

(45) Data de Concessão: 06/12/2022

(54) Título: MÉTODO REALIZADO POR UM PRIMEIRO DISPOSITIVO CONFIGURADOR DE UMA REDE, PRIMEIRO DISPOSITIVO CONFIGURADOR E MEMÓRIA LEGÍVEL POR COMPUTADOR

(51) Int.Cl.: H04W 12/04; H04L 9/08.

(30) Prioridade Unionista: 12/07/2017 US 15/648,437; 19/10/2016 US 62/410,309.

(73) Titular(es): QUALCOMM INCORPORATED.

(72) Inventor(es): ROSARIO CAMMAROTA; JOUNI KALEVI MALINEN; PEERAPOL TINNAKORNSRISUPHAP.

(86) Pedido PCT: PCT US2017048560 de 25/08/2017

(87) Publicação PCT: WO 2018/075135 de 26/04/2018

(85) Data do Início da Fase Nacional: 15/04/2019

(57) Resumo: Esta divulgação fornece sistemas, métodos e aparelhos, incluindo programas de computador codificados em mídia de armazenamento de computador, para aprimorar um protocolo de provisionamento de dispositivo (DPP) para suportar múltiplos configuradores. Em um aspecto, um primeiro dispositivo configurador pode exportar um pacote de chave do configurador. Em um aspecto, o pacote de chave do configurador pode ser usado para backup e restauração das chaves do configurador. O pacote de chave do configurador pode incluir uma chave de assinatura privada do configurador e, opcionalmente, uma chave de verificação pública do configurador. Um segundo dispositivo configurador pode obter o pacote de chave do configurador e pode obter informações de descriptografia que podem ser usadas para descriptografar o pacote de chave do configurador. Assim, em outro aspecto, tanto o primeiro dispositivo configurador quanto o segundo dispositivo configurador podem usar as mesmas chaves do configurador com o protocolo de provisionamento de dispositivos para configurar os cadastros em uma rede.

“MÉTODO REALIZADO POR UM PRIMEIRO DISPOSITIVO CONFIGURADOR DE UMA REDE, PRIMEIRO DISPOSITIVO CONFIGURADOR E MEMÓRIA LEGÍVEL POR COMPUTADOR”

PEDIDOS RELACIONADOS

[001] Este pedido reivindica o benefício prioritário do Pedido de Patente US Nº 15/648,437, apresentado em 12 de julho de 2017, que reivindica o benefício prioritário do Pedido Provisório US Nº 62/410,309, depositado em 19 de outubro de 2016, intitulado “DEVICE PROVISIONING PROTOCOL (DPP) WITH MULTIPLE CONFIGURATORS”, e atribuído ao seu cessionário. A divulgação dos pedidos anteriores são considerados parte e são incorporados por referência no presente pedido de patente.

CAMPO TÉCNICO

[002] Essa divulgação geralmente se refere ao campo de sistemas de comunicação e, mais particularmente, a um protocolo de provisionamento de dispositivos (DPP) em uma rede de comunicação.

DESCRIÇÃO DA TECNOLOGIA RELACIONADA

[003] Uma rede inclui dispositivos que se comunicam um com o outro através de um meio de comunicação. Um dispositivo é configurado com parâmetros para acessar o meio de comunicação antes que o dispositivo possa se comunicar com outros dispositivos da rede. O processo de configuração de um dispositivo pode ser denominado como provisionamento de dispositivo e pode incluir operações para associação, cadastro, autenticação ou outras operações. Um novo dispositivo que ainda não esteja configurado para uma

rede é denominado como dispositivo de cadastro. Um protocolo de provisionamento de dispositivo (DPP) pode facilitar a configuração de um dispositivo de cadastro sendo introduzido na rede. Um dispositivo configurador é um dispositivo que tem a capacidade, de acordo com o protocolo de provisionamento de dispositivo, de configurar o dispositivo de cadastro para a rede.

SUMÁRIO

[004] Os sistemas, métodos e dispositivos desta divulgação têm, cada um, vários aspectos inovadores, nenhum dos quais é o único responsável pelos atributos desejáveis aqui divulgados.

[005] Um aspecto inovador da matéria objeto descrito nesta divulgação pode ser implementado em um primeiro dispositivo configurador de uma rede. O primeiro dispositivo configurador pode gerar um pacote de chave do configurador que inclua pelo menos uma chave de assinatura privada do configurador associada com o primeiro dispositivo configurador. O primeiro dispositivo configurador pode criptografar pelo menos uma parte do pacote de chave do configurador. O primeiro dispositivo configurador pode armazenar o pacote de chave do configurador em um local de armazenamento como um backup para a restauração subsequente pelo primeiro dispositivo configurador ou por um segundo dispositivo configurador.

[006] Em algumas implementações, o pacote de chave do configurador inclui ainda uma chave de verificação pública do configurador associada com a chave de assinatura

privada do configurador.

[007] Em algumas implementações, o primeiro dispositivo configurador pode criptografar o pacote de chave do configurador usando uma chave de criptografia que é diferente da chave de assinatura privada do configurador.

[008] Em algumas implementações, o primeiro dispositivo configurador pode criptografar a chave de assinatura privada do configurador usando uma técnica de criptografia de chave privada e pode incluir uma indicação da técnica de criptografia de chave privada em um cabeçalho do pacote de chave do configurador.

[009] Em algumas implementações, o primeiro dispositivo configurador pode gerar um envelope digital que inclui o pacote de chave do configurador e as informações de decriptografia. As informações de decriptografia podem habilitar o segundo dispositivo configurador a decriptografar pelo menos a parte do pacote de chave do configurador.

[0010] Em algumas implementações, o local de armazenamento é pelo menos um membro selecionado de um grupo que consiste em uma memória do primeiro dispositivo configurador, um local compartilhado na rede, um computador pessoal, um servidor doméstico, um serviço de armazenamento baseado em nuvem, e um ponto de acesso (AP) de uma rede sem fio.

[0011] Em algumas implementações, o armazenamento do pacote de chave do configurador inclui o armazenamento de um backup do pacote de chave do configurador. O primeiro dispositivo configurador pode

recuperar o backup do pacote de chave do configurador do local de armazenamento. O primeiro dispositivo configurador pode decriptografar pelo menos a parte do pacote de chave do configurador e pode obter a chave de assinatura privada do configurador a partir do pacote de chave do configurador.

[0012] Em algumas implementações, o primeiro dispositivo configurador pode determinar a chave de verificação pública do configurador com base, pelo menos em parte, na chave de assinatura privada do configurador obtida a partir do pacote de chave do configurador.

[0013] Em algumas implementações, o primeiro dispositivo configurador pode determinar um endereço de localização do pacote de chave do configurador no local de armazenamento e pode fornecer o endereço de localização ao segundo dispositivo configurador.

[0014] Em algumas implementações, o primeiro dispositivo configurador pode fornecer as informações de decriptografia usando uma técnica de bootstrapping associada ao protocolo de provisionamento de dispositivo.

[0015] Em algumas implementações, o primeiro dispositivo configurador pode fornecer informações de decriptografia para o segundo dispositivo configurador. As informações de decriptografia podem permitir que o segundo dispositivo configurador decriptografe pelo menos a parte do pacote de chave do configurador e possa obter a chave de assinatura privada do configurador e a chave de verificação pública do configurador.

[0016] Em algumas implementações, as informações

de decriptografia incluem pelo menos um membro selecionado de um grupo que consiste em um endereço de localização do pacote de chave do configurador no local de armazenamento, uma frase secreta e uma chave de criptografia que pode ser usada para decriptografar pelo menos a parte do pacote de chave do configurador.

[0017] Em algumas implementações, fornecer as informações de decriptografia inclui fornecer as informações de decriptografia usando pelo menos um membro selecionado de um grupo que consiste em uma tela, um alto-falante, um sinal luminoso, uma interface de sensor e uma interface de frequência de rádio de curto alcance do primeiro dispositivo configurador.

[0018] Em algumas implementações, o primeiro dispositivo configurador pode fornecer as informações de decriptografia, exibindo uma imagem tendo as informações de decriptografia codificadas no mesmo.

[0019] Em algumas implementações, a imagem é um código de barras ou uma imagem de código de resposta rápida (QR).

[0020] Em algumas implementações, a chave de assinatura privada do configurador e a chave de verificação pública do configurador são compartilhadas entre uma pluralidade de configuradores de uma primeira rede. Cada um da pluralidade de configuradores pode ser capaz de usar a chave de assinatura privada do configurador e a chave de verificação pública do configurador, de acordo com um protocolo de provisionamento de dispositivo, para configurar

um dispositivo de cadastro para a primeira rede.

[0021] Um outro aspecto inovador da matéria objeto descrito nesta divulgação pode ser implementado em um segundo dispositivo configurador. O segundo dispositivo configurador pode obter, a partir de um local de armazenamento, um pacote de chave do configurador. Pelo menos uma parte do pacote de chave do configurador pode ser criptografada, e o pacote de chave do configurador pode incluir pelo menos uma chave de verificação pública do configurador e uma chave de assinatura privada do configurador associada a um primeiro dispositivo configurador. O segundo dispositivo configurador pode decriptografar pelo menos a parte do pacote de chave do configurador. O segundo dispositivo configurador pode obter a chave de assinatura privada do configurador a partir do pacote de chave do configurador. O segundo dispositivo configurador pode provisionar um dispositivo de cadastro para uma rede, utilizando a chave de assinatura privada do configurador, de acordo com um protocolo de provisionamento de dispositivo.

[0022] Em algumas implementações, o segundo dispositivo configurador pode obter informações de decriptografia a partir do primeiro dispositivo configurador. As informações de decriptografia podem habilitar o segundo dispositivo configurador a decriptografar pelo menos a parte do pacote de chave do configurador.

[0023] Em algumas implementações, o segundo dispositivo configurador pode obter a informação de

decriptografia usando pelo menos um membro selecionado de um grupo que consiste em uma tela, um alto-falante, um sinal luminoso, uma interface de sensor e uma interface de frequência de rádio de curto alcance do primeiro dispositivo configurador.

[0024] Em algumas implementações, o segundo dispositivo configurador pode obter, através de uma câmera associada ao segundo dispositivo configurador, uma imagem tendo as informações de decriptografia codificadas no mesmo. O segundo dispositivo configurador pode decodificar a imagem para recuperar as informações de decriptografia.

[0025] Um outro aspecto inovador da matéria objeto descrito nesta divulgação pode ser implementado em um método. O método pode ser realizado por um primeiro dispositivo configurador de uma rede e pode incluir a geração de um pacote de chave de configuração que inclua pelo menos uma chave de assinatura privada do configurador associada com o primeiro dispositivo configurador. O método pode incluir a criptografia de pelo menos uma parte do pacote de chave do configurador. O método pode incluir o armazenamento do pacote de chave do configurador em um local de armazenamento como um backup para restauração subsequente pelo primeiro dispositivo configurador ou por um segundo dispositivo configurador.

[0026] Em algumas implementações, o pacote de chave do configurador pode incluir ainda uma chave de verificação pública do configurador associada com a chave de assinatura privada do configurador.

[0027] Em algumas implementações, a criptografia

de pelo menos a parte do pacote de chave do configurador pode incluir a criptografia do pacote de chave do configurador usando uma chave de criptografia que é diferente da chave de assinatura privada do configurador.

[0028] Em algumas implementações, a criptografia de pelo menos a parte do pacote de chave do configurador pode incluir a criptografia da chave de assinatura privada do configurador usando uma técnica de criptografia de chave privada e inclui uma indicação da técnica de criptografia de chave privada em um cabeçalho do pacote de chave do configurador.

[0029] Em algumas implementações, o armazenamento do pacote de chave do configurador pode incluir a geração de um envelope digital que inclui o pacote de chave do configurador e informações de decriptografia, em que as informações de decriptografia permitem que o segundo dispositivo configurador decriptografe pelo menos a parte do pacote de chave do configurador.

[0030] Em algumas implementações, o local de armazenamento pode ser pelo menos um membro selecionado de um grupo consistindo de uma memória do primeiro dispositivo configurador, um local compartilhado na rede, um computador pessoal, um servidor doméstico, um serviço de armazenamento baseado em nuvem e um ponto de acesso (AP) de uma rede sem fio.

[0031] Em algumas implementações, o armazenamento do pacote de chave do configurador pode incluir o armazenamento de um backup do pacote de chave do

configurador. O método pode incluir a recuperação, pelo primeiro dispositivo configurador, do backup do pacote de chave do configurador a partir do local de armazenamento. O método pode incluir a decriptografia de pelo menos a parte do pacote de chave do configurador. O método pode incluir obter a chave de assinatura privada do configurador a partir do pacote de chave do configurador.

[0032] Em algumas implementações, o método pode incluir determinar uma chave de verificação pública do configurador com base, pelo menos em parte, na chave de assinatura privada do configurador obtida a partir do pacote de chave do configurador.

[0033] Em algumas implementações, o método pode incluir determinar um endereço de localização do pacote de chave do configurador no local de armazenamento. O método pode incluir fornecer o endereço de localização ao segundo dispositivo configurador.

[0034] Em algumas implementações, o método pode incluir fornecer as informações de decriptografia ao segundo dispositivo configurador, em que as informações de decriptografia permitem que o segundo dispositivo configurador decriptografe pelo menos a parte do pacote de chave do configurador e obtenha a chave de assinatura privada do configurador.

[0035] Em algumas implementações, as informações de decriptografia podem incluir pelo menos um membro selecionado de um grupo que consiste em um endereço de localização do pacote de chave do configurador no local de

armazenamento e uma chave de criptografia que pode ser usada para decriptografar pelo menos a parte do pacote de chave do configurador.

[0036] Em algumas implementações, fornecer informações de decriptografia pode incluir fornecer as informações de decriptografia usando pelo menos um membro selecionado de um grupo consistindo de uma tela, um alto-falante, um sinal luminoso, uma interface de sensor e uma interface de frequência de rádio de curto alcance do primeiro dispositivo configurador.

[0037] Em algumas implementações, fornecer as informações de decriptografia pode incluir a exibição de uma imagem tendo as informações de decriptografia codificadas.

[0038] Em algumas implementações, a imagem pode ser um código de barras ou uma imagem de código de Resposta Rápida (QR).

[0039] Em algumas implementações, uma chave de verificação pública do configurador pode ser derivada da chave de assinatura privada do configurador ou obtida a partir do pacote de chave do configurador. A chave de assinatura privada do configurador e a chave de verificação pública do configurador podem ser compartilhadas entre uma pluralidade de configuradores de uma primeira rede. Cada um da pluralidade de configuradores pode ser capaz de usar a chave de assinatura privada do configurador e a chave de verificação pública do configurador, de acordo com um protocolo de provisionamento de dispositivo, para configurar um dispositivo de cadastro para a primeira rede.

[0040] Um outro aspecto inovador da matéria objeto descrito nesta divulgação pode ser implementado em um primeiro dispositivo configurador, que inclui um processador e memória tendo instruções armazenadas nele. As instruções, quando realizadas pelo processador, podem fazer com que o primeiro dispositivo configurador gere um pacote de chave do configurador que inclua pelo menos uma chave de assinatura privada do configurador associada com o primeiro dispositivo configurador. As instruções, quando realizadas pelo processador, podem fazer com que o primeiro dispositivo configurador criptografe pelo menos uma parte do pacote de chave do configurador e armazene o pacote de chave do configurador em um local de armazenamento como backup para restauração subsequente pelo primeiro dispositivo configurador ou dispositivo configurador.

[0041] Em algumas implementações, as instruções, quando realizadas pelo processador, podem fazer com que o primeiro dispositivo configurador criptografe o pacote de chave do configurador usando uma chave de criptografia diferente da chave de assinatura privada do configurador.

[0042] Em algumas implementações, as instruções, quando realizadas pelo processador, podem fazer com que o primeiro dispositivo configurador criptografe a chave de assinatura privada do configurador usando uma técnica de criptografia de chave privada e inclua uma indicação da técnica de criptografia de chave privada em um cabeçalho do pacote de chave do configurador.

[0043] Em algumas implementações, as instruções,

quando realizadas pelo processador, podem fazer com que o primeiro dispositivo configurador gere um envelope digital que inclui o pacote de chave do configurador e informações de decriptografia, em que as informações de decriptografia permitem que o segundo dispositivo configurador decriptografe pelo menos a parte do pacote de chave do configurador.

[0044] Em algumas implementações, as instruções para armazenar o pacote de chave do configurador incluem instruções para armazenar um backup do pacote de chave do configurador. As instruções, quando realizadas pelo processador, podem fazer com que o primeiro dispositivo configurador recupere o backup do pacote de chave do configurador do local de armazenamento, decriptografe pelo menos a parte do pacote de chave do configurador e obtenha a chave de assinatura privada do configurador no pacote de chave do configurador.

[0045] Em algumas implementações, as instruções, quando realizadas pelo processador, podem fazer com que o primeiro dispositivo configurador determine um endereço de localização do pacote de chave do configurador no local de armazenamento e forneça o endereço de localização ao segundo dispositivo configurador.

[0046] Em algumas implementações, as instruções, quando realizadas pelo processador, podem fazer com que o primeiro dispositivo configurador forneça informações de decriptografia para o segundo dispositivo configurador, em que as informações de decriptografia permitem que o segundo dispositivo configurador decriptografe pelo menos a parte do

pacote de chave do configurador e obtenha a chave de assinatura privada do configurador.

[0047] Em algumas implementações, as informações de decriptografia incluem pelo menos um membro selecionado de um grupo que consiste em um endereço de localização do pacote de chave do configurador no local de armazenamento e uma chave de criptografia que pode ser usada para decriptografar pelo menos a parte do pacote de chave do configurador.

[0048] Em algumas implementações, as instruções, quando realizadas pelo processador, podem fazer com que o primeiro dispositivo configurador forneça as informações de decriptografia usando pelo menos um membro selecionado de um grupo que consiste em uma tela, um alto-falante, um sinal luminoso, um sensor interface e uma interface de frequência de rádio de curto alcance do primeiro dispositivo configurador.

[0049] Um outro aspecto inovador da matéria objeto descrito nesta divulgação pode ser implementado em um meio legível por computador tendo armazenado nele instruções que, quando realizadas por um processador de um primeiro dispositivo configurador, podem fazer com que o primeiro dispositivo configurador gere um pacote de chave do configurador que inclui pelo menos uma chave de assinatura privada do configurador associada com o primeiro dispositivo configurador. As instruções, quando realizadas pelo processador do primeiro dispositivo configurador, podem fazer com que o primeiro dispositivo configurador criptografe pelo menos uma parte do pacote de chave do configurador e armazene

o pacote de chave do configurador em um local de armazenamento para recuperação subsequente pelo primeiro dispositivo configurador ou um segundo dispositivo configurador.

[0050] Um outro aspecto inovador da matéria objeto descrito nesta divulgação pode ser implementado em um método realizado por um segundo dispositivo configurador. O método pode incluir obter, no segundo dispositivo configurador de um local de armazenamento, de um pacote de chave do configurador, em que pelo menos uma parte do pacote de chave do configurador é criptografada, e o pacote de chave do configurador inclui pelo menos uma chave de assinatura privada do configurador associada a um primeiro configurador. O método pode incluir a decriptografia de pelo menos a parte do pacote de chave do configurador, obtendo a chave de assinatura privada do configurador a partir do pacote de chave do configurador e provisionando um dispositivo de cadastro para uma rede utilizando a chave de assinatura privada do configurador de acordo com um protocolo de provisionamento de dispositivo.

[0051] Em algumas implementações, o método pode incluir obter as informações de decriptografia do primeiro dispositivo configurador, em que as informações de decriptografia permitem que o segundo dispositivo configurador decriptografe pelo menos a parte do pacote de chave do configurador.

[0052] Em algumas implementações, as informações de decriptografia podem incluir pelo menos um membro

selecionado de um grupo que consiste em um endereço de localização do pacote de chave do configurador no local de armazenamento e uma chave de criptografia que pode ser usada para decriptografar pelo menos a parte do pacote de chave do configurador.

[0053] Em algumas implementações, obter as informações de decriptografia podem incluir obter as informações de decriptografia usando pelo menos um membro selecionado de um grupo consistindo de uma tela, um alto-falante, um sinal luminoso, uma interface de sensor e uma interface de frequência de rádio de curto alcance do primeiro dispositivo configurador.

[0054] Em algumas implementações, obter as informações de decriptografia pode incluir obter, através de uma câmara associada ao segundo dispositivo configurador, de uma imagem tendo as informações de decriptografia codificadas nele; e decriptografia da imagem para recuperar as informações de decriptografia.

[0055] Detalhes de uma ou mais implementações da matéria objeto descrita nesta descrição são apresentados nos desenhos juntos e na descrição abaixo. Outras características, aspectos e vantagens tornar-se-ão evidentes a partir da descrição, dos desenhos e das reivindicações. Observe que as dimensões relativas das figuras a seguir podem não ser desenhadas para escala.

BREVE DESCRIÇÃO DOS DESENHOS

[0056] A Figura 1 mostra um diagrama de sistema de exemplo para introduzir conceitos de um protocolo de

provisionamento de dispositivo com vários configuradores.

[0057] A Figura 2 mostra um diagrama de fluxo de mensagens de exemplo de um protocolo de provisionamento de dispositivo.

[0058] A Figura 3 mostra um exemplo de fluxograma para um primeiro dispositivo configurador que armazena as chaves do configurador.

[0059] A Figura 4 mostra um diagrama de sistema de exemplo para descrever um backup e uma restauração das chaves do configurador por um primeiro dispositivo configurador.

[0060] A Figura 5 mostra um diagrama de sistema de exemplo para descrever as chaves do configurador de compartilhamento de um primeiro dispositivo configurador para um segundo dispositivo configurador.

[0061] A Figura 6 mostra um diagrama de fluxo de mensagens de exemplo do protocolo de provisionamento de dispositivo com vários configuradores.

[0062] A Figura 7 mostra um exemplo de fluxograma para operar o primeiro dispositivo configurador.

[0063] A Figura 8 mostra um exemplo de fluxograma para operar o segundo dispositivo configurador.

[0064] A Figura 9 mostra um exemplo de fluxograma para operar um dispositivo configurador para fazer backup e restaurar as chaves do configurador.

[0065] A Figura 10 mostra um diagrama de blocos de um exemplo de dispositivo eletrônico para implementar aspectos desta divulgação.

[0066] Tal como números de referência e designações nos vários desenhos indicam elementos semelhantes.

DESCRIÇÃO DETALHADA

[0067] A descrição que se segue é dirigida a certas implementações com o propósito de descrever os aspectos inovadores desta divulgação. Contudo, uma pessoa de habilidade comum na técnica reconhecerá prontamente que os ensinamentos aqui apresentados podem ser aplicados de várias maneiras diferentes. As implementações descritas podem ser implementadas em qualquer dispositivo, sistema ou rede que seja capaz de transmitir e receber sinais de radiofrequência (RF) de acordo com qualquer um dos padrões do Instituto de Engenharia Elétrica e Eletrônica (IEEE) 16.11, ou qualquer um dos padrões IEEE 802.11, o padrão Bluetooth®, acesso múltiplo por divisão de código (CDMA), acesso múltiplo por divisão de frequência (FDMA), acesso múltiplo por divisão de tempo (TDMA), Sistema Global para comunicações móveis (GSM), GSM/Serviço Geral de Pacote Via Rádio (GPRS), Ambiente GSM de Dados Aprimorados (EDGE), Rádio Terrestre com Troncos (TETRA), Banda Larga-CDMA (W-CDMA), Dados Evoluídos Otimizados (EV-DO), lxEV-DO, EV-DO Rev A, EV-DO Rev B, Acesso a Pacotes de Downlink de Alta Velocidade (HSPA), HSDPA, HSUPA, HSPA +, LTE, AMPS ou outros sinais conhecidos que são usados para comunicar-se dentro de uma rede sem fio, celular ou de internet de coisas (IOT), tal como um sistema utilizando 3G, 4G ou 5G, ou outras implementações do mesmo, tecnologia.

[0068] Como dito acima, um protocolo de provisionamento de dispositivo (DPP, como o Protocolo de Provisionamento de Dispositivo Wi-Fi) pode facilitar a configuração de um dispositivo de cadastro sendo introduzido na rede. Por exemplo, o DPP pode fornecer autenticação e estabelecimento de chave autenticada entre o dispositivo de cadastro e um dispositivo configurador. Em algumas implementações, o DPP usa menos mensagens do que normalmente usadas para um protocolo de autenticação. Por exemplo, o protocolo de autenticação DPP pode usar uma chave pública "bootstrapped" para uma primeira autenticação e para gerar uma chave de protocolo efêmera antes de continuar o provisionamento. Bootstrapping refere-se ao uso de uma técnica fora de banda confiável para obter uma chave pública. A técnica fora da banda fornece um nível de confiança com base na proximidade dos dispositivos. Por exemplo, o bootstrapping pode incluir o uso de uma câmera em um primeiro dispositivo para varrer e decodificar uma imagem que é exibida por (ou afixada em) um segundo dispositivo.

[0069] No DPP, os dispositivos configuradores são responsáveis por apoiar a configuração dos cadastros. Normalmente, a chave de bootstrapping pode ser usada para uma primeira autenticação entre um dispositivo configurador e um novo cadastro. Após a conclusão da autenticação, o dispositivo configurador pode provisionar o cadastro para comunicação através da rede. Como parte desse provisionamento, o dispositivo configurador permite que o cadastro estabeleça associações seguras com outros pares na

rede. As chaves do configurador são usadas pelo dispositivo configurador para gerar um "conector" (que também pode ser denominado como "objeto de configuração"). Um conector carrega a configuração do cadastro e autoriza a conectividade entre o dispositivo de cadastro e um dispositivo semelhante (como um ponto de acesso ou um vizinho ponto a ponto). As chaves do configurador incluem o par de chaves de assinatura formado por uma chave de assinatura privada do configurador (que pode ser chamada de "chave de sinal c") e uma chave de verificação pública do configurador (que pode ser chamada de "chave de sinal C"). A chave de assinatura privada do configurador (chave de sinal C) é usada pelo configurador para assinar conectores, enquanto a chave de verificação pública do configurador (Chave de sinal C) é usada pelos dispositivos provisionados para verificar se os conectores de outros dispositivos são assinados pelo mesmo configurador. Como descrito mais abaixo, as chaves do configurador correspondem matematicamente e podem ser usadas para verificar a autenticidade de uma mensagem assinada pelo dispositivo configurador. Cada conector pode ser assinado usando uma chave de assinatura privada do configurador do dispositivo configurador. Um dispositivo configurador pode produzir um ou mais conectores para cada cadastro configurado pelo dispositivo configurador. Depois que o conector for assinado usando uma chave de assinatura privada do configurador do dispositivo configurador, o conector poderá ser verificado por qualquer ponto na rede. Por exemplo, a chave de verificação pública do configurador pode ser usada

para verificar a autenticidade do conector que foi assinado usando a chave de assinatura privada do configurador. Como as chaves do configurador podem ser um aspecto fundamental do protocolo de provisionamento de dispositivos, pode haver uma situação em que as chaves do configurador possam ser armazenadas com segurança como um backup ou compartilhadas com outro dispositivo configurador.

[0070] Em um aspecto, um dispositivo configurador pode preparar um pacote de chave do configurador como um backup seguro das chaves do configurador. O pacote de chave do configurador pode ser armazenado como um backup para restauração posterior. Por exemplo, o pacote de chave do configurador pode ser exportado para um local acessível pelo dispositivo configurador e, potencialmente, por outros dispositivos configuradores. Em um outro aspecto, os vários dispositivos configuradores podem compartilhar as mesmas chaves do configurador. Por exemplo, as chaves do configurador podem ser compartilhadas com um segundo dispositivo configurador para que o segundo dispositivo configurador possa usar as chaves do configurador. Como cenário hipotético, considere um exemplo quando dois colegas de quarto compartilham uma residência, e cada colega de quarto opera um dispositivo configurador (como seus telefones celulares pessoais) para configurar os dispositivos de cadastro de cliente. As implementações descritas nesta divulgação melhoram o protocolo de provisionamento de dispositivo para que as chaves de configurador possam ser usadas por vários dispositivos configuradores.

[0071] Um primeiro dispositivo configurador pode gerar um pacote de chave do configurador que inclui pelo menos uma chave de assinatura privada do configurador associada com o primeiro dispositivo configurador. O pacote de chave do configurador também pode incluir uma chave de verificação pública do configurador que está associada com a chave de assinatura privada do configurador. O primeiro dispositivo configurador pode criptografar pelo menos uma parte do pacote de chave do configurador e armazenar o pacote de chave do configurador em um local de armazenamento para recuperação subsequente pelo primeiro dispositivo configurador ou por um segundo dispositivo configurador. O pacote de chave do configurador pode ser criptografado usando uma chave de criptografia que pode ser compartilhada desde o primeiro dispositivo configurador para o segundo dispositivo configurador. Em algumas implementações, o protocolo de provisionamento de dispositivos usa o bootstrapping para obter uma chave de bootstrap pública de um dispositivo de cadastro. As técnicas similares de bootstrap podem ser usadas para compartilhar a chave de criptografia entre dispositivos configuradores. O bootstrap fornece confiança na chave de criptografia porque a técnica fora da banda geralmente envolve proximidade ou associação física com o ponto do dispositivo.

[0072] As implementações particulares da matéria objeto descritas nesta divulgação podem ser implementadas para realizar uma ou mais das seguintes vantagens potenciais. Usando implementações nesta divulgação, um protocolo de

provisionamento de dispositivo pode suportar backup/restauração ou exportação/importação de chaves de configurador. Em algumas implementações, o protocolo de provisionamento de dispositivo pode se beneficiar de ter vários dispositivos configuradores para uma rede. Os dispositivos com vários configuradores podem usar as mesmas chaves do configurador compartilhadas, o que pode melhorar a compatibilidade entre os pontos configurados para a rede. Por exemplo, os conectores podem ser assinados e verificados usando as mesmas chaves do configurador, independentemente de qual dispositivo configurador configurou o dispositivo de cadastro para a rede. As técnicas para compartilhar as chaves de configurador nesta divulgação podem fornecer uma abordagem escalonável e menos complexa para adicionar mais dispositivos configuradores ao protocolo de provisionamento de dispositivo, em comparação com abordagens que dependem de chaves de configurador diferentes para cada dispositivo configurador. Definindo um formato de armazenamento seguro para armazenar ou compartilhar as chaves do configurador, o protocolo de provisionamento de dispositivo pode se beneficiar do aumento da interoperabilidade entre os dispositivos configuradores.

[0073] A Figura 1 mostra um diagrama de sistema de exemplo para introduzir conceitos de um protocolo de provisionamento de dispositivo com vários configuradores. O sistema de exemplo 100 inclui um primeiro dispositivo configurador 110, um segundo dispositivo configurador 120 e dispositivos de cadastro 150A e 150B. Um dispositivo de

cadastro pode ser qualquer tipo de dispositivo que ainda não tenha sido configurado para utilização em uma rede gerenciada pelo primeiro dispositivo configurador 110 ou pelo segundo dispositivo configurador 120. O primeiro dispositivo configurador 110 pode ter um par de chaves configuradoras que incluem uma chave de assinatura privada do configurador e uma chave de verificação pública do configurador. A chave de assinatura privada do configurador pode ser usada para criar uma mensagem assinada digitalmente. A chave de verificação pública do configurador pode ser usada para verificar se a mensagem assinada digitalmente foi assinada usando a chave de assinatura particular do configurador.

[0074] Como mostrado na Figura 1, o primeiro dispositivo configurador 110 pode implementar um protocolo de provisionamento de dispositivo (mostrado como seta 158) para configurar um dispositivo de cadastro 150A para uso em uma rede. Para usar o protocolo de provisionamento de dispositivo com vários dispositivos configuradores, o primeiro dispositivo configurador 110 pode compartilhar (mostrado como seta 152) seu par de chaves do configurador com o segundo dispositivo configurador 120. Como discutido mais abaixo, as chaves do configurador podem não ser transmitidas diretamente para o segundo dispositivo configurador 120. Em vez disso, o primeiro dispositivo configurador 110 pode gerar um pacote de chave do configurador. Alguns ou todos os conteúdos do pacote de chave do configurador podem ser criptografados usando uma chave de criptografia. O pacote de chave do configurador pode ser exportado para um local na rede acessível pelo segundo

dispositivo configurador 120. Em algumas implementações, o primeiro dispositivo configurador 110 pode fornecer as informações de decriptografia para o segundo dispositivo configurador 120 de modo que o segundo dispositivo configurador 120 possa obter e decriptografar o pacote de chave do configurador. Por exemplo, as informações de decriptografia podem incluir um endereço de local em que o pacote de chave do configurador é armazenado. Em algumas implementações, as informações de decriptografia podem incluir a chave de criptografia. As informações de decriptografia podem ser fornecidas usando uma técnica de bootstrapping semelhante que é usada pelo dispositivo configurador para obter uma chave de bootstrap pública de um dispositivo de cadastro. As técnicas de bootstrap são descritas com mais detalhe na descrição da Figura 2. Em algumas outras implementações, as informações de decriptografia podem incluir uma senha ou outra informação que pode ser inserida manualmente no segundo dispositivo configurador 120 para decriptografar o pacote de chave do configurador.

[0075] Uma vez que o segundo dispositivo configurador 120 obteve as informações de decriptografia e o pacote de chave do configurador, o segundo dispositivo configurador 120 pode decriptografar o pacote de chave do configurador (como, usando a chave de criptografia) e recuperar as chaves do configurador. O segundo dispositivo configurador 120 pode armazenar as chaves do configurador e usar as chaves do configurador compartilhado ao configurar

outros dispositivos de cadastro. Por exemplo, o segundo dispositivo configurador 120 pode implementar o protocolo de provisionamento de dispositivo (mostrado como seta 154) para configurar dispositivo de cadastro 150B. Embora os dispositivos de cadastro 150A e 150B tenham sido configurados por dispositivos configuradores diferentes, cada um dos dispositivos de cadastro 150A e 150B pode verificar os conectores assinados (que os autorizam a se comunicarem pela rede) usando uma mesma chave de verificação pública do configurador.

[0076] A Figura 2 mostra um diagrama de fluxo de mensagens de exemplo de um protocolo de provisionamento de dispositivo. O DPP 200 na Figura 2 está entre um par de dispositivos, o dispositivo de cadastro 250 e um dispositivo configurador 210. O DPP 200 inclui três operações: a técnica de bootstrap, a autenticação DPP e a configuração DPP. A autenticação DPP depende da chave de bootstrap da parte de autenticação ter sido obtida por meio de uma técnica de bootstrapping (como as descritas abaixo).

[0077] Bootstrapping refere-se a uma técnica fora de banda para obter uma chave compartilhada de outro dispositivo. Cada dispositivo de cadastro 250 e o dispositivo de configuração 210 podem ter uma chave de bootstrap pública (também por vezes denominada como uma "chave de identidade pública") que é confiável para uma autenticação inicial e para gerar uma chave temporária de fornecimento. Bootstrapping é uma das várias técnicas que podem ser usadas para compartilhar a chave de bootstrap pública. Por exemplo,

o bootstrapping pode incluir a varredura de um código Quick Response® (QR) que codifica a chave de bootstrap pública. O suporte a essa forma de autenticação permite que determinados dispositivos (como dispositivos IOT, acessórios vestíveis, dispositivos de automação residencial, etc.) não tenham uma interface de usuário para serem autenticados com um dispositivo configurador.

[0078] Em 205, o dispositivo configurador 210 pode obter dados de bootstrapping de cadastro a partir do dispositivo de cadastro 250. Por exemplo, o dispositivo de cadastro 250 pode ter um indicador visual impresso sobre ele (ou no pacote, ou inserido no pacote). O indicador visual pode ser um código de barras, código de matriz, código bidimensional ou semelhante. Um exemplo comum de código de barras pode ser um código QR. O dispositivo configurador 210 pode detectar o código de barras (ou indicador visual semelhante) usando uma câmera e o software correspondente. O dispositivo configurador 210 pode obter os dados de bootstrap do cadastro decodificando-se o código de barras. Em uma implementação, os dados de bootstrapping cadastrados podem incluir uma chave de bootstrap pública para o dispositivo de cadastro 250. Além da chave de bootstrap pública, outras informações também podem ser incluídas nos dados de bootstrapping cadastrados. Por exemplo, os dados de bootstrapping cadastrados podem incluir a chave de bootstrap pública, bem como uma classe operacional global e uma lista de números de canais. A lista de classe operacional global e número de canal pode ser usada para determinar quais

parâmetros de rádio ou quais canais sem fio o dispositivo de cadastro 250 usará para a autenticação DPP. Por exemplo, em conjunto, a lista da Classe Operacional Global e do Canal pode indicar qual canal sem fio o dispositivo de cadastro 250 irá escutar (ou enviar) uma mensagem de solicitação de autenticação DPP. Em 207, em algumas implementações, o dispositivo de cadastro 250 também pode obter um configurador de dados de bootstrap do dispositivo configurador 210. Quando ambas as partes obtém os dados de bootstrap um do outro, a autenticação DPP pode utilizar autenticação bidirecional mútua.

[0079] Além da técnica de bootstrapping mostrada na Figura 2, uma variedade de outras técnicas de bootstrapping pode ser usada. A técnica de bootstrapping permite que um destinatário confie que os dados de bootstrapping pertencem a um dispositivo específico. Conforme descrito na Figura 1, a varredura de um código de barras de matriz bidimensional (como um código QR) é uma técnica para obter dados de bootstrapping. Como uma alternativa para varrer um código de barras, o dispositivo configurador 210 pode usar rede de vizinhança ciente (NAN) (não mostrada). A NAN fornece a capacidade de descoberta e troca de informações de serviço por meio sem fio sem ter uma associação entre dispositivos. Uma outra técnica de bootstrapping é transferir dados de bootstrapping sobre outras mídias que podem fornecer uma certa quantidade de confiança para a integridade do conteúdo de transferência. Por exemplo, em algumas implementações, o bootstrapping pode incluir o uso de

barramento serial universal (USB), comunicação de campo próximo (NFC) ou comunicação de rádio de curto alcance (como a comunicação por Bluetooth™). Ainda uma outra técnica de bootstrapping é mascarar os dados de bootstrapping com um código compartilhado/chave/frase/palavra (doravante, "código") e confiar no conhecimento do código compartilhado para desmascarar a chave de bootstrapping. Se um par for capaz de provar que sabe e pode usar o código compartilhado, os dados de bootstrap do ponto podem ser confiáveis.

[0080] A fase de autenticação do DPP usa os dados de bootstrapping, obtidos usando uma técnica de bootstrapping, para autenticar fortemente o configurador e o cadastro. A autenticação DPP consiste em uma troca de 3 mensagens e gera um segredo compartilhado e uma chave autenticada. Em 215, o dispositivo configurador 210 gera um primeiro identificador único, gera um par de chaves de protocolo, executa uma função hash da chave de bootstrap pública do cadastro e gera uma primeira chave simétrica com base em um segredo compartilhado derivado dos dados de bootstrap com hash. O dispositivo configurador 210 envia uma mensagem de Pedido de Autenticação DPP 217 através de um ou mais dos canais na Lista de Canais. A mensagem de solicitação de autenticação do DPP 217 inclui o segredo compartilhado e o primeiro identificador único criptografado pela primeira chave simétrica.

[0081] O dispositivo de cadastro 250 recebe a mensagem de Solicitação de Autenticação DPP 217. No 225, o dispositivo de cadastro 250 verifica se existe um hash da sua

chave de bootstrap pública na mensagem. Se um hash de sua chave de bootstrap pública estiver na mensagem, o dispositivo de cadastro 250 gera o segredo compartilhado e deriva a primeira chave simétrica. O dispositivo de cadastro 250 tenta desembrulhar o primeiro identificador único usando a primeira chave simétrica. Em seguida, o dispositivo de cadastro 250 gera um segundo identificador único, um segredo compartilhado e uma segunda chave simétrica. O dispositivo de cadastro 250 envolve as duas peças e as suas capacidades na primeira chave simétrica e envolve o indicador de autenticação na segunda chave simétrica. O dispositivo de cadastro 250 coloca então um hash da sua chave de bootstrap pública (e opcionalmente inclui um hash da chave de bootstrap pública dos configuradores se estiver fazendo autenticação mútua), a sua chave de protocolo pública, os identificadores únicos envolvidos juntamente com a sua chave pública de rede envolvida e o indicador de autenticação envolvido em uma mensagem de Resposta de Autenticação DPP 227. A mensagem 227 de Resposta de Autenticação DPP transmitida para o dispositivo configurador 210.

[0082] Após receber com sucesso uma resposta, o dispositivo configurador 210 valida o resultado em 235 e transmite uma mensagem de Confirmação de Autenticação DPP 237 para completar a fase de autenticação DPP. Após a conclusão bem-sucedida dessas trocas de quadros, um canal seguro entre o Iniciador/Configurador e o Dispositivo de Resposta/Cadastro é estabelecido em 245.

[0083] Após a autenticação DPP estar concluída,

o dispositivo configurador 210 provisiona o dispositivo de cadastro 250 para comunicação de dispositivo para dispositivo ou comunicação de infraestrutura. Como parte deste provisionamento, o dispositivo configurador 210 permite que o dispositivo de cadastro 250 estabeleça associações seguras com outros pares na rede. O dispositivo de cadastro 250 inicia a fase de configuração transmitindo uma mensagem 263 de Solicitação de Configuração de DPP e é fornecido com informação de configuração em uma mensagem 267 de Resposta de Configuração de DPP. Depois de receber com sucesso a mensagem 267 de Resposta de Configuração de DPP, o dispositivo de cadastro 250 é provisionado com a configuração informações úteis para estabelecer acesso seguro à rede.

[0084] Em algumas implementações, o dispositivo configurador 210 também pode ser um ponto de acesso de uma rede local sem fio (WLAN). Em alternativa, o dispositivo configurador 210 pode ser separado do ponto de acesso. Por exemplo, as informações de configuração fornecidas pelo dispositivo configurador 210 podem ser utilizadas pelo dispositivo de cadastro 250 para estabelecer uma conexão segura sem fios com um ponto de acesso 280. Em uma outra implementação, o dispositivo configurador 210 pode ser um proprietário do grupo ponto-a-ponto (P2P) ou membro do grupo P2P.

[0085] Na conclusão da fase de configuração do DPP, o dispositivo configurador 210 pode criar um conector (representado pela seta 277). O conector é uma introdução assinada que permite ao dispositivo de cadastro 250 obter uma

declaração confiável que outros dispositivos na rede têm permissão para se comunicar com ele. Cada conector pode incluir uma tupla de um identificador de grupo, uma função de rede e uma chave de provisionamento de acesso à rede, todas assinadas usando uma chave de assinatura privada do configurador do dispositivo configurador. O identificador pode indicar um par específico ou o caractere curinga, indicando todos os pares. Como descrito acima, o conector é assinado pela chave de assinatura privada do configurador (chave de sinal c) do dispositivo configurador 210 e pode ser verificado usando a chave de verificação pública do configurador (chave de sinal C) do dispositivo configurador 210

[0086] Se o dispositivo configurador 210 estiver separado do ponto de acesso 280, o dispositivo de cadastro 250 pode utilizar as informações de configuração e o conector como credenciais para uma associação sem fios 287 com o ponto de acesso 280. O dispositivo de cadastro 250 pode descobrir o ponto de acesso 280, transmitem um quadro de Solicitação de Descoberta de Pares (não mostrado) e, em seguida, aguardam um quadro de Resposta de Descoberta de Pares (não mostrado). Após a validação bem sucedida dos quadros de descoberta de pares, o dispositivo de cadastro 250 e o ponto de acesso 280 obtêm, mutuamente, uma chave mestra de pares (PMK) e seguem os procedimentos normais de IEEE 802.11. Por exemplo, um procedimento de aperto de mão de 4 vias pode ser realizado entre o dispositivo de cadastro (cadastro) 250 e o ponto de acesso (280) para completar a autenticação e associação sem

fios do dispositivo de cadastro (cadastro) com o ponto de acesso (280). Uma chave mestra de pares (PMK) pode ser usada para mensagens subsequentes de aperto de mão e configuração do Acesso Protegido por Wi-Fi™ (WPA). Alternativamente, se o ponto de acesso 280 é um ponto de acesso legado, as informações de configuração podem incluir uma chave pré-compartilhada (PSK) ou uma credencial de Senha de PSK para permitir que o dispositivo de cadastro 250 se conecte ao ponto de acesso 280. Nesta implementação, o dispositivo de cadastro 250 usará a informações de configuração para descobrir e associar-se a um AP usando os procedimentos de acesso à rede IEEE 802.11 e WPA2 -Pessoal.

[0087] A Figura 3 mostra um exemplo de fluxograma para um primeiro dispositivo configurador que armazena as chaves do configurador. O fluxograma 300 começa no bloco 310. No bloco 310, o primeiro dispositivo configurador pode gerar um pacote de chave do configurador que inclui pelo menos uma chave de assinatura privada do configurador associada ao dispositivo do primeiro configurador. Em algumas implementações, o pacote de chave do configurador pode incluir a chave de assinatura privada do configurador e a chave de verificação pública do configurador.

[0088] No bloco 320, o primeiro dispositivo configurador pode criptografar pelo menos uma parte do pacote de chave do configurador. Por exemplo, o pacote de chave do configurador pode ser criptografado usando uma chave de criptografia diferente da chave de assinatura particular do

configurador. Em algumas implementações, o primeiro dispositivo configurador pode criptografar a chave de assinatura privada do configurador (e, opcionalmente, a chave de verificação pública do configurador) usando uma técnica de criptografia de chave privada. Em algumas implementações, o pacote de chave do configurador pode incluir um cabeçalho que descreve uma estrutura, conteúdo ou uma técnica de criptografia usada para preparar o pacote de chave do configurador.

[0089] No bloco 330, o primeiro dispositivo configurador pode armazenar o pacote de chave do configurador em um local de armazenamento como um backup para a restauração subsequente pelo primeiro dispositivo configurador ou por um segundo dispositivo configurador. Por exemplo, o local de armazenamento pode ser uma memória do primeiro dispositivo configurador, um local compartilhado na rede, um computador pessoal, um servidor doméstico, um serviço de armazenamento com base em nuvem ou um ponto de acesso (AP) de uma rede sem fio.

[0090] Após o pacote de chave do configurador ter sido armazenado, pode haver diferentes maneiras de usar o pacote de chave do configurador armazenado. Por exemplo, no bloco 340, o primeiro dispositivo configurador pode recuperar o backup do pacote de chave do configurador do local de armazenamento. O primeiro dispositivo configurador pode decriptografar o pacote de chave do configurador e obter a chave de assinatura privada do configurador a partir do pacote de chave do configurador. Em um outro exemplo, no

bloco 350, o primeiro dispositivo configurador pode fornecer informações de decriptografia para um segundo dispositivo configurador. As informações de decriptografia podem permitir que o segundo dispositivo configurador decriptografe pelo menos a parte do pacote de chave do configurador que foi criptografada pelo primeiro dispositivo configurador. O segundo dispositivo configurador pode obter a chave de assinatura privada do configurador a partir do pacote de chave do configurador. Se o pacote de chave do configurador incluir a chave de verificação pública do configurador, o segundo dispositivo configurador poderá restaurar a chave de verificação pública do configurador a partir do pacote de chave do configurador. Se o pacote de chave do configurador não incluir a chave de verificação pública do configurador, o segundo dispositivo configurador poderá determinar a chave de verificação pública do configurador com base, pelo menos em parte, na chave de assinatura privada do configurador.

[0091] A Figura 4 mostra um exemplo de diagrama do sistema para descrever um backup e uma restauração das chaves do configurador por um primeiro dispositivo configurador. O sistema de exemplo 400 inclui um primeiro dispositivo configurador 110 e um local de armazenamento 410. O primeiro dispositivo configurador 110 tem chaves do configurador 412 e capaz de criptografar pelo menos parte das chaves do configurador 412 utilizando uma técnica de criptografia 416. Pode haver uma variedade de técnicas de criptografia que podem ser prontamente aplicadas às implementações desta divulgação. Exemplos de diferentes

técnicas de criptografia são descritos abaixo.

[0092] O primeiro dispositivo configurador 110 pode gerar um pacote de chave de configuração 427 que inclui as chaves do configurador 412 e foi pelo menos parcialmente criptografado (denotado por chaves) usando a técnica de criptografia 416. O primeiro dispositivo configurador 110 também tem um módulo de backup/restauração 455 pode fazer com que o pacote de chave de configurador 427 seja armazenado (mostrado na seta 467) no local de armazenamento 410. Por exemplo, o ato de armazenar o pacote de chave de configurador 427 pode ser referido como uma cópia de segurança.

[0093] Após o pacote de chave do configurador 427 ter sido armazenado, o módulo de backup/restauração 455 pode ser capaz de restaurar as chaves do configurador. O módulo de backup/restauração 455 pode recuperar (mostrado na seta 477) o pacote de chave de configuração 427 a partir do local de armazenamento 410. Por exemplo, o módulo de backup/restauração 455 pode acessar ou baixar o pacote de chave de configurador 427 do local de armazenamento 410. O módulo de backup/restauração 455 pode restaurar as chaves do configurador invertendo a técnica de criptografia e obtendo as chaves do configurador a partir do pacote de chave do configurador 427.

[0094] A Figura 5 mostra um exemplo de diagrama de sistema para descrever as chaves do configurador de compartilhamento de um primeiro dispositivo configurador para um segundo dispositivo configurador. O sistema de exemplo 500 inclui um primeiro dispositivo configurador 110, um segundo

dispositivo configurador 120 e um local de armazenamento 410. O local de armazenamento 410 pode ser uma memória compartilhada na rede, uma unidade de rede, um recurso de um ponto de acesso, local de armazenamento, ou qualquer outro recurso que seja acessível pelo segundo dispositivo configurador 120 através de uma rede de comunicação. Como descrito acima, o primeiro dispositivo configurador 110 tem as chaves de configuração 412, que podem incluir uma chave de assinatura privada do configurador e uma chave de verificação pública do configurador. Para fornecer as chaves do configurador para o segundo dispositivo configurador 120, o primeiro dispositivo configurador 110 pode exportar as chaves do configurador no pacote de chave do configurador 427. Representado em 517, o primeiro dispositivo configurador 110 pode criptografar (utilizando uma chave de criptografia) as chaves do configurador e criar o pacote de chave do configurador 427. ***

[0095] Em algumas implementações, o primeiro dispositivo configurador 110 pode gerar o pacote de chave do configurador de acordo com uma família de padrões denominados Padrões de Criptografia de Chave Pública (PKCS). Por exemplo, o PKCS # 8 é um dos padrões e define um Sintaxe padrão para armazenar informações de chave privada. A criptografia no PCKS # 8 especifica um Envelope Digital, que é composto de um Pacote de Chave Assimétrica (com informações sobre a configuração) e uma chave de criptografia. A chave de criptografia pode ser protegida usando o gerenciamento de chaves, o contrato de chave, a chave simétrica derivada de

uma senha compartilhada ou a criptografia de chave simétrica por meio de informações compartilhadas. Assim, apenas um dispositivo que pode derivar a chave de criptografia pode decriptografar o pacote de chave do configurador. Em uma implementação, o primeiro dispositivo configurador 110 pode criar um perfil de conector público na rede, de modo que qualquer dispositivo configurador possa obter o pacote de chave de configurador 427 a partir do local de armazenamento 410 (na forma de um bloco PKCS # 8).

[0096] O perfil de conector público pode incluir, por exemplo, um endereço de localização, como um localizador uniforme de recursos (URL) ou um Identificador de Recurso Uniforme (URI) para o local de armazenamento 410, onde o pacote de chave do configurador pode ser baixado. Embora o pacote de chave do configurador possa ser acessível por vários dispositivos, apenas um dispositivo de configuração autorizado (tal como o segundo dispositivo configurador 120) terá as informações de decriptografia necessárias para decriptografar o pacote de chave do configurador. Por exemplo, as informações de decriptografia podem ser uma senha compartilhada para derivar a chave de criptografia do Envelope Digital associado ao pacote de chave do configurador. Como alternativa, as informações de decriptografia podem ser qualquer outro meio para um dispositivo obter a chave de criptografia usada para criptografar o pacote de chave do configurador. Noutro implementação, o endereço de localização pode ser mantido como um segredo que é fornecido apenas aos configuradores

autorizados. No 547, o pacote de chave do configurador 427 é armazenado no local de armazenamento 410 para recuperação subsequente. Em algumas implementações, o primeiro dispositivo configurador 110 pode enviar o pacote de chave do configurador 427 para o segundo dispositivo configurador 120 através de uma rede e fazer com que o pacote de chave do configurador 427 seja armazenado em um local de armazenamento que esteja localizado no segundo dispositivo configurador 120.

[0097] O segundo dispositivo configurador 120 pode obter (representado pela seta 537) informações de decriptografia do primeiro dispositivo configurador 110. Em algumas implementações, as informações de decriptografia podem incluir uma chave de criptografia necessária para decriptografar o pacote de chave do configurador. Em algumas implementações, as informações de decriptografia podem incluir um endereço de localização indicando onde o pacote de chave do configurador é armazenado no local de armazenamento 410. Pode haver uma variedade de maneiras para o primeiro dispositivo configurador 110 fornecer as informações de decriptografia para o segundo dispositivo configurador. - incluindo bootstrapping. Por exemplo, a chave de criptografia pode ser codificada em uma imagem de código de barras que pode ser digitalizada pelo segundo dispositivo configurador 120. Em algumas implementações, a imagem do código de barras pode ser estática ou efêmera. Por exemplo, o primeiro dispositivo configurador 110 pode estar equipado com um mostrador e pode criar uma imagem de código de barras (ou

outra imagem codificada) codificada com a chave de criptografia. A chave de criptografia pode ser determinada digitalizando e decodificando a imagem legível por máquina (como o código QR) com uma câmera, smartphone, scanner ou outro leitor de código legível por máquina do segundo dispositivo configurador 120. Além da chave de criptografia, a imagem de código de barras também pode ser codificada com o endereço de localização onde o segundo dispositivo de configuração 120 pode descarregar o pacote de chave de configuração 427.

[0098] O segundo dispositivo configurador 120 pode baixar (representado pela seta 557) o pacote de chave do configurador 427 a partir do local da rede. Uma vez que o segundo dispositivo configurador 120 tenha obtido o pacote de chave do configurador 5427 e a chave de criptografia, o segundo dispositivo configurador 120 pode desencriptar o pacote de chave privada criptografada para obter as chaves do configurador e armazenar as chaves do configurador em uma memória do segundo dispositivo configurador 120 para uso com o protocolo de provisionamento de dispositivos.

[0099] A Figura 6 mostra um diagrama de fluxo de mensagens de exemplo do protocolo de provisionamento de dispositivo com vários configuradores. O diagrama de fluxo de mensagens 600 inclui mensagens entre um primeiro dispositivo configurador 110, um segundo dispositivo configurador 120 e um local de armazenamento 410. No 605, o primeiro dispositivo configurador 110 pode gerar um pacote de chave configuradoras que inclui as chaves do configurador (chave de sinal C e

Chave de sinal C) do primeiro dispositivo configurador 110. O pacote de chave do configurador é criptografado utilizando uma chave de criptografia. No 611, o primeiro dispositivo configurador 110 exporta e armazena o pacote de chave do configurador no local de armazenamento 410. O primeiro dispositivo configurador 110 também pode determinar um endereço de localização indicando onde o pacote de chave do configurador é armazenado. A chave de criptografia e o endereço de localização podem ser codificados como uma imagem de código de barras ou outro tipo de estrutura de dados.

[00100] No 613, o segundo dispositivo configurador 120 pode obter o pacote de chave do configurador (e, opcionalmente, o endereço de localização). Por exemplo, o segundo dispositivo configurador 120 pode obter e descodificar a imagem de código de barras ou outra estrutura de dados. No 619, o segundo dispositivo configurador 120 pode determinar o endereço de localização do pacote de chave do configurador. O segundo dispositivo de configuração 120 pode determinar o endereço de localização a partir da imagem de código de barras, através de uma outra mensagem (não mostrada) a partir do primeiro dispositivo configurador 110, usando um perfil de conector público ou por qualquer outro mecanismo para compartilhar um endereço de localização. Com base no endereço de localização, o segundo dispositivo configurador 120 pode enviar uma solicitação (em 621) para o pacote de chave do configurador para o local de armazenamento 410. No 623, o segundo dispositivo configurador 120 pode receber o pacote de chave do configurador a partir do local

de armazenamento 410. Em 625, o segundo dispositivo configurador 120 pode decriptografar o pacote de chave do configurador (usando a chave de criptografia) e recuperar as chaves do configurador. Uma vez que o segundo dispositivo configurador 120 tenha as chaves do configurador, o segundo dispositivo configurador 120 pode configurar um dispositivo de cadastro 250 usando as mesmas chaves do configurador que o primeiro dispositivo configurador 110 usaria.

[00101] O provisionamento de dispositivo (incluindo bootstrap, autenticação e configuração) pode continuar como descrito anteriormente (consulte as descrições correspondentes das mensagens 205, 207, 217, 227, 237, 263, 267 e 277 na Figura 2).

[00102] A Figura 7 mostra um exemplo de fluxograma para operar o primeiro dispositivo configurador. O fluxograma 700 começa no bloco 710. No bloco 710, o primeiro dispositivo configurador pode gerar um pacote de chave do configurador tendo pelo menos uma parte criptografada usando uma chave de criptografia. O pacote de chave do configurador pode incluir pelo menos uma chave de assinatura privada do configurador para o primeiro dispositivo configurador. No bloco 720, o primeiro dispositivo configurador pode armazenar o pacote de chave do configurador em um local de armazenamento acessível por um segundo dispositivo configurador. No bloco 730, o primeiro dispositivo configurador pode fornecer a chave de criptografia para o segundo dispositivo configurador para permitir que o segundo dispositivo configurador decriptografe o pacote de chave do

configurador a partir do local de armazenamento. No bloco 740, o primeiro dispositivo configurador pode, opcionalmente, fornecer um endereço de localização para o segundo dispositivo configurador. O endereço do local pode indicar onde o pacote de chave do configurador está armazenado no local de armazenamento.

[00103] A Figura 8 mostra um exemplo de fluxograma para operar o segundo dispositivo configurador. O fluxograma 800 começa no bloco 810. No bloco 810, o segundo dispositivo configurador pode obter, no segundo dispositivo configurador, informações de decriptografia de um primeiro dispositivo configurador. Por exemplo, as informações de decriptografia podem ser uma chave de criptografia que foi usada anteriormente para criptografar o pacote de chave do configurador. No bloco 820, o segundo dispositivo configurador pode obter, no segundo dispositivo configurador a partir de um local de armazenamento, um pacote de chave do configurador. O pacote de chave do configurador pode incluir pelo menos uma chave de assinatura privada do configurador para o primeiro dispositivo configurador. No bloco 830, o segundo dispositivo configurador pode decriptografar o pacote de chave do configurador usando as informações de decriptografia para recuperar a chave de assinatura privada do configurador. Se o pacote de chave do configurador incluir a chave de verificação pública do configurador, o segundo dispositivo configurador poderá restaurar a chave de verificação pública do configurador a partir do pacote de chave do configurador. Se o pacote de chave do configurador

não incluir a chave de verificação pública do configurador, o segundo dispositivo configurador poderá determinar a chave de verificação pública do configurador com base, pelo menos em parte, na chave de assinatura privada do configurador. No bloco 840, o segundo dispositivo configurador pode configurar um dispositivo de cadastro para uma rede utilizando a chave de assinatura privada do configurador e a chave de verificação pública do configurador, de acordo com um protocolo de provisionamento de dispositivo. Se o pacote de chave do configurador não incluir a chave de verificação pública do configurador, o segundo dispositivo configurador poderá determinar a chave de verificação pública do configurador com base, pelo menos em parte, na chave de assinatura privada do configurador. No bloco 840, o segundo dispositivo configurador pode configurar um dispositivo de cadastro para uma rede utilizando a chave de assinatura privada do configurador e a chave de verificação pública do configurador, de acordo com um protocolo de provisionamento de dispositivo. Se o pacote de chave do configurador não incluir a chave de verificação pública do configurador, o segundo dispositivo configurador poderá determinar a chave de verificação pública do configurador com base, pelo menos em parte, na chave de assinatura privada do configurador. No bloco 840, o segundo dispositivo configurador pode configurar um dispositivo de cadastro para uma rede utilizando a chave de assinatura privada do configurador e a chave de verificação pública do configurador, de acordo com um protocolo de provisionamento de dispositivo. O segundo

dispositivo configurador pode configurar um dispositivo de cadastro para uma rede utilizando a chave de assinatura privada do configurador e a chave de verificação pública do configurador, de acordo com um protocolo de provisionamento de dispositivo. O segundo dispositivo configurador pode configurar um dispositivo de cadastro para uma rede utilizando a chave de assinatura privada do configurador e a chave de verificação pública do configurador, de acordo com um protocolo de provisionamento de dispositivo.

[00104] A Figura 9 mostra um exemplo de fluxograma para operar um dispositivo configurador para fazer backup e restaurar chaves do configurador. O fluxograma 900 começa no bloco 910. No bloco 910, o dispositivo configurador pode gerar um pacote de chave do configurador que inclui pelo menos uma cópia criptografada de uma chave de assinatura privada do configurador. A cópia criptografada pode ser criptografada usando uma técnica de criptografia de chave privada. Por exemplo, a técnica de criptografia de chave privada pode ser definida em pelo menos uma solicitação de comentários (RFC) 5958 e RFC 5208 da Internet Engineering Task Force (IETF). Em algumas implementações, a técnica de criptografia de chave privada pode ser identificada em um cabeçalho do pacote de chave do configurador.

[00105] No bloco 920, o dispositivo configurador pode armazenar o pacote de chave do configurador em um local de armazenamento acessível pelo dispositivo configurador como um backup. O local de armazenamento pode ser qualquer dispositivo de armazenamento que esteja disponível para o

dispositivo configurador. Exemplos do local de armazenamento incluem uma memória local do dispositivo configurador, um local de armazenamento, um computador pessoal, um servidor doméstico, um serviço de armazenamento com base em nuvem e semelhantes. Em algumas implementações, o local de armazenamento pode ser usado para armazenar backups de diferentes dispositivos configuradores usando diferentes chaves do configurador.

[00106] No bloco 930, o dispositivo configurador pode subsequentemente restaurar o backup obtendo o pacote de chave do configurador e decriptografar o pacote de chave do configurador usando a técnica de criptografia de chave privada.

[00107] Abaixo está um exemplo de um pacote de chave do configurador que pode ser usado com qualquer uma das implementações descritas aqui. O pacote de chave do configurador de exemplo é um pacote de chave assimétricas é um ASN. 1 sequência de uma chave assimétrica definida no RFC5958 (usando PKCS # 8):

```
AsymmetricKeyPackage:: = SEQUENCE SIZE (1) DE
OneAsymmetricKey
OneAsymmetricKey ::= SEQUENCE {
version        Version,
privateKeyAlgorithm PrivateKey Algorithmldentifier,
privateKey PrivateKey,
[[publicKey    PublicKey OPTIONAL,]]
[Optional Information as needed]
}
```

```
PrivateKey : := SEQUENCE {
        encryptionAlgorithm EncryptionAlgorithmIdentifier,
        encryptedData   EncryptedData }
        EncryptionAlgorithmIdentifier::=AlgorithmIdentifier
        { CONTENT-ENCRYPTION,
        { KeyEncryptionAlgorithms } }
```

EncryptedData:: = OCTET STRING contendo a versão criptografada da chave de assinatura privada do configurador

[00108] A Figura 10 mostra um diagrama de blocos de um exemplo de dispositivo eletrônico 1000 para implementar aspectos desta divulgação. Em algumas implementações, o dispositivo eletrônico 1000 pode ser semelhante ao primeiro dispositivo configurador 110 ou ao segundo dispositivo configurador 120. O dispositivo eletrônico 1000 pode ser um computador portátil, um computador tipo tablet, um telefone móvel, um console de jogos, um relógio inteligente, dispositivo de realidade aumentada ou virtual, um drone ou outro sistema eletrônico. O dispositivo eletrônico 1000 inclui um processador 1002 (possivelmente incluindo vários processadores, vários núcleos, vários nós, ou implementação de multi-rosqueamento, etc.). O dispositivo eletrônico 1000 inclui uma memória 1006. A memória 1006 pode ser memória do sistema ou qualquer uma ou mais das possíveis realizações descritas abaixo de um meio legível por máquina ou de um meio legível por computador. O dispositivo eletrônico 1000 também pode incluir um barramento 1001 (como PCI, ISA, PCI-Express, HyperTransport, InfiniBand, NuBus, AHB, AXI, etc.). O dispositivo eletrônico pode incluir uma ou mais interfaces de

rede 1004, que podem ser uma interface de rede sem fio (como uma interface WLAN, uma interface Bluetooth®, uma interface WiMAX, uma interface ZigBee®, uma interface USB sem fio, etc.) ou interface de rede com fio (como uma interface de comunicação através de rede elétrica, uma interface Ethernet, etc.). Em algumas implementações, o dispositivo eletrônico 1000 pode suportar múltiplas interfaces de rede 1004, cada uma das quais pode ser configurada para acoplar o dispositivo eletrônico 1000 a uma rede de comunicação diferente. O dispositivo eletrônico pode incluir uma ou mais interfaces de rede 1004, que podem ser uma interface de rede sem fio (como uma interface WLAN, uma interface Bluetooth®, uma interface WiMAX, uma interface ZigBee®, uma interface USB sem fio, etc.) ou interface de rede com fio (como uma interface de comunicação powerline, uma interface Ethernet, etc.). Em algumas implementações, o dispositivo eletrônico 1000 pode suportar múltiplas interfaces de rede 1004, cada uma das quais pode ser configurada para acoplar o dispositivo eletrônico 1000 a uma rede de comunicação diferente. O dispositivo eletrônico pode incluir uma ou mais interfaces de rede 1004, que podem ser uma interface de rede sem fio (como uma interface WLAN, uma interface Bluetooth®, uma interface WiMAX, uma interface ZigBee®, uma interface USB sem fio, etc.) ou interface de rede com fio (como uma interface de comunicação através de rede elétrica, uma interface Ethernet, etc.). Em algumas implementações, o dispositivo eletrônico 1000 pode suportar múltiplas interfaces de rede 1004, cada uma das quais pode ser configurada para acoplar o dispositivo

eletrônico 1000 a um dispositivo eletrônico de rede de comunicação diferente 1000 pode suportar múltiplas interfaces de rede 1004, cada uma das quais pode ser configurada para acoplar o dispositivo eletrônico 1000 a um dispositivo eletrônico de rede de comunicação diferente 1000 pode suportar múltiplas interfaces de rede 1004, cada uma das quais pode ser configurada para acoplar o dispositivo eletrônico 1000 a uma rede de comunicação diferente.

[00109] A memória 1006 inclui funcionalidade para suportar várias implementações descritas acima. A memória 1006 pode incluir uma ou mais funcionalidades que facilitam a implementação de um protocolo de provisionamento de dispositivo. Por exemplo, a memória 1006 pode implementar um ou mais aspectos do primeiro dispositivo configurador 110 ou segundo dispositivo configurador 120 como descrito acima. A memória 1006 pode incorporar funcionalidade para permitir implementações descritas nas Figuras 1 a 9 acima. Em algumas implementações, a memória 1006 pode incluir uma ou mais funcionalidades que facilitam a geração, o armazenamento ou a recuperação do pacote de chave do configurador. O dispositivo eletrônico 1000 pode incluir um módulo de criptografia/decriptografia 1016 ou um módulo de backup/restauração 1055. Por exemplo, o módulo de criptografia/decriptografia 1016 pode facilitar a criptografia de pelo menos parte do pacote de chave do configurador ou a decriptografia do pacote de chave do configurador. O módulo de backup/restauração 1055 pode facilitar o armazenamento do pacote de chave do configurador

e a recuperação do pacote de chave do configurador a partir de um local de armazenamento. O dispositivo eletrônico 1000 também pode incluir outros componentes 1020, como uma unidade de sensor, componentes de interface de usuário ou outro componente de entrada/saída. Em algumas outras implementações, o dispositivo eletrônico 1000 pode ter outros sensores apropriados (como uma câmera, microfone, detector NFC, scanner de código de barras, etc.) usados para obter informações de decriptografia usando uma técnica de bootstrapping.

[00110] Qualquer uma destas funcionalidades pode ser parcialmente (ou inteiramente) implementadas em hardware, tal como no processador 1002. Por exemplo, a funcionalidade pode ser implementada com um circuito integrado específico da aplicação, em lógica implementada no processador 1002, em um co-processador em um dispositivo periférico ou cartão, etc. Além disso, as realizações podem incluir menos ou componentes adicionais não ilustrados na Figura 10 (como placas de vídeo, placas de áudio, interfaces de rede adicionais, dispositivos periféricos, etc.). O processador 1002 e a memória 1006 podem ser acoplados ao barramento 1001. Embora ilustrado como sendo acoplado ao barramento 1001, a memória 1006 pode ser diretamente acoplada ao processador 1002.

[00111] Como usado aqui, uma frase referindo-se a "pelo menos um de uma lista de itens refere-se a qualquer combinação desses itens, incluindo membros individuais. Como exemplo, "pelo menos um de: a, b ou c" é destinado a cobrir: a, b, c, ab, ac, bc e abc.

[00112] Os vários processos de lógica ilustrativa, blocos lógicos, módulos, circuitos e algoritmos descritos em conexão com as implementações aqui divulgadas podem ser implementados como hardware eletrônico, software de computador ou combinações de ambos. A permutabilidade de hardware e software foi descrita em termos gerais, em termos de funcionalidade e ilustrada nos vários componentes ilustrativos, blocos, módulos, circuitos e processos descritos acima. Se tal funcionalidade é implementada em hardware ou software depende da aplicação particular e das restrições de projeto impostas ao sistema como um todo.

[00113] O hardware e dispositivos de processamento de dados usados para implementar as várias lógicas ilustrativas, blocos lógicos, módulos e circuitos descritos em conexão com os aspectos aqui divulgados podem ser implementados ou executados com um processador de um ou vários chips de uso geral, processador de sinal (DSP), um circuito integrado específico de aplicativo (ASIC), uma matriz de portas programáveis em campo (FPGA) ou outro dispositivo lógico programável, lógica discreta de porta ou transistor, componentes de hardware discretos ou qualquer combinação deles projetada para executar as funções descritas aqui. Um processador de uso geral pode ser um microprocessador ou qualquer processador convencional, controlador, microcontrolador ou máquina de estado. Um processador também pode ser implementado como uma combinação de dispositivos de computação, como uma combinação de um DSP e um microprocessador, uma pluralidade de microprocessadores,

um ou mais microprocessadores em conjunto com um núcleo DSP ou qualquer outra configuração desse tipo. Em algumas implementações, processos e métodos particulares podem ser executados por circuitos específicos para uma determinada função.

[00114] Em um ou mais aspectos, as funções descritas podem ser implementadas em hardware, circuitos eletrônicos digitais, software de computador, firmware, incluindo as estruturas divulgadas neste relatório descritivo e seus equivalentes estruturais, ou em qualquer combinação dos mesmos. As implementações da matéria objeto descritas neste relatório descritivo também podem ser implementadas como um ou mais programas de computador, isto é, um ou mais módulos de instruções de programas de computador, codificados em uma mídia de armazenamento de computador para execução por, ou para controlar o aparelho de operação de processamento de dados.

[00115] Se implementado em software, as funções podem ser armazenadas ou transmitidas como uma ou mais instruções ou código em um meio legível por computador. Os processos de um método ou algoritmo divulgados aqui podem ser implementados em um módulo de software executável por processador que pode residir em um meio legível por computador. A mídia legível por computador inclui mídia de armazenamento de computador e mídia de comunicação, incluindo qualquer meio que possa ser ativado para transferir um programa de computador de um lugar para outro. Uma mídia de armazenamento pode ser qualquer mídia disponível que possa

ser acessada por um computador. A título de exemplo, e não limitativo, tais mídias legíveis por computador podem incluir memória cache, RAM (incluindo SRAM, DRAM, RAM de capacitor zero, RAM de transistor duplo, eDRAM, RAM EDO, RAM DDR, EEPROM, NRAM, RRAM, SONOS, PRAM, ou similar), ROM, EEPROM,CD-ROM ou outro armazenamento em disco ótico, armazenamento em disco magnético ou outros dispositivos de armazenamento magnético, ou qualquer outro meio que possa ser usado para armazenar o código de programa desejado na forma de instruções ou estruturas de dados e que possa ser acessado por um computador. Além disso, qualquer conexão pode ser apropriadamente denominada mídia legível por computador. Disquete e disco, como usado aqui, inclui disco compacto (CD), disco laser, disco ótico, disco versátil digital (DVD), disquete e disco Blu-ray™, em que os discos geralmente reproduzem os dados magneticamente, enquanto os discos reproduzem dados oticamente com lasers. As combinações dos itens acima também podem ser incluídas no escopo de mídia legível por computador. Adicionalmente, as operações de um método ou algoritmo podem residir como uma ou qualquer combinação ou conjunto de códigos e instruções em um meio legível por máquina e meio legível por computador, o qual pode ser incorporado em um produto de programa de computador.

[00116] Várias modificações para as implementações descritas nesta divulgação podem ser prontamente aparentes para as pessoas habilitadas na técnica, e os princípios genéricos definidos aqui podem ser aplicados a outras implementações sem se afastar do espírito ou escopo

desta divulgação. Assim, as reivindicações não se destinam a ser limitadas às implementações aqui mostradas, mas devem estar de acordo com o escopo mais amplo consistente com esta divulgação, os princípios e as novas características aqui reveladas.

[00117] Além disso, uma pessoa com habilidade ordinária na técnica irá apreciar prontamente, os termos "superior" e "inferior" são por vezes utilizados para facilitar a descrição das figuras, e indicar posições relativas correspondentes à orientação da figura em uma página corretamente orientada, e pode não refletir a orientação adequada de qualquer dispositivo como implementado.

[00118] Alguns recursos que são descritos neste relatório descritivo no contexto de implementações separadas também podem ser implementados em combinação em uma única implementação. Por outro lado, vários recursos descritos no contexto de uma única implementação também podem ser implementados em várias implementações separadamente ou em qualquer subcombinação adequada. Além disso, embora as características possam ser descritas acima como atuando em certas combinações e até mesmo inicialmente reivindicadas como tal, uma ou mais características de uma combinação reivindicada podem, em alguns casos, ser extirpadas da combinação, e a combinação reivindicada pode ser direcionada a uma subcombinação ou variação de uma subcombinação.

[00119] Da mesma forma, enquanto as operações são representadas nos desenhos em uma ordem particular, isso não

deve ser entendido como exigindo que tais operações sejam realizadas na ordem particular mostrada ou em ordem sequencial, ou que todas as operações ilustradas sejam realizadas, para alcançar resultados desejáveis. Além disso, os desenhos podem representar esquematicamente mais um exemplo de processos na forma de um fluxograma. No entanto, outras operações que não são representadas podem ser incorporadas nos processos de exemplo ilustrados esquematicamente. Por exemplo, uma ou mais operações adicionais podem ser realizadas antes, depois, simultaneamente ou entre qualquer uma das operações. Em determinadas circunstâncias, a multitarefa e o processamento paralelo podem ser vantajosos. Além disso, a separação de vários componentes do sistema nas implementações descritas acima não deve ser entendida como exigindo tal separação em todas as implementações, e deve ser entendido que os componentes e sistemas do programa descritos geralmente podem ser integrados em um único produto de software ou empacotados em vários produtos de software. Além disso, outras implementações estão dentro do escopo das seguintes afirmações. Em alguns casos, as ações citadas nas reivindicações podem ser realizadas em uma ordem diferente e ainda alcançar resultados desejáveis.

REIVINDICAÇÕES

1. Método realizado por um primeiro dispositivo configurador (110) de uma rede, caracterizado pelo fato de que compreende:

implementar, pelo primeiro dispositivo configurador, um protocolo de provisionamento de dispositivo no qual o primeiro dispositivo configurador é capaz de usar uma chave de assinatura privada do configurador para cadastrar um dispositivo de cadastro com a rede;

gerar (310) um pacote de chave do configurador que inclua pelo menos a chave de assinatura privada do configurador associada ao primeiro dispositivo configurador (110);

criptografar (320) pelo menos uma parte do pacote de chave do configurador;

armazenar (330) o pacote de chave do configurador em um local de armazenamento como um backup para restauração subsequente por um segundo dispositivo configurador (120), em que a mesma chave de assinatura privada do configurador e a mesma chave de verificação pública do configurador são compartilhadas entre uma pluralidade de configuradores (110, 120) de uma primeira rede que é capaz de usar a chave de assinatura privada do configurador e uma chave de verificação pública do configurador de acordo com um protocolo de provisionamento para cadastrar diferentes dispositivos de cadastro (150A, 150B) com a primeira rede;

em que a chave de verificação pública do configurador é derivada da chave de assinatura privada do configurador ou obtida a partir do pacote de chave do configurador;

determinar um endereço de localização do pacote de chave do configurador no local de armazenamento; e

fornecer o endereço de localização para o segundo dispositivo configurador.

2. Método, de acordo com a reivindicação 1, caracterizado pelo fato de que o pacote de chave do configurador inclui adicionalmente uma chave de verificação pública do configurador associada com a chave de assinatura privada do configurador.

3. Método, de acordo com a reivindicação 1, caracterizado pelo fato de que criptografar pelo menos a parte do pacote de chave do configurador inclui criptografar o pacote de chave do configurador usando uma chave de criptografia que é diferente da chave de assinatura privada do configurador.

4. Método, de acordo com a reivindicação 1, caracterizado pelo fato de que criptografar pelo menos a parte do pacote de chave do configurador inclui criptografar a chave de assinatura privada do configurador usando uma técnica de criptografia de chave privada, e incluir uma indicação da técnica de criptografia de chave privada em um cabeçalho do pacote de chave do configurador.

5. Método, de acordo com a reivindicação 1, caracterizado pelo fato de que armazenar o pacote de chave do configurador inclui:

gerar um envelope digital que inclui o pacote de chave do configurador e informações de decriptografia, em que as informações de decriptografia permitem que o segundo dispositivo configurador descriptografe pelo menos a parte do pacote de chave do configurador.

6. Método, de acordo com a reivindicação 1, caracterizado pelo fato de que o local de armazenamento é pelo menos um membro selecionado de um grupo consistindo em uma memória do primeiro dispositivo configurador, um local compartilhado na rede, um computador pessoal, um servidor doméstico, um serviço de armazenamento baseado em nuvem e um ponto de acesso, AP, de uma rede sem fio.

7. Método, de acordo com a reivindicação 1, caracterizado pelo fato de que o armazenamento do pacote de chave do configurador inclui armazenar um backup do pacote de chave do configurador, o método compreendendo adicionalmente:

recuperar, pelo primeiro dispositivo configurador, o backup do pacote de chave do configurador a partir do local de armazenamento;

decriptografar pelo menos a parte do pacote de chave do configurador; e

obter a chave de assinatura privada do configurador a partir do pacote de chave do configurador.

8. Método, de acordo com a reivindicação 7, caracterizado pelo fato de que compreende adicionalmente:

determinar uma chave de verificação pública do configurador com base, pelo menos em parte, na chave de assinatura privada do configurador obtida a partir do pacote de chave do configurador.

9. Método, de acordo com a reivindicação 1, caracterizado pelo fato de que compreende adicionalmente:

fornecer informações de decriptografia ao segundo dispositivo configurador, em que as informações de decriptografia permitem que o segundo dispositivo

configurador decriptografe pelo menos a parte do pacote de chave do configurador e obtenha a chave de assinatura privada do configurador.

10. Método, de acordo com a reivindicação 9, caracterizado pelo fato de que as informações de decriptografia incluem pelo menos um membro selecionado de um grupo consistindo em um endereço de localização do pacote de chave do configurador no local de armazenamento e uma chave de criptografia que é utilizável para decriptografar pelo menos a parte do pacote de chave do configurador.

11. Método, de acordo com a reivindicação 9, caracterizado pelo fato de que fornecer as informações de decriptografia inclui fornecer as informações de decriptografia usando pelo menos um membro selecionado de um grupo consistindo em uma tela, um alto-falante, um sinal luminoso, uma interface de sensor e uma interface de frequência de rádio de curto alcance do primeiro dispositivo configurador.

12. Método, de acordo com a reivindicação 9, caracterizado pelo fato de que o fornecimento das informações de decriptografia inclui exibir uma imagem tendo as informações de decriptografia codificadas na mesma, em que a imagem é um código de barras ou uma imagem de código de resposta rápida, QR.

13. Primeiro dispositivo configurador (110), compreendendo:

um processador; e

memória tendo instruções armazenadas na mesma,

o primeiro dispositivo configurador (110) caracterizado pelo fato de que, quando as instruções

armazenadas na memória são executadas pelo processador, fazem com que o primeiro dispositivo configurador (110):

implemente, pelo primeiro dispositivo configurador, um protocolo de provisionamento de dispositivo no qual o primeiro dispositivo configurador é capaz de usar uma chave de assinatura privada do configurador para cadastrar um dispositivo de cadastro com a rede;

gere (310) um pacote de chave do configurador que inclua pelo menos a chave de assinatura privada do configurador associada ao primeiro dispositivo configurador (110);

criptografe (320) pelo menos uma parte do pacote de chave do configurador; e

armazene (330) o pacote de chave do configurador em um local de armazenamento como um backup para a restauração subsequente por um segundo dispositivo configurador (120), em que a mesma chave de assinatura privada do configurador e a mesma chave de verificação pública do configurador são compartilhadas entre uma pluralidade de configuradores (110, 120) de uma primeira rede que é capaz de usar a chave de assinatura privada do configurador e uma chave de verificação pública do configurador de acordo com um protocolo de provisionamento para cadastrar diferentes dispositivos de cadastro (150A, 150B) com a primeira rede;

em que a chave de verificação pública do configurador é derivada da chave de assinatura privada do configurador ou obtida a partir do pacote de chave do configurador;

determinar um endereço de localização do pacote de

chave do configurador no local de armazenamento; e

fornecer o endereço de localização para o segundo dispositivo configurador.

14. Memória legível por computador caracterizada pelo fato de que compreende instruções executáveis para fazer com que pelo menos um computador realize as etapas do método conforme definido em qualquer uma das reivindicações 1 a 12.

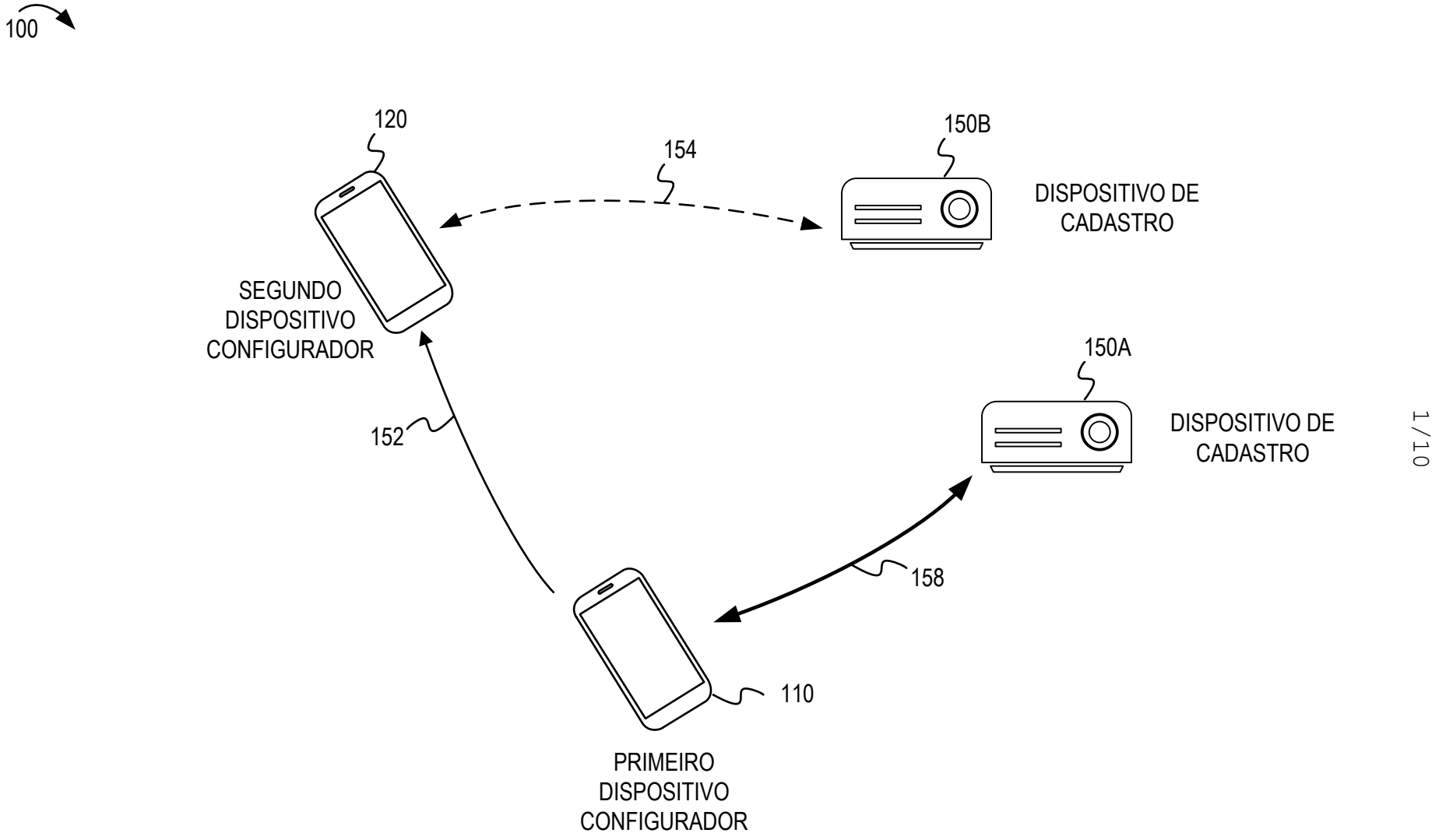
100
120
154
150B
DISPOSITIVO DE CADASTRO
SEGUNDO DISPOSITIVO CONFIGURADOR
150A
152
DISPOSITIVO DE CADASTRO
158
110
PRIMEIRO DISPOSITIVO CONFIGURADOR

FIG. 1

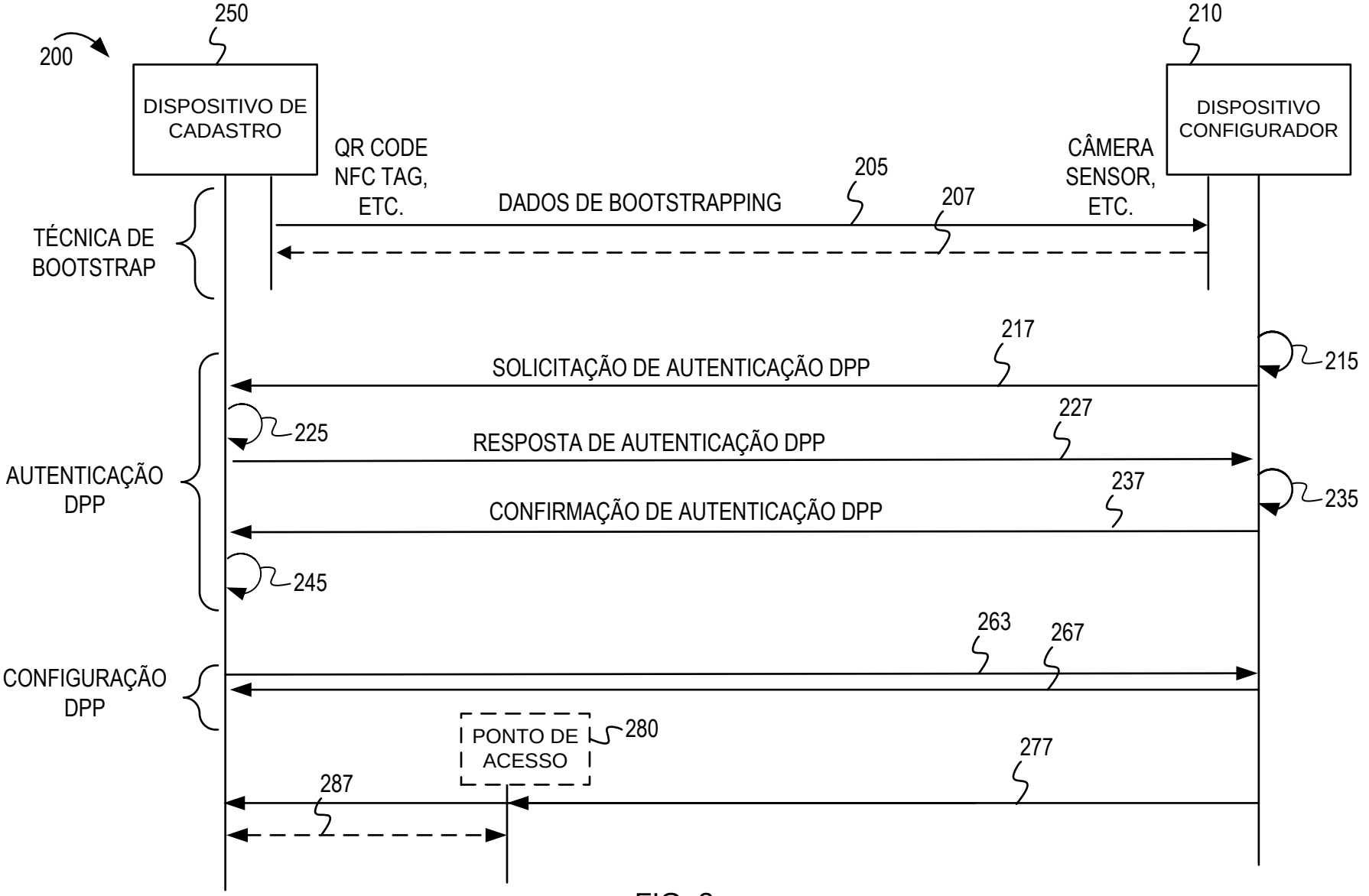
200
250
DISPOSITIVO DE CADASTRO
210
DISPOSITIVO CONFIGURADOR
QR CODE NFC TAG, ETC.
CÂMERA SENSOR, ETC.
205
207
DADOS DE BOOTSTRAPPING
TÉCNICA DE BOOTSTRAP
217
SOLICITAÇÃO DE AUTENTICAÇÃO DPP
215
225
227
RESPOSTA DE AUTENTICAÇÃO DPP
AUTENTICAÇÃO DPP
237
CONFIRMAÇÃO DE AUTENTICAÇÃO DPP
235
245
263
267
CONFIGURAÇÃO DPP
PONTO DE ACESSO
280
277
287

FIG. 2

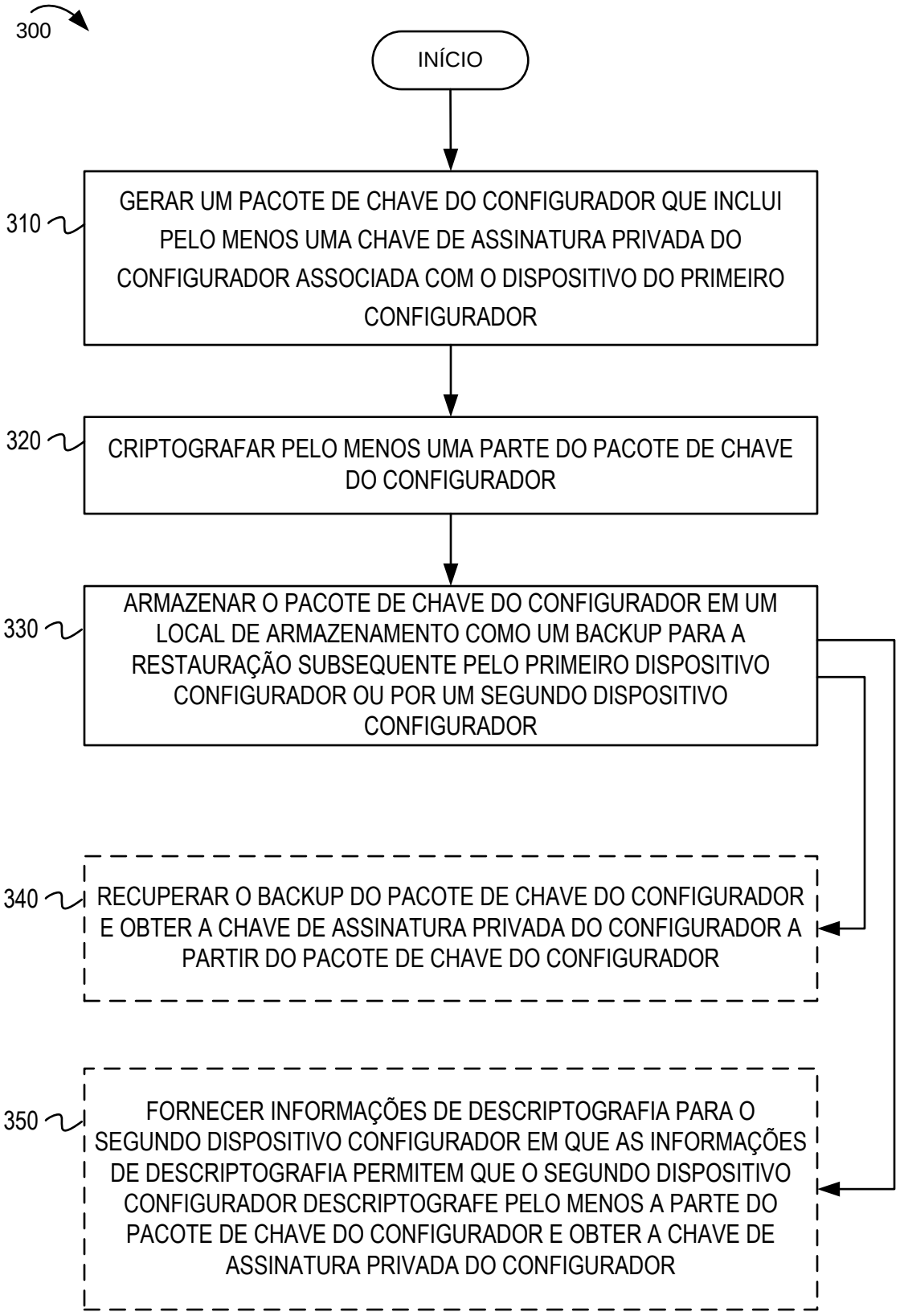
300
INÍCIO
310
GERAR UM PACOTE DE CHAVE DO CONFIGURADOR QUE INCLUI PELO MENOS UMA CHAVE DE ASSINATURA PRIVADA DO CONFIGURADOR ASSOCIADA COM O DISPOSITIVO DO PRIMEIRO CONFIGURADOR
320
CRIPTOGRAFAR PELO MENOS UMA PARTE DO PACOTE DE CHAVE DO CONFIGURADOR
330
ARMAZENAR O PACOTE DE CHAVE DO CONFIGURADOR EM UM LOCAL DE ARMAZENAMENTO COMO UM BACKUP PARA A RESTAURAÇÃO SUBSEQUENTE PELO PRIMEIRO DISPOSITIVO CONFIGURADOR OU POR UM SEGUNDO DISPOSITIVO CONFIGURADOR
340
RECUPERAR O BACKUP DO PACOTE DE CHAVE DO CONFIGURADOR E OBTER A CHAVE DE ASSINATURA PRIVADA DO CONFIGURADOR A PARTIR DO PACOTE DE CHAVE DO CONFIGURADOR
350
FORNECER INFORMAÇÕES DE DESCRIPTOGRAFIA PARA O SEGUNDO DISPOSITIVO CONFIGURADOR EM QUE AS INFORMAÇÕES DE DESCRIPTOGRAFIA PERMITEM QUE O SEGUNDO DISPOSITIVO CONFIGURADOR DESCRIPTOGRAFE PELO MENOS A PARTE DO PACOTE DE CHAVE DO CONFIGURADOR E OBTER A CHAVE DE ASSINATURA PRIVADA DO CONFIGURADOR

FIG. 3

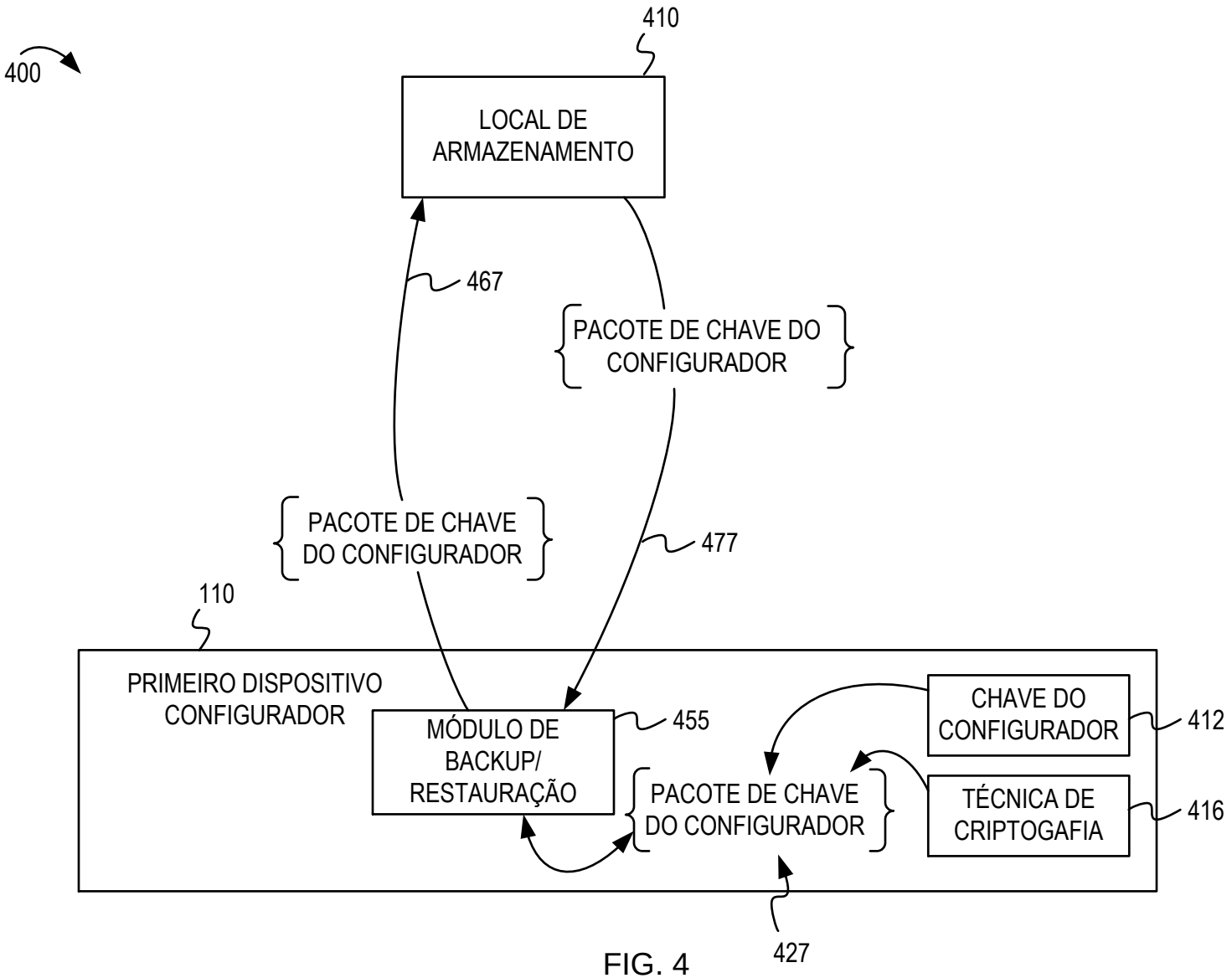
400
410
LOCAL DE ARMAZENAMENTO
467
PACOTE DE CHAVE DO CONFIGURADOR
PACOTE DE CHAVE DO CONFIGURADOR
477
110
PRIMEIRO DISPOSITIVO CONFIGURADOR
MÓDULO DE BACKUP/ RESTAURAÇÃO
455
CHAVE DO CONFIGURADOR
412
PACOTE DE CHAVE DO CONFIGURADOR
TÉCNICA DE CRIPTOGAFIA
416
427

FIG. 4

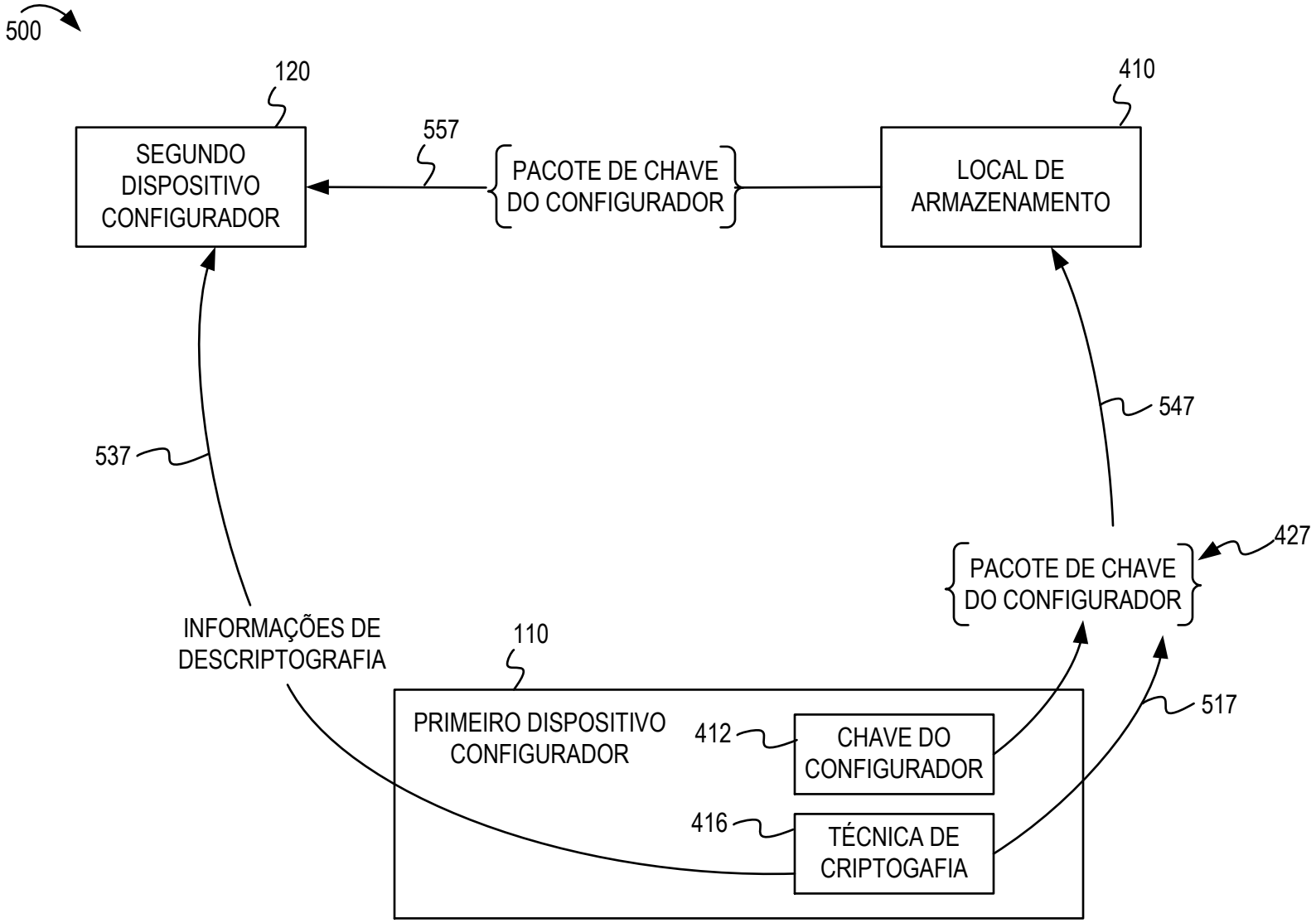
500
120
SEGUNDO DISPOSITIVO CONFIGURADOR
557
PACOTE DE CHAVE DO CONFIGURADOR
410
LOCAL DE ARMAZENAMENTO
537
547
427
PACOTE DE CHAVE DO CONFIGURADOR
INFORMAÇÕES DE DESCRIPTOGRAFIA
110
PRIMEIRO DISPOSITIVO CONFIGURADOR
412
CHAVE DO CONFIGURADOR
517
416
TÉCNICA DE CRIPTOGAFIA

FIG. 5

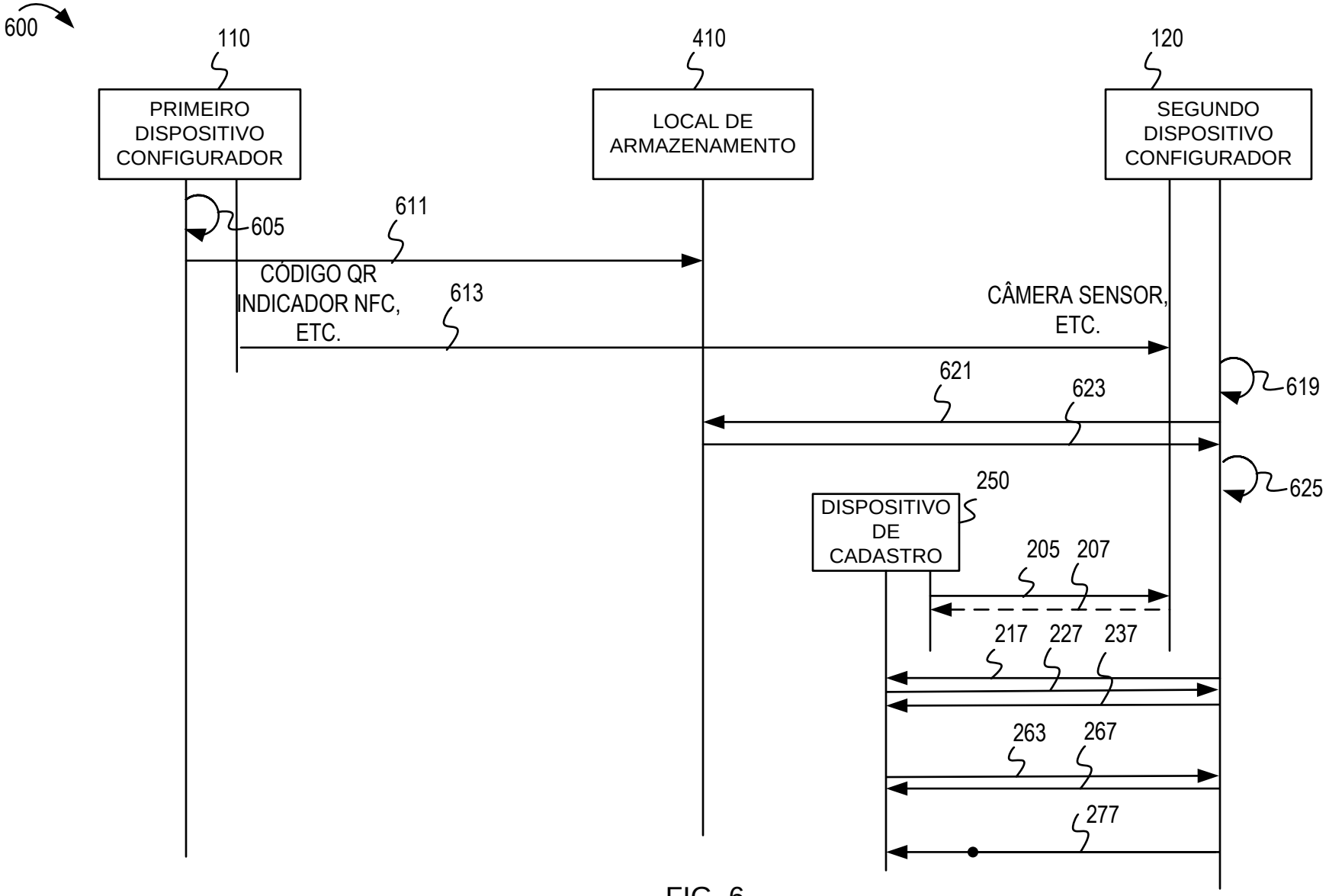
600
110
PRIMEIRO DISPOSITIVO CONFIGURADOR
410
LOCAL DE ARMAZENAMENTO
120
SEGUNDO DISPOSITIVO CONFIGURADOR
605
611
CÓDIGO QR INDICADOR NFC, ETC.
613
CÂMERA SENSOR, ETC.
621
623
619
625
250
DISPOSITIVO DE CADASTRO
205
207
217
227
237
263
267
277

FIG. 6

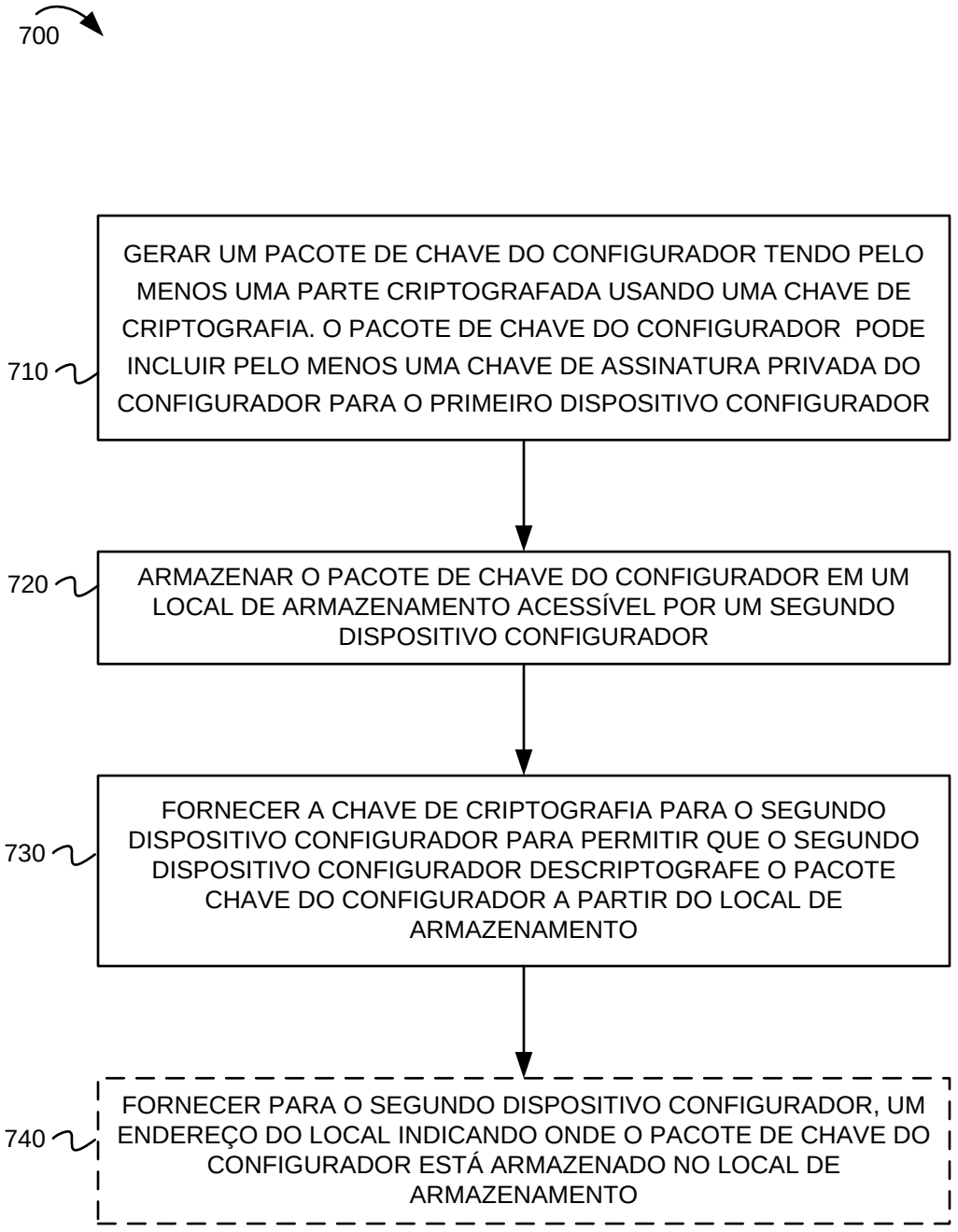
700
GERAR UM PACOTE DE CHAVE DO CONFIGURADOR TENDO PELO MENOS UMA PARTE CRIPTOGRAFADA USANDO UMA CHAVE DE CRIPTOGRAFIA. O PACOTE DE CHAVE DO CONFIGURADOR PODE INCLUIR PELO MENOS UMA CHAVE DE ASSINATURA PRIVADA DO CONFIGURADOR PARA O PRIMEIRO DISPOSITIVO CONFIGURADOR
710
ARMAZENAR O PACOTE DE CHAVE DO CONFIGURADOR EM UM LOCAL DE ARMAZENAMENTO ACESSÍVEL POR UM SEGUNDO DISPOSITIVO CONFIGURADOR
720
FORNECER A CHAVE DE CRIPTOGRAFIA PARA O SEGUNDO DISPOSITIVO CONFIGURADOR PARA PERMITIR QUE O SEGUNDO DISPOSITIVO CONFIGURADOR DESCRIPTOGRAFE O PACOTE CHAVE DO CONFIGURADOR A PARTIR DO LOCAL DE ARMAZENAMENTO
730
FORNECER PARA O SEGUNDO DISPOSITIVO CONFIGURADOR, UM ENDEREÇO DO LOCAL INDICANDO ONDE O PACOTE DE CHAVE DO CONFIGURADOR ESTÁ ARMAZENADO NO LOCAL DE ARMAZENAMENTO
740

FIG. 7

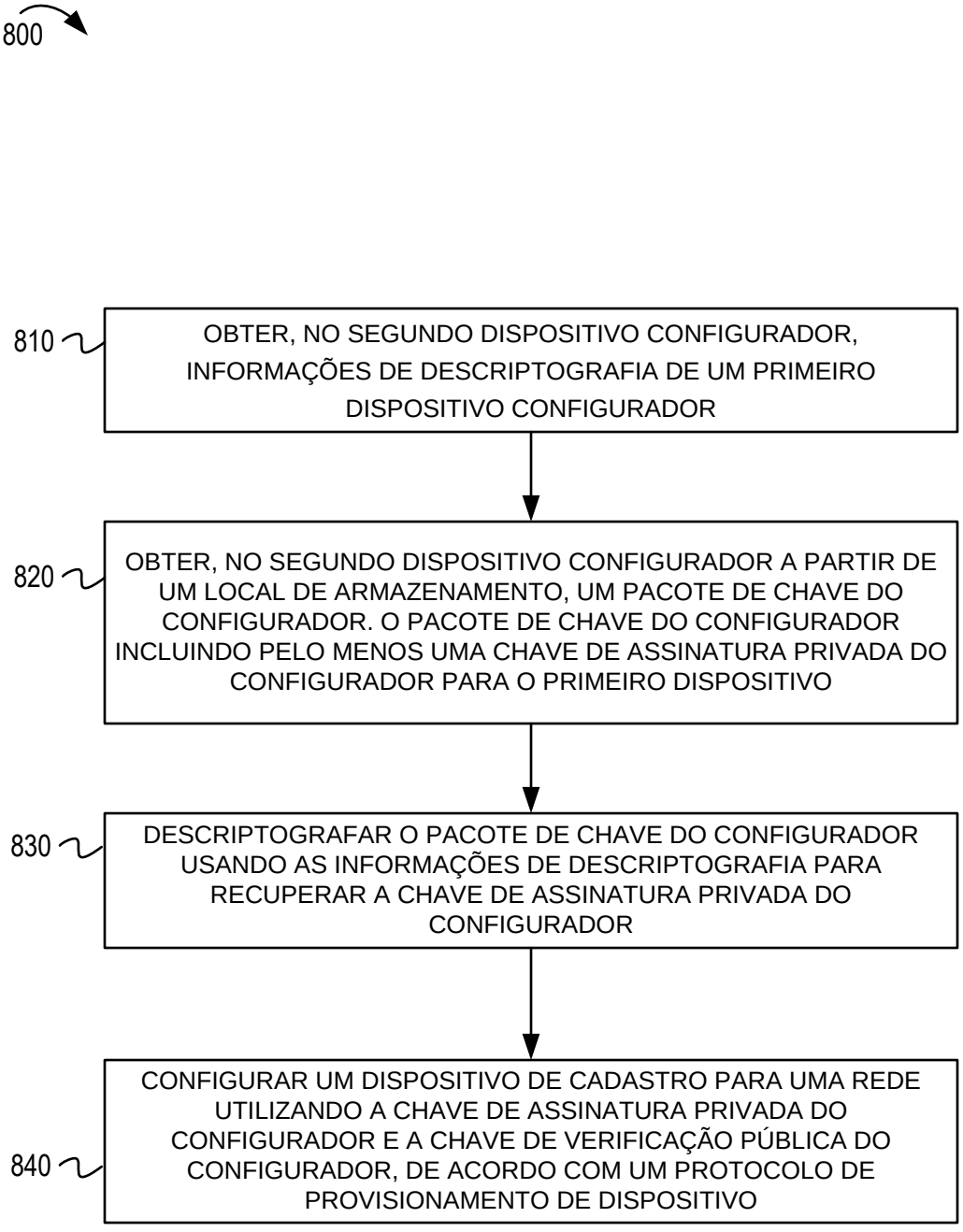
800
810
OBTER, NO SEGUNDO DISPOSITIVO CONFIGURADOR, INFORMAÇÕES DE DESCRIPTOGRAFIA DE UM PRIMEIRO DISPOSITIVO CONFIGURADOR
820
OBTER, NO SEGUNDO DISPOSITIVO CONFIGURADOR A PARTIR DE UM LOCAL DE ARMAZENAMENTO, UM PACOTE DE CHAVE DO CONFIGURADOR. O PACOTE DE CHAVE DO CONFIGURADOR INCLUINDO PELO MENOS UMA CHAVE DE ASSINATURA PRIVADA DO CONFIGURADOR PARA O PRIMEIRO DISPOSITIVO
830
DESCRIPTOGRAFAR O PACOTE DE CHAVE DO CONFIGURADOR USANDO AS INFORMAÇÕES DE DESCRIPTOGRAFIA PARA RECUPERAR A CHAVE DE ASSINATURA PRIVADA DO CONFIGURADOR
840
CONFIGURAR UM DISPOSITIVO DE CADASTRO PARA UMA REDE UTILIZANDO A CHAVE DE ASSINATURA PRIVADA DO CONFIGURADOR E A CHAVE DE VERIFICAÇÃO PÚBLICA DO CONFIGURADOR, DE ACORDO COM UM PROTOCOLO DE PROVISIONAMENTO DE DISPOSITIVO

FIG. 8

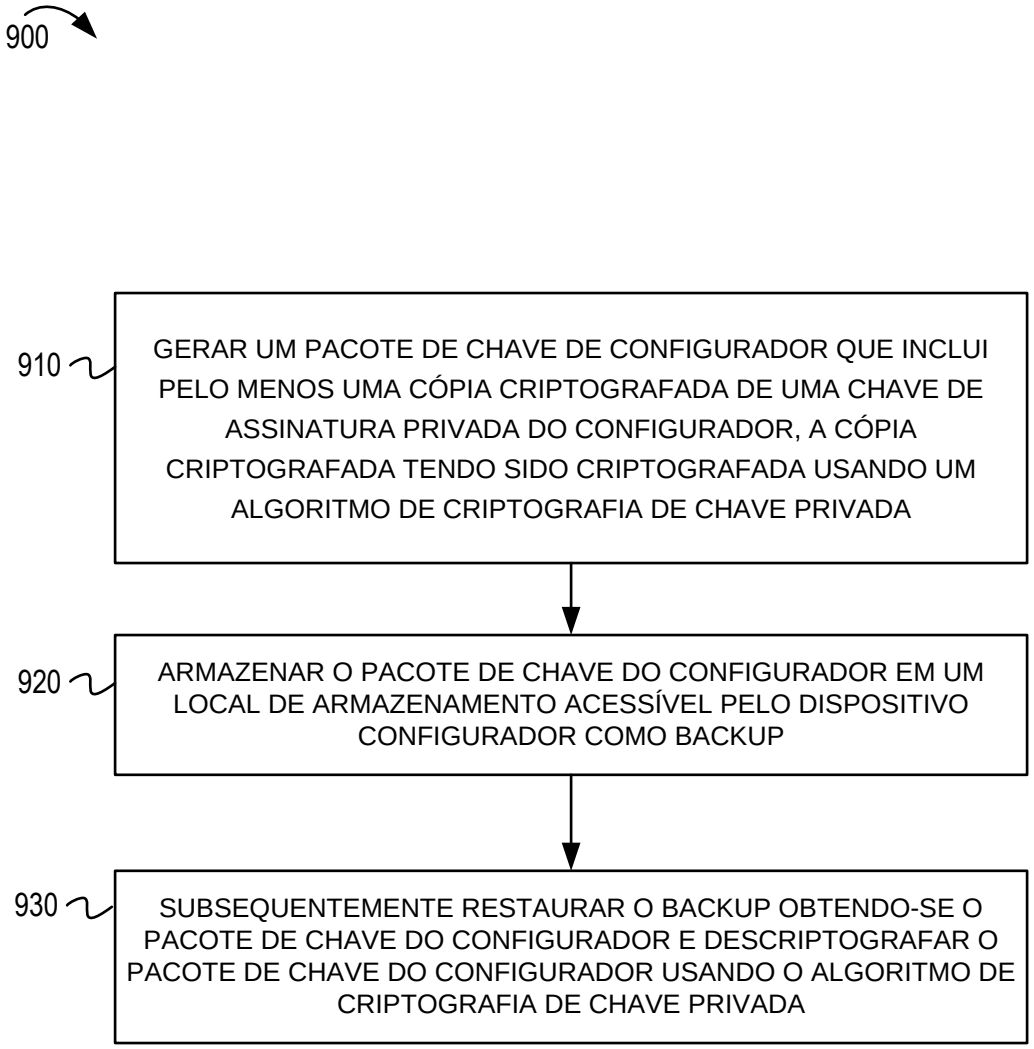
900
910
GERAR UM PACOTE DE CHAVE DE CONFIGURADOR QUE INCLUI PELO MENOS UMA CÓPIA CRIPTOGRAFADA DE UMA CHAVE DE ASSINATURA PRIVADA DO CONFIGURADOR, A CÓPIA CRIPTOGRAFADA TENDO SIDO CRIPTOGRAFADA USANDO UM ALGORITMO DE CRIPTOGRAFIA DE CHAVE PRIVADA
920
ARMAZENAR O PACOTE DE CHAVE DO CONFIGURADOR EM UM LOCAL DE ARMAZENAMENTO ACESSÍVEL PELO DISPOSITIVO CONFIGURADOR COMO BACKUP
930
SUBSEQUENTEMENTE RESTAURAR O BACKUP OBTENDO-SE O PACOTE DE CHAVE DO CONFIGURADOR E DESCRIPTOGRAFAR O PACOTE DE CHAVE DO CONFIGURADOR USANDO O ALGORITMO DE CRIPTOGRAFIA DE CHAVE PRIVADA

FIG. 9

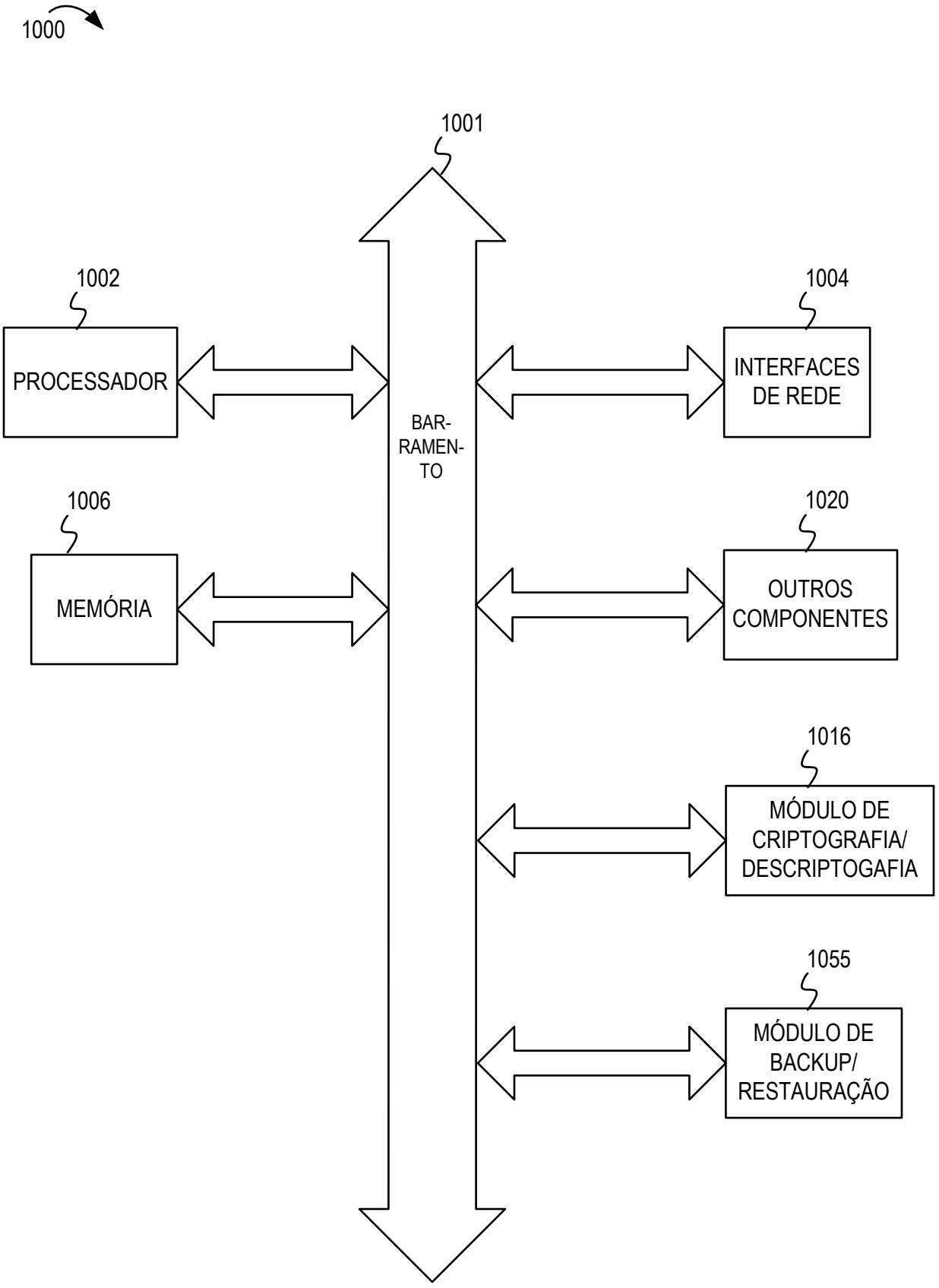
1000
1001
1002
PROCESSADOR
1004
INTERFACES DE REDE
BAR-RAMEN-TO
1006
MEMÓRIA
1020
OUTROS COMPONENTES
1016
MÓDULO DE CRIPTOGRAFIA/ DESCRIPTOGAFIA
1055
MÓDULO DE BACKUP/ RESTAURAÇÃO

FIG. 10