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

(21) BR 112019019327-8 A2

(22) Data do Depósito: 15/03/2018

(43) Data da Publicação Nacional: 14/04/2020

(54) Título: DISPOSITIVO INICIADOR, DISPOSITIVO RESPONDEDOR, SISTEMA DE COMUNICAÇÃO SEM FIO, MÉTODO DO INICIADOR PARA USO EM UM DISPOSITIVO INICIADOR PARA COMUNICAÇÃO SEM FIO COM UM DISPOSITIVO RESPONDEDOR, MÉTODO DO RESPONDEDOR PARA USO EM UM DISPOSITIVO RESPONDEDOR PARA COMUNICAÇÃO SEM FIO COM UM DISPOSITIVO INICIADOR DE ACORDO COM UM PROTOCOLO DE COMUNICAÇÃO E PRODUTO DE PROGRAMA DE COMPUTADOR

(51) Int. Cl.: H04L 29/06; H04L 9/32; H04W 12/06; H04L 9/08; H04W 4/00; (...).

(30) Prioridade Unionista: 20/03/2017 EP 17161856.4.

(71) Depositante(es): KONINKLIJKE PHILIPS N.V..

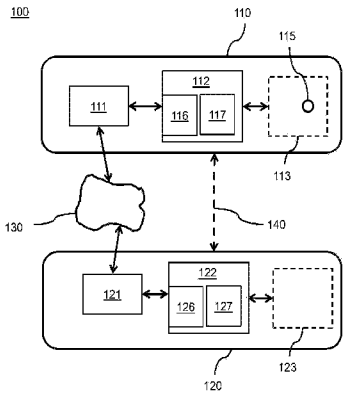
(72) Inventor(es): JOHANNES ARNOLDUS CORNELIS BERNSEN; FRANCISCUS ANTONIUS MARIA VAN DE LAAR; RONALD FELIX ALBERTUS LINDERS.

(86) Pedido PCT: PCT EP2018056491 de 15/03/2018

(87) Publicação PCT: WO 2018/172171 de 27/09/2018

(85) Data da Fase Nacional: 17/09/2019

(57) Resumo: A presente invenção se refere a um sistema de comunicação sem fio que possibilita a autenticação unilateral de um dispositivo respondedor (210) por um dispositivo iniciador (110) e a autenticação mútua de ambos os dispositivos. As modalidades do iniciador podem ter uma unidade de mensagem (116) e uma máquina de estado (117). O iniciador inicia mediante a aquisição de uma chave pública do respondedor através de uma ação fora da banda e envia um pedido de autenticação. O respondedor envia uma resposta de autenticação compreendendo os dados de autenticação do respondedor com base em uma chave privada do respondedor e um estado de andamento mútuo indicativo de que a autenticação mútua está em andamento, para possibilitar que o dispositivo respondedor adquira a chave pública do iniciador através de uma ação fora da banda do respondedor. A máquina de estado do iniciador é disposta de modo a fornecer um estado de autenticação mútua, acionado mediante o recebimento do estado de andamento mútuo, para esperar autenticação mútua. Assim, evita-se períodos longos de interrupção durante a comunicação sem fio, além de possibilitar que o iniciador relate erros de comunicação ao usuário dentro de um curto período de tempo.



DISPOSITIVO INICIADOR, DISPOSITIVO RESPONDEDOR, SISTEMA DE COMUNICAÇÃO SEM FIO, MÉTODO DO INICIADOR PARA USO EM UM DISPOSITIVO INICIADOR PARA COMUNICAÇÃO SEM FIO COM UM DISPOSITIVO RESPONDEDOR, MÉTODO DO RESPONDEDOR PARA USO EM UM DISPOSITIVO RESPONDEDOR PARA COMUNICAÇÃO SEM FIO COM UM DISPOSITIVO INICIADOR DE ACORDO COM UM PROTOCOLO DE COMUNICAÇÃO E PRODUTO DE PROGRAMA DE COMPUTADOR

Campo da invenção

[001] A invenção se refere a um dispositivo iniciador e a um dispositivo respondedor dispostos para comunicação sem fio de acordo com um protocolo de comunicação e a métodos e produtos de programa de computador para uso em tais dispositivos. O protocolo de comunicação compreende um protocolo de autenticação para acomodar uma autenticação sendo uma dentre

[002] - autenticação unilateral do dispositivo respondedor pelo dispositivo iniciador e

[003] - autenticação mútua do dispositivo respondedor pelo dispositivo iniciador e do dispositivo iniciador pelo dispositivo respondedor. O dispositivo respondedor compreende um transceptor do respondedor disposto para comunicação sem fio de acordo com o protocolo de comunicação e um processador do respondedor disposto de modo a processar o protocolo de comunicação. O dispositivo iniciador compreende um transceptor do iniciador disposto para comunicação sem fio de acordo com o protocolo de comunicação e um processador do iniciador disposto de modo a processar o protocolo de comunicação.

[004] A presente invenção se refere ao campo de sistemas de comunicação sem fio de curto alcance, por exemplo,

sistemas de comunicação em ambientes internos e, mais em particular, fornece vários dispositivos e métodos para configurar conexões sem fio com segurança com base na autenticação do dispositivo respondedor e/ou do dispositivo iniciador. O Wi-Fi, consultar ref [1], fornece um exemplo de um protocolo de comunicação e um mecanismo para estabelecer conexões sem fio de dispositivo.

Antecedentes da invenção

[005] As chaves públicas podem ser usadas como um meio para identificar e autenticar dispositivos em comunicação sem fio. A chave privada associada a uma chave pública deve ser gerada em cada dispositivo e protegida de ser revelada. Os dispositivos usam técnicas criptográficas de chave pública para autenticar dispositivos pares, sendo que os dispositivos precisam provar a posse da chave privada correspondente à sua chave pública e estabelecer chaves compartilhadas para comunicações mais seguras. Essa arquitetura de segurança simplifica o estabelecimento de uma conectividade segura entre dispositivos e fornece uma base para uma melhor usabilidade no provisionamento e conexão de dispositivos.

[006] Um dispositivo que inicia um protocolo de autenticação desempenha o papel de Iniciador. O dispositivo que responde a um pedido do Iniciador desempenha o papel de Respondedor. O protocolo de autenticação pode fornecer a autenticação de um respondedor para um iniciador, e opcionalmente, a autenticação do iniciador para o respondedor. Isso pressupõe que o iniciador tenha obtido uma chave de carga inicial (*bootstrapping*) do respondedor para realizar autenticação unidirecional, e ambas as partes tenham obtido

entre si as chaves de carga inicial para, opcionalmente, executar autenticação mútua.

[007] Diffie-Hellman, consultar ref [6], é uma técnica bem conhecida para estabelecer uma chave secreta entre duas partes, sendo que a comunicação entre as partes não revela quaisquer informações a terceiros sobre a chave secreta estabelecida. Cada uma das duas partes usa seu próprio par de chaves pública/privada e troca entre si a chave pública. Cada parte pode calcular a chave secreta com o uso de sua própria chave privada e da chave pública da outra parte e, possivelmente, algumas outras informações, por exemplo, um *nonce* (número aleatório) de cada parte. Cada parte pode gerar um novo par de chaves cada vez que realizar a técnica Diffie-Hellman ou pode reutilizar um par de chaves mais antigo.

[008] Ao executar a técnica Diffie-Hellman através de uma rede, um dispositivo que recebe uma chave pública para executar a técnica Diffie-Hellman não sabe a partir de qual dispositivo essa chave pública foi recebida. Isso pode ser explorado por um invasor em um assim chamado ataque intermediário. Um invasor E poderia se disfarçar como o verdadeiro dispositivo B com o qual o dispositivo A deseja se conectar. O invasor E executa a técnica Diffie-Hellman como dispositivo A e estabelece uma chave secreta “Kae” com o dispositivo A. De modo similar, o invasor se disfarça como o dispositivo A para o dispositivo B e estabelece uma chave secreta “Kbe” com o dispositivo B. Quando uma mensagem vem de um dos dispositivos A ou B, o invasor descriptografa a mensagem com a uma chave secreta, a criptografa com a outra e a encaminha para o outro dispositivo. Dessa forma, os dispositivos A e B não notam nada de estranho em sua comunicação, exceto por algum

atraso adicional. Mas o invasor tem pleno conhecimento sobre o que eles estão comunicando.

[009] Para aumentar a segurança da comunicação sem fio, um protocolo pode ser usado para autenticação de um ou mais dos dispositivos que participam em comunicação sem fio segura de acordo com um protocolo de comunicação. Tal protocolo de autenticação pode ser iniciado por um primeiro dispositivo participante, geralmente chamado de um dispositivo iniciador, em comunicação com um segundo dispositivo participante, geralmente chamado de dispositivo respondedor. No contexto atual, um dispositivo iniciador pode ser qualquer dispositivo eletrônico que tenha a capacidade de configurar uma conexão com o uso de comunicação sem fio. O dispositivo iniciador pode ser um dispositivo estacionário como um PC ou um ponto de acesso ou uma estação de ancoragem sem fio ou um hub USB sem fio, ou um monitor de vídeo ou AV sem fio, mas pode também ser um dispositivo portátil como um laptop ou um telefone móvel. O dispositivo respondedor, de modo similar, pode ser qualquer tipo de dispositivo eletrônico que tem a capacidade de configurar uma conexão com o uso de comunicação sem fio.

[010] Então, um protocolo de comunicação pode incluir um protocolo de autenticação para acomodar uma autenticação do respondedor e/ou do iniciador. A autenticação pode ser uma autenticação unilateral do dispositivo respondedor pelo dispositivo iniciador. Além disso, a autenticação pode ser autenticação mútua, que envolve a autenticação do dispositivo respondedor pelo dispositivo iniciador e a autenticação do dispositivo iniciador pelo dispositivo respondedor.

Sumário da invenção

[011] Em tais protocolos de autenticação, por exemplo, para impedir os ataques intermediários ao usar Diffie-Hellman, uma outra forma de comunicação pode ser usada para trocar as chaves públicas, ou hashes das chaves públicas, ou seja, além do canal de comunicação sem fio usado de acordo com o protocolo de comunicação sem fio, que é geralmente chamado de comunicação em banda. A outra forma de comunicação é comumente denominada de comunicação Fora-de-Banda (OOB, *out-of-band*), por exemplo, com o uso de um marcador visual como um código de barras ou na qual o usuário insere um código.

[012] Além disso, os protocolos de comunicação comumente têm um mecanismo para lidar com ruído e perturbações da troca de mensagens sem fio. Por exemplo, quando nenhuma resposta é recebida dentro de um período de tempo predeterminado, a mensagem é transmitida novamente. Após um número predeterminado de tentativas, o protocolo de comunicação pode ser abortado.

[013] É um objetivo da invenção fornecer um sistema seguro de comunicação sem fio para configurar confiavelmente uma conexão entre um dispositivo iniciador e um dispositivo respondedor, ao mesmo tempo em que evita longos períodos de interrupção indevida durante a autenticação.

[014] Para esse propósito, são fornecidos dispositivos e métodos definidos nas reivindicações anexas.

[015] De acordo com um aspecto da presente invenção, um dispositivo iniciador disposto para comunicação sem fio com um dispositivo respondedor de acordo com um protocolo de comunicação, sendo que o protocolo de comunicação compreende um protocolo de autenticação para acomodar uma autenticação sendo uma dentre

[016] - autenticação unilateral do dispositivo respondedor pelo dispositivo iniciador e

[017] - autenticação mútua do dispositivo respondedor pelo dispositivo iniciador e do dispositivo iniciador pelo dispositivo respondedor;

[018] sendo que o dispositivo respondedor compreende:

[019] - um transceptor do respondedor disposto para comunicação sem fio de acordo com o protocolo de comunicação e

[020] - um processador do respondedor disposto de modo a processar o protocolo de comunicação, sendo que o dispositivo iniciador compreende

[021] - um transceptor do iniciador disposto para comunicação sem fio de acordo com o protocolo de comunicação,

[022] - um processador do iniciador disposto de modo a processar o protocolo de comunicação e que tem

[023] - uma unidade de mensagem do iniciador para compor mensagens a serem enviadas para o dispositivo respondedor e para decompor mensagens recebidas a partir do dispositivo respondedor de acordo com o protocolo de autenticação; e

[024] - uma máquina de estado do iniciador para fornecer estados do iniciador de acordo com o protocolo de autenticação dependentes da interação com o usuário e das mensagens recebidas a partir do dispositivo respondedor, sendo que os estados do iniciador compreendem

[025] um estado inicial para carga inicial mediante a aquisição de uma chave pública do respondedor

proveniente do dispositivo respondedor através de uma ação fora da banda do iniciador,

[026] um estado de carga inicial indicativo de que a carga inicial foi executada corretamente mediante a aquisição da chave pública do respondedor, e

[027] um estado autenticado indicativo de que a autenticação foi executada corretamente;

[028] sendo que a unidade de mensagem do iniciador é disposta de modo a compor mensagens que compreendem

[029] - um pedido de autenticação a ser enviado no estado de carga inicial e que compreende um verificador do iniciador para verificar uma chave pública do iniciador e um verificador do respondedor para verificar a chave pública do respondedor;

[030] e disposta para decompor as mensagens que compreendem

[031] - uma resposta de autenticação que compreende dados de autenticação unilateral do respondedor com base em uma chave privada do respondedor que corresponde à chave pública do respondedor e em um estado de andamento mútuo indicativo da autenticação mútua estar em andamento para possibilitar que o dispositivo respondedor adquira a chave pública do iniciador a partir do dispositivo iniciador através de uma ação fora da banda do respondedor; e

[032] disposta de modo a compor

[033] - uma confirmação de autenticação mútua que compreende um estado de confirmação mútua que indica a confirmação da autenticação mútua e dados de autenticação mútua do iniciador baseados na chave pública do respondedor e em uma

chave privada do iniciador correspondente à chave pública do iniciador.

[034] De acordo com um aspecto adicional da presente invenção, além de um método de autenticação unilateral ou como uma alternativa, pode-se realizar uma autenticação mútua do dispositivo respondedor pelo dispositivo iniciador e do dispositivo iniciador pelo dispositivo respondedor. De acordo com esse aspecto, a máquina de estado do iniciador é disposta de modo a fornecer um estado de autenticação mútua, acionado mediante o recebimento do estado de andamento mútuo, para esperar autenticação mútua; e

[035] a unidade de mensagem do iniciador é disposta de modo a decompor

[036] - uma resposta de autenticação mútua que compreende dados de autenticação mútua do respondedor com base na chave pública do iniciador e na chave privada do respondedor; e

[037] a máquina de estado do iniciador é disposta de modo a ativar o estado autenticado mediante o recebimento da resposta de autenticação mútua e o processador do iniciador processar corretamente os dados de autenticação mútua do respondedor com base na chave pública do respondedor e em uma chave privada do iniciador correspondente à chave pública do iniciador.

[038] De acordo com um aspecto adicional da presente invenção, um dispositivo respondedor é disposto para comunicação sem fio com um dispositivo iniciador de acordo com um protocolo de comunicação, sendo que o protocolo de comunicação compreende um protocolo de autenticação para acomodar uma autenticação sendo uma dentre

[039] - autenticação unilateral do dispositivo respondedor pelo dispositivo iniciador e

[040] - autenticação mútua do dispositivo respondedor pelo dispositivo iniciador e do dispositivo iniciador pelo dispositivo respondedor;

[041] sendo que o dispositivo iniciador compreende:

[042] - um transceptor do iniciador disposto para comunicação sem fio de acordo com o protocolo de comunicação,

[043] - um processador do iniciador disposto de modo a processar o protocolo de comunicação, e sendo que o dispositivo respondedor compreende

[044] - um transceptor do respondedor disposto para comunicação sem fio de acordo com o protocolo de comunicação,

[045] - um processador do respondedor disposto de modo a processar o protocolo de comunicação e que tem

[046] - uma unidade de mensagem do respondedor para compor mensagens a serem enviadas para o dispositivo iniciador e para decompor mensagens recebidas a partir do dispositivo iniciador de acordo com o protocolo de autenticação,

[047] - uma máquina de estado do respondedor para fornecer estados do respondedor de acordo com o protocolo de autenticação dependentes da interação com o usuário e das mensagens recebidas a partir do dispositivo iniciador, sendo que os estados do respondedor compreendem

[048] um estado de espera para receber mensagens a partir do iniciador, e

[049] um estado autenticado do respondedor indicando que a autenticação foi realizada corretamente;

[050] a unidade de mensagem do respondedor é disposta de modo a compor mensagens que compreendem

[051] - uma resposta de autenticação que compreende dados de autenticação unilateral do respondedor com base em uma chave privada do respondedor correspondente à chave pública do respondedor e em um estado de andamento mútuo indicativo da autenticação mútua estar em andamento;

[052] e disposta para decompor as mensagens que compreendem

[053] - um pedido de autenticação que compreende um verificador do iniciador para verificar uma chave pública do iniciador e um verificador do respondedor para verificar a chave pública do respondedor.

[054] De acordo com um aspecto adicional da presente invenção, além de um método de autenticação unilateral ou como uma alternativa, pode-se realizar uma autenticação mútua do dispositivo respondedor pelo dispositivo iniciador e do dispositivo iniciador pelo dispositivo respondedor. De acordo com esse aspecto, a máquina de estado do respondedor é disposta

[055] - para fornecer um estado de autenticação mútua do respondedor para possibilitar que o dispositivo respondedor adquira uma chave pública do iniciador a partir do dispositivo iniciador através de uma ação fora da banda do respondedor; e

[056] a unidade de mensagem do respondedor é disposta de modo a compor

[057] - uma resposta de autenticação mútua a ser enviada no estado de autenticação mútua do respondedor e que compreende dados de autenticação mútua do respondedor com base na chave pública do iniciador e em uma chave privada do respondedor correspondente à chave pública do respondedor;

[058] e disposta de modo a decompor

[059] - uma confirmação de autenticação mútua que compreende um estado de confirmação mútua indicando a confirmação da autenticação mútua e dados de autenticação mútua do iniciador com base na chave pública do respondedor e em uma chave privada do iniciador correspondente à chave pública do iniciador;

[060] sendo que a máquina de estado do respondedor está disposta de modo a, após o processador do respondedor processar corretamente os dados de autenticação do iniciador com base na chave pública do iniciador e na chave privada do respondedor, ativar o estado autenticado do respondedor.

[061] De acordo com um aspecto da presente invenção, é fornecido um método iniciador para uso em um dispositivo iniciador para comunicação sem fio com um dispositivo respondedor de acordo com um protocolo de comunicação, sendo que o protocolo de comunicação compreende um protocolo de autenticação para acomodar uma autenticação sendo uma dentre

[062] - autenticação unilateral do dispositivo respondedor pelo dispositivo iniciador e

[063] - autenticação mútua do dispositivo respondedor pelo dispositivo iniciador e do dispositivo iniciador pelo dispositivo respondedor;

[064] sendo que o método compreende

[065] - fornecer estados do iniciador de acordo com o protocolo de autenticação dependentes da interação com o usuário e das mensagens recebidas a partir do dispositivo respondedor, sendo que os estados do iniciador compreendem

[066] um estado inicial para carga inicial mediante a aquisição de uma chave pública do respondedor proveniente do dispositivo respondedor através de uma ação fora da banda do iniciador,

[067] um estado de carga inicial indicativo de que a carga inicial foi executada corretamente mediante a aquisição da chave pública do respondedor, e

[068] um estado autenticado indicativo de que a autenticação foi executada corretamente;

[069] - compor um pedido de autenticação a ser enviado no estado de carga inicial e que compreende um verificador do iniciador para verificar uma chave pública do iniciador e um verificador do respondedor para verificar a chave pública do respondedor;

[070] - decompor uma resposta de autenticação que compreende dados de autenticação unilateral do respondedor com base em uma chave privada do respondedor correspondente à chave pública do respondedor e um estado de andamento mútuo indicativo da autenticação mútua estar em andamento para possibilitar que o dispositivo respondedor adquira a chave pública do iniciador a partir do dispositivo iniciador através de uma ação fora da banda do respondedor;

[071] - fornecer um estado de autenticação mútua, ativado mediante o recebimento do estado de andamento mútuo, para esperar autenticação mútua;

[072] - decompor uma resposta de autenticação mútua que compreende os dados de autenticação mútua do respondedor com base na chave pública do iniciador e na chave privada do respondedor;

[073] - compor uma confirmação de autenticação mútua que compreende um estado de confirmação mútua que indica a confirmação da autenticação mútua e dados de autenticação mútua do iniciador com base na chave pública do respondedor e em uma chave privada do iniciador correspondente à chave pública do iniciador; e

[074] - ativar o estado autenticado mediante o recebimento da resposta de autenticação mútua e processar corretamente os dados de autenticação mútua do respondedor com base na chave pública do respondedor e em uma chave privada do iniciador correspondente à chave pública do iniciador.

[075] De acordo com um outro aspecto da presente invenção, é fornecido um método respondedor para uso em um dispositivo respondedor para comunicação sem fio com um dispositivo iniciador de acordo com um protocolo de comunicação, sendo que o protocolo de comunicação compreende um protocolo de autenticação para acomodar uma autenticação sendo uma dentre

[076] - autenticação unilateral do dispositivo respondedor pelo dispositivo iniciador e

[077] - autenticação mútua do dispositivo respondedor pelo dispositivo iniciador e do dispositivo iniciador pelo dispositivo respondedor;

[078] sendo que o método compreende

[079] - fornecer estados do respondedor de acordo com o protocolo de autenticação dependentes da interação com o usuário e das mensagens recebidas a partir do dispositivo iniciador, sendo que os estados do respondedor compreendem

[080] um estado de espera para receber mensagens a partir do iniciador, e

[081] um estado autenticado do respondedor indicando que a autenticação foi realizada corretamente;

[082] - compor uma resposta de autenticação que compreende dados de autenticação unilateral do respondedor com base em uma chave privada do respondedor correspondente à chave pública do respondedor e em um estado de andamento mútuo indicativo de que a autenticação mútua está em andamento;

[083] - decompor um pedido de autenticação que compreende um verificador do iniciador para verificar uma chave pública do iniciador e um verificador do respondedor para verificar a chave pública do respondedor;

[084] - ativar o estado de autenticação do respondedor mediante o processamento correto do pedido de autenticação;

[085] - fornecer um estado de autenticação mútua do respondedor para possibilitar que o dispositivo respondedor adquira uma chave pública do iniciador a partir do dispositivo iniciador através de uma ação fora da banda do respondedor;

[086] - compor uma resposta de autenticação mútua a ser enviada no estado de autenticação mútua do respondedor e que compreende dados de autenticação mútua do respondedor com base na chave pública do iniciador e em uma

chave privada do respondedor correspondente à chave pública do respondedor;

[087] - decompor uma confirmação de autenticação mútua que compreende um estado de confirmação mútua indicando a confirmação da autenticação mútua e dados de autenticação mútua do iniciador com base na chave pública do respondedor e em uma chave privada do iniciador correspondente à chave pública do iniciador;

[088] - ativar o estado autenticado do respondedor mediante o processamento correto dos dados de autenticação mútua do iniciador com base na chave pública do iniciador e na chave privada do respondedor.

[089] De acordo com um outro aspecto da invenção, é fornecido um produto de programa de computador transferível por download de uma rede e/ou armazenado em uma mídia legível por computador e/ou mídia executável por microprocessador, sendo que o produto compreende instruções de código de programa para implementar os métodos acima quando executado em um computador.

[090] Os recursos acima têm o efeito de fazer com que o protocolo de autenticação suporte tanto a autenticação unilateral e quanto a comunicação mútua. O protocolo é executado mediante a troca de várias mensagens, que podem ser compostas e decompostas pelas respectivas unidades de mensagem responsiva e iniciadora. Além disso, a sequência de troca das mensagens e processamento de elementos nas mensagens pode ser controlada através de respectivas máquinas de estado do respondedor e do iniciador, as quais determinam os estados dos dispositivos iniciador e respondedor durante a execução do protocolo de autenticação.

[091] Além disso, o protocolo de autenticação possibilita o uso de comunicação fora da banda (OOB, *out-of-band*) para adquirir uma chave pública do respondedor a partir do dispositivo respondedor. A ação fora da banda no lado do iniciador pode envolver receber a própria chave pública do respondedor ou dados codificados da chave pública do respondedor para verificar uma chave pública do respondedor recebida através de uma outra ação de comunicação, por exemplo, recebida em uma mensagem na banda ou armazenou em uma sessão de comunicação prévia. O processo de aquisição de uma quantidade inicial de material de chave é chamado de *bootstrapping* (carga inicial). Depois de uma carga inicial bem-sucedida, o iniciador pode ativar o estado de autenticação para executar a autenticação do dispositivo respondedor.

[092] Entretanto, no caso de uma autenticação mútua, o dispositivo respondedor tem que adquirir uma chave pública do iniciador a partir do dispositivo iniciador através de uma ação fora da banda do respondedor; A troca de códigos através de comunicação OOB pode demorar muito, por exemplo, se a interação com o usuário envolver tanto ler um código no dispositivo iniciador como inseri-lo no dispositivo respondedor ou tirar uma foto de um código legível por máquina como um código de barras ou um código QR sobre o dispositivo iniciador (na ordem de décimos de segundos). Esse tempo é longo comparado ao tempo para trocar mensagens através de comunicação sem fio (geralmente milissegundos ou menos). O dispositivo iniciador pode permanecer, após o envio do pedido de autenticação, à espera da resposta de autenticação. Para possibilitar a dita autenticação mútua, uma resposta de autenticação completa precisa fornecer os dados de

autenticação do respondedor com base também na chave pública do iniciador. Os inventores constataram que a resposta de autenticação completa pode ser transmitida apenas após um período de tempo relativamente longo suficiente para a ação de OOB do respondedor. Portanto, um longo período de interrupção seria necessário em um protocolo de autenticação mútua tradicional. Desvantajosamente, no caso de o pedido de autenticação não ser recebido, por exemplo, devido a um ruído, uma retransmissão ocorreria apenas após o dito longo período de interrupção.

[093] Além disso, no caso de o pedido de autenticação não ser recebido ou no caso de a resposta de autenticação conter dados errôneos fazendo com a autenticação falhe, o usuário tem que esperar muito tempo antes de o dispositivo iniciador poder avisar o usuário de que a autenticação falhou. Para evitar tais longos períodos de interrupção, a invenção fornece a resposta de autenticação contendo os dados de autenticação do respondedor com base em uma chave privada do respondedor correspondendo à chave pública do respondedor, que não envolve qualquer chave do iniciador. Vantajosamente, tal resposta de autenticação pode ser transmitida diretamente após o processamento do pedido de autenticação, possibilitando um curto período de interrupção no dispositivo iniciador mediante o envio do pedido de autenticação. Portanto, no caso de ruído, uma nova transmissão ocorrerá com base em tal curto período de interrupção e o usuário saberá muito mais rápido quando uma tentativa de autenticação falhou.

[094] Além disso, os inventores observaram que tal resposta de autenticação pode ser similar à resposta para

autenticação unilateral. No entanto, será realizada a autenticação mútua. Então, além disso, a resposta de autenticação aprimorada acima mencionada contém ainda um estado de andamento mútuo indicativo de que a autenticação mútua está em andamento. Da mesma forma, a máquina de estado do iniciador é disposta de modo a fornecer um estado de autenticação mútua, acionado mediante o recebimento do estado de andamento mútuo, para esperar autenticação mútua. Vantajosamente, em tal estado de autenticação mútua, o dispositivo iniciador está ciente da autenticação mútua, o que possibilita mais tarde receber a resposta de autenticação mútua que compreende os dados de autenticação mútua do respondedor com base na chave pública do iniciador e na chave privada do respondedor. Subsequentemente, no caso de processamento correto dos dados de autenticação mútua do respondedor recebidos, o iniciador transmite a confirmação de autenticação mútua que compreende um estado de confirmação mútua indicando a confirmação da autenticação mútua e dados de autenticação do iniciador com base na chave pública do respondedor e em uma chave privada do iniciador correspondente à chave pública do iniciador.

[095] Portanto, mediante o fornecimento do estado de autenticação mútua e estado de andamento adicionais na primeira mensagem de resposta de autenticação, a autenticação mútua é realizada sem a necessidade de longos períodos de interrupção, ao mesmo tempo em que, no mesmo protocolo de autenticação, também possibilita a autenticação unilateral. Vantajosamente, em caso de más condições para comunicação sem fio, a retransmissão das mensagens necessárias

é relativamente rápida devido aos curtos períodos de interrupção.

[096] Um método de acordo com a invenção pode ser implementado em um computador como um método implementado por computador, ou em um hardware dedicado, ou em uma combinação de ambos. O código executável para um método de acordo com a invenção pode ser armazenado em um produto de programa de computador. Exemplos de produtos de programa de computador incluem dispositivos de memória, como um pen-drive, dispositivos de armazenamento óptico, como um disco óptico, circuitos integrados, servidores, software online etc. O produto de programa de computador pode compreender meios de código de programa não transitórios armazenados em uma mídia legível por computador para realizar um método de acordo com a invenção, quando o dito produto de programa é executado em um computador. Em uma modalidade, o programa de computador compreende meios de código de programa de computador adaptados para executar todas as etapas ou estágios de um método de acordo com a invenção, quando o programa de computador é executado em um computador. De preferência, o programa de computador é incorporado em uma mídia legível por computador. É fornecido um produto de programa de computador que pode ser obtido por download de uma rede e/ou armazenado em uma mídia legível por computador e/ou uma mídia executável por microprocessador, sendo que o produto compreende instruções de código de programa para implementar um método conforme descrito acima quando executado em um computador.

[097] Um outro aspecto da invenção apresenta um método para produção do programa de computador disponível para transferência por download, por exemplo, incluído em um

aplicativo. Este aspecto é usado quando o programa de computador é transferido via upload para, por exemplo, a App Store da Apple, a Play Store da Google ou a Windows Store da Microsoft, e quando o programa de computador está disponível para download a partir de tal loja.

[098] São apresentadas modalidades preferenciais adicionais dos dispositivos e dos métodos de acordo com a invenção nas reivindicações anexas, cuja revelação está aqui incorporada a título de referência.

Breve descrição dos desenhos

[099] Esses e outros aspectos da invenção se tornarão evidentes e serão adicionalmente elucidados por referência às modalidades descritas a título de exemplo na descrição a seguir e por referência aos desenhos anexos, nos quais:

[100] a Figura 1 mostra dispositivos para comunicação sem fio e autenticação,

[101] a Figura 2 mostra um diagrama esquemático de um protocolo de autenticação,

[102] a Figura 3 mostra um exemplo de uma máquina de estado do iniciador,

[103] a Figura 4 mostra um exemplo de uma máquina de estado do respondedor,

[104] a Figura 5 mostra um método para um iniciador,

[105] a Figura 6 mostra um método para um respondedor,

[106] a Figura 7a mostra uma mídia legível por computador, e

[107] a Figura 7b mostra uma representação esquemática de um sistema processador.

[108] As Figuras são puramente diagramáticas e não estão em escala. Nas figuras, os elementos que correspondem a elementos já descritos podem ter as mesmas referências numéricas.

Descrição detalhada das modalidades

[109] As seguintes abreviações são usadas:

[110] Estados:

[111] IST Estado inicial

[112] BST Bootstrapped (carga inicial)

[113] AG1 Autenticação (iniciador, sentido único)

[114] AG2 Autenticação Mútua (Iniciador, mútua)

[115] ATD Autenticação (Iniciador)

[116] AWG Espera (Respondedor)

[117] AR1 Autenticação (Respondedor, sentido único)

[118] AR2 Autenticação mútua (Respondedor, mútua)

[119] ARD Autenticado (Respondedor)

[120] Mensagens:

[121] ARQ Solicitação de Autenticação

[122] ARP Resposta de Autenticação

[123] ACF1 Confirmação de Autenticação (sentido único)

[124] ACF2 Confirmação de Autenticação Mútua

[125] ARP1 Resposta de Autenticação (sentido único)

[126] ARP2 Resposta de Autenticação Mútua

[127] Eventos/Ações/Estado:

[128] OOB Fora da Banda (ação de comunicação)

[129] OOB_I Fora da Banda (ação de comunicação pelo iniciador)

[130] OOB_R Fora da banda (ação de comunicação pelo respondedor)

[131] BA Má Autenticação (evento)

[132] BTG Bootstrapping (evento)

[133] NP Sem parceiro (evento)

[134] TO Período de interrupção (evento)

[135] TR Acionador (evento)

[136] MPS Estado de Andamento Mútuo

[137] MAS Estado de Espera Mútuo

[138] MCS Estado de Confirmação Mútua

[139] Chaves:

[140] BI Chave pública de carga inicial do Iniciador

[141] BR Chave pública de carga inicial do Respondedor

[142] PI Chave Pública do Iniciador

[143] PR Chave pública do Respondedor

[144] bI Chave privada do Iniciador correspondente a BI

[145] bR Chave privada do Respondedor correspondente a BR

[146] A Figura 1 mostra dispositivos para comunicação sem fio e autenticação. Um sistema 100 para comunicação sem fio compreende um dispositivo iniciador 110 e um dispositivo respondedor 120, sendo que os dispositivos estão fisicamente separados. O dispositivo iniciador tem um transceptor do iniciador 111 disposto para comunicação sem fio de acordo com o protocolo de comunicação e um processador do iniciador 112 disposto de modo a processar o protocolo de comunicação. De modo semelhante, o dispositivo respondedor tem um transceptor do respondedor 121 disposto para comunicação sem fio de acordo com o protocolo de comunicação e um processador do respondedor 122 disposto de modo a processar o protocolo de comunicação. Os dispositivos são equipados para comunicação sem fio, conforme indicado esquematicamente pelo formato 130 e pelas setas que conectam os transceptores 111 e 121. O dispositivo iniciador pode ter uma interface de usuário 113, que pode incluir elementos bem conhecidos como um ou mais botões 115, um teclado, um monitor, uma tela sensível ao toque etc. O dispositivo respondedor pode também ter uma interface de usuário 123. A interface de usuário do respondedor pode ser disposta para acomodar a interação com o usuário para executar uma ação fora da banda do respondedor para adquirir uma chave pública do iniciador proveniente do dispositivo iniciador.

[147] Os dispositivos são dispostos para comunicação sem fio de acordo com um protocolo de comunicação entre o dispositivo iniciador e o dispositivo respondedor. Os dispositivos são dispostos para executar um protocolo de autenticação para acomodar uma autenticação sendo uma dentre a autenticação unilateral do dispositivo respondedor pelo

dispositivo iniciador e a autenticação mútua do dispositivo respondedor pelo dispositivo iniciador e do dispositivo iniciador pelo dispositivo respondedor, sendo que um exemplo detalhado é dado abaixo com referência à Figura 2. O protocolo de comunicação pode incluir o protocolo de autenticação. Nos exemplos, o protocolo de comunicação é Wi-Fi de acordo com o padrão IEEE 802.11 [ref 1], mas outros protocolos sem fio também podem ser usados, como Bluetooth, quando dotados de um protocolo de autenticação adequado com base no sistema como elucidado abaixo.

[148] O processador do iniciador 112 tem uma unidade de mensagem do iniciador 116 para compor mensagens a serem enviadas para o dispositivo respondedor e para decompor mensagens recebidas a partir do dispositivo respondedor de acordo com o protocolo de autenticação. O processador do iniciador também tem uma máquina de estado do iniciador 117 para fornecer estados do iniciador de acordo com o protocolo de autenticação dependentes da interação com o usuário e das mensagens recebidas a partir do dispositivo respondedor, sendo que um exemplo é detalhado abaixo com referência à Figura 3.

[149] O processador do respondedor 122 tem uma unidade de mensagem do respondedor 126 para compor mensagens a serem enviadas para o dispositivo iniciador e para decompor mensagens recebidas a partir do dispositivo iniciador de acordo com o protocolo de autenticação. O processador do respondedor também tem uma máquina de estado do respondedor 127 para fornecer estados do respondedor de acordo com o protocolo de autenticação dependentes da interação com o usuário e das mensagens recebidas a partir do dispositivo iniciador.

[150] A função do processador do iniciador e do processador do respondedor de acomodar o protocolo de autenticação com base nas respectivas mensagens e nos respectivos estados do iniciador e do respondedor, com o uso das respectivas unidades de mensagem e máquinas de estado, é explicada a seguir com referência às Figuras 2, 3 e 4.

[151] Para a autenticação, o sistema proposto pode usar qualquer forma de criptografia de chave pública, tal como RSA, consultar [7], ou Criptografia de Curva Elíptica (ECC), consultar [8].

[152] A Figura 2 mostra um diagrama esquemático de um protocolo de autenticação. De acordo com o protocolo de autenticação 200, um primeiro dispositivo INIT_DEV troca mensagens com um segundo dispositivo RESP_DEV conforme indicado pelas setas entre duas linhas de tempo verticais que representam o avanço do tempo na direção descendente. O primeiro dispositivo pode ser o dispositivo iniciador começando em IST e o segundo dispositivo pode ser o dispositivo respondedor começando em AWG, mas essas funções podem ser invertidas. As mensagens são compostas pela unidade de mensagem no lado de envio, e decompostas pela unidade de mensagem no lado de recepção.

[153] Nesta descrição, B_I indica uma chave pública de carga inicial do iniciador, enquanto b_I indica a chave privada correspondente. De modo similar, B_R indica uma chave pública de carga inicial do respondedor, enquanto b_R indica a chave privada correspondente. H indica uma função hash (função de dispersão criptográfica), por exemplo, com base em um algoritmo hash de sentido único adequado conhecido

como tal. Exemplos adequados de funções hash podem ser encontrados na ref [4].

[154] O valor de uma função hash da chave pública do iniciador é indicado por $H(B_I)$. Um valor hash pode ser facilmente verificado para corresponder a um valor hash protegido, mas manipular tal valor mantendo, ao mesmo tempo, o mesmo hash é virtualmente impossível. Os dados de autenticação são calculados com base em uma ou mais chaves, sendo que as respectivas chaves públicas e privadas, por exemplo, indicadas por $\{auth1\}_{k1}$, o que significa o valor de auth1 criptografado pela chave k1, enquanto {auth1} significa o valor de auth1. Essas chaves são geradas, usadas para codificar e decodificar, produzindo assinaturas ou valores de controle, e verificar tais valores, como é bem conhecido como tal, por exemplo, a partir do sistema de criptografia Diffie Hellman mencionado anteriormente.

[155] Inicialmente, o dispositivo iniciador pode realizar a carga inicial mediante a aquisição de uma chave pública do respondedor a partir do dispositivo respondedor através de uma ação fora da banda do iniciador. A ação OOB é mostrada pela ação OOB marcada pela seta tracejada (indicada de modo correspondente na Figura 1 pela seta 140). Vários exemplos de ações de OOB são descritos em ref [2]; capítulo 10. Outros exemplos são: o usuário ler um código no dispositivo iniciador e inserir o mesmo no dispositivo respondedor, o usuário tirar uma foto com a câmera do dispositivo iniciador de um código legível por máquina como um código de barras ou código QR que um é impresso sobre ou exibido pelo dispositivo respondedor.

[156] Subsequentemente, a unidade de mensagem do iniciador pode compor um pedido de autenticação ARQ a ser enviado em um estado de carga inicial. O pedido de autenticação pode conter um verificador iniciador $H(B_I)$ para verificar uma chave pública do iniciador e um verificador do respondedor $H(B_R)$ para verificar a chave pública do respondedor. O ARQ pode conter, ainda, uma chave pública do iniciador P_I, e dados do iniciador adicionais como um número aleatório do iniciador *I-nonce*, e recursos de capacidade do iniciador *I-cababilities*, que podem ser codificados com o uso de uma primeira chave K_1 indicada por $\{\text{I-nonce} \mid \text{I-capabilities}\}_{K1}$. A primeira chave K_1 pode ser derivada pelo Iniciador pelo método Diffie-Hellman a partir da chave pública do respondedor B_R e da chave privada do iniciador p_I correspondente à chave pública do iniciador P_I. A primeira chave K_1 pode ser derivada pelo Respondedor pelo método Diffie-Hellman a partir da chave pública do iniciador P_I e da chave privada do respondedor b_R correspondente à chave pública do respondedor B_R. De modo correspondente, a unidade de mensagem do respondedor é disposta de modo a decompor o pedido de autenticação ARQ.

[157] Depois de um período de interrupção TO, quando nenhuma resposta for recebida, o ARQ pode ser transmitido novamente, por exemplo, até 3 vezes. Presume-se que uma resposta ARP1 é recebida em tempo.

[158] A unidade de mensagem do respondedor é disposta de modo a compor a resposta de autenticação ARP1, que pode conter dados de autenticação do respondedor unilateral $\{\text{R-auth1}\}_{k1}$. O ARP1 pode conter adicionalmente uma chave pública do respondedor P_R, e adicionalmente dados do respondedor como um número aleatório *R-nonce*. A primeira chave

intermediária de k_1 pode ser baseada em uma chave pública do iniciador P_I, em uma chave privada do respondedor (p_R) correspondente à chave pública do respondedor (p_R) (se p_R estava presente em ARP1) e em uma chave privada do respondedor (b_R) correspondente à chave pública do respondedor (B_R). A primeira chave intermediária é adequada para autenticação unilateral do dispositivo respondedor. O valor R-auth1 pode ser a (um hash de) concatenação de qualquer seleção de valores usados no protocolo de autenticação, como o número aleatório *I-nonce*, um número aleatório do respondedor *R-nonce* e/ou as chaves públicas usadas como P_R, B_R e P_I. Devido à aleatoriedade dos *nonces*, o valor R-auth1 é diferente cada vez que o protocolo é executado, protegendo, assim, contra um ataque de repetição. No caso de autenticação mútua, o ARP1 também pode incluir um estado de andamento mútuo indicativo de que a autenticação mútua está em andamento, para possibilitar que o dispositivo respondedor adquira a chave pública do iniciador proveniente do dispositivo iniciador através de uma ação fora da banda do respondedor. De modo correspondente, a unidade de mensagem do iniciador é disposta de modo a decompor a resposta de autenticação ARP1.

[159] Opcionalmente, a unidade de mensagem do iniciador é disposta de modo a compor, mediante o recebimento do estado de andamento mútuo no estado de autenticação, uma confirmação de espera de autenticação ACF1 contendo um estado mútuo de espera. O ACF1 pode conter dados de autenticação unilateral do iniciador $\{I\text{-auth1}\}_{k1}$ com base na chave pública do respondedor (B_R) e uma chave p do iniciador (p_I) correspondente à chave pública do iniciador P_I. O valor de {I-auth1} é calculado de maneira similar a {R-auth1} com o uso

das mesmas entradas. Entretanto, o valor de {I-auth1} precisará ser diferente do valor de {R-auth1}, para se defender contra um ataque de repetição. Portanto, a ordem das entradas ao computar o hash precisa ser escolhida diferentemente e/ou um valor constante precisa ser incluído no hash diferente do que na computação do hash para {R-auth1}. De modo correspondente, a unidade de mensagem do respondedor pode ser disposta para decompor a confirmação de espera de autenticação ACF1.

[160] Posteriormente, o dispositivo respondedor pode executar ou já executou a aquisição de uma chave pública do iniciador a partir do dispositivo iniciador através de um dispositivo respondedor em ação fora da banda. A ação OOB é mostrada pela ação OOB marcada pela seta tracejada (indicada de modo correspondente na Figura 1 pela seta 140). Após completar a dita aquisição, a máquina de estado do respondedor prossegue conforme elucidado abaixo para enviar uma resposta de autenticação mútua ARP2.

[161] A unidade de mensagem do respondedor é disposta de modo a compor a resposta de autenticação mútua ARP2 que compreende os dados de autenticação mútua do respondedor $\{R\text{-auth2}\}_{k2}$. O ARP2 pode conter, ainda, uma chave pública do respondedor P_R, e dados adicionais do respondedor como um número aleatório *R-nonce*. A segunda chave intermediária de k_2 pode ser baseada na chave pública do iniciador (B_I) e em uma chave privada do respondedor (b_R) correspondente à chave pública do respondedor (B_R). A segunda chave intermediária é adequada para autenticação mútua do dispositivo respondedor e do dispositivo iniciador. A segunda chave intermediária pode ser determinada com o uso de {b_R, p_R, B_I e P_I} no respondedor ou {p_I, b_I, B_R e P_R} no iniciador. O valor de R-auth2 pode ser

um hash da concatenação de valores usados no protocolo de autenticação, como o número aleatório do iniciador *I-nonce*, um número aleatório do respondedor *R-nonce* e as chaves públicas usadas como B_I, B_R, P_R e P_I. Devido à aleatoriedade dos *nonces*, o valor de {R-auth2} é diferente cada vez que o protocolo é executado, protegendo, assim, contra um ataque de repetição. De modo correspondente, a unidade de mensagem do iniciador é disposta de modo a decompor a resposta de autenticação ARP2. Processar corretamente significa que o processador iniciador chega ao mesmo valor para k_2 que o Respondedor, e que o Iniciador encontra o mesmo valor para {R-auth2} ao computar o próprio R-auth2 e por descriptografia com a chave k_2 do valor $\{R\text{ -auth2}\}_{k2}$ recebido na mensagem ARP2.

[162] A unidade de mensagem do iniciador está disposta de modo a compor uma confirmação de autenticação mútua ACF2 que compreende um estado de confirmação mútua indicativo da confirmação da autenticação mútua e dados de autenticação do iniciador mútuo $\{I\text{-auth2}\}_{k2}$ com base na chave pública do respondedor (B_R) e em uma chave privada do iniciador (b_I) correspondente à chave pública do iniciador (B_I). A segunda chave intermediária k_2 pode ser determinada com o uso de {p_I, b_I, B_R e P_R} no iniciador. O valor de {I-auth2} é calculado de maneira similar a {R-auth2} com o uso das mesmas entradas. No entanto, o valor de {I-auth2} deve ser diferente do valor de {R-auth2}, para se defender contra um ataque de repetição. Portanto, a ordem das entradas ao computar o hash precisa ser escolhida diferentemente e/ou um valor constante precisa ser incluído no hash diferente do que na computação do hash para {R-auth2}. De modo correspondente, a unidade de mensagem do respondedor é disposta de modo a decompor a confirmação de

autenticação mútua ACF2. Se o Respondedor chegar na mesma chave intermediária k2 e obtiver o mesmo valor para os dados I-auth2, computando-se o próprio I-auth2 e por descriptografia do $\{I\text{-}auth2\}_{k2}$ recebido com a chave k2, então, o Respondedor realmente autenticou o BI e o processamento dos dados de autenticação mútua do iniciador $\{I\text{-}auth2\}_{k2}$ foi bem-sucedido.

[163] A Figura 3 mostra um exemplo de uma máquina de estado do iniciador. A máquina de estado do iniciador 300 fornece estados do iniciador de acordo com o protocolo de autenticação dependentes da interação com o usuário e das mensagens recebidas a partir do dispositivo respondedor. Os estados do iniciador podem incluir

[164] - um estado inicial IST para carga inicial mediante a aquisição de uma chave pública a partir do dispositivo respondedor através de uma ação fora da banda do iniciador;

[165] - um estado de carga inicial BST indicativo de que a carga inicial foi executada corretamente mediante a aquisição da chave pública do respondedor;

[166] - um estado de autenticação AG1 para executar a autenticação;

[167] - um estado de autenticação mútua AG2 para executar a autenticação mútua;

[168] - um estado autenticado ATD indicativo de que a autenticação foi executada corretamente.

[169] Inicialmente, a máquina de estado inicia no estado inicial IST. As setas indicam transições de estado, e são marcadas por um acrônimo indicando a mensagem ou evento que corresponde à transição de estado. A máquina de estado do iniciador é disposta de modo a ativar o estado de carga inicial

BST mediante a execução correta da carga inicial BTG mediante a aquisição da chave pública do respondedor.

[170] A máquina do estado do iniciador pode ser disposta de modo a ativar subsequentemente o estado de autenticação AG1 mediante o envio do ARQ, e/ou através de um evento acionador TR pelo usuário ou um outro evento, ou imediatamente após a dita carga inicial bem-sucedida. Após um período de interrupção TO, o estado pode ser acionado novamente depois de retransmitir o ARQ, enquanto conta o número de tentativas e, depois que exceder um número predeterminado de tentativas, retornar ao estado de carga inicial BST, ou ao estado inicial IST. Os estados BST e AG1 podem também ser combinados.

[171] A máquina de estado do iniciador é disposta de modo a ativar o estado de autenticação mútua AG2 mediante o recebimento do estado de andamento mútuo em ARP1, para esperar a autenticação mútua. Opcionalmente, a confirmação da espera de autenticação ACF1 pode ser enviada contendo o estado de espera mútua.

[172] A máquina de estado do iniciador está disposta de modo a ativar o estado autenticado ATD mediante o recebimento da resposta de autenticação mútua ARP2 e o processador do iniciador processar corretamente os dados de autenticação mútua do respondedor $\{R\text{-}auth2\}_{k2}$ com base na chave pública do respondedor e em uma chave privada do iniciador (b_I) correspondente à chave pública do iniciador (B_I). Então, pode também ser enviada a confirmação da espera de autenticação ACF2 contendo o estado de espera mútua.

[173] Opcionalmente, a máquina de estado do iniciador está disposta de modo a ativar o estado autenticado

mediante o recebimento da resposta de autenticação mútua ACF2 no estado de autenticação AG1 e o processador do iniciador processar corretamente os dados de autenticação mútua do respondedor $\{R\text{-}auth2\}_{k2}$. Então, pode também ser enviada a confirmação da espera de autenticação ACF2 contendo o estado de espera mútua. Então, efetivamente, o estado de autenticação mútua é ignorado.

[174] Opcionalmente, a unidade de mensagem do iniciador está disposta de modo a decompor, no caso da autenticação unilateral, uma resposta de autenticação unilateral (ARP1) que compreende dados de autenticação unilateral do respondedor $\{R\text{-}auth1\}_{k1}$ com base em uma chave privada do respondedor b_R correspondente à chave pública do respondedor B_R e um estado unilateral indicativo da autenticação unilateral. Além disso, a máquina de estado do iniciador está disposta de modo a ativar o estado autenticado quando o processador do iniciador processar corretamente os dados de autenticação mútua do respondedor $\{R\text{-}auth1\}_{k1}$ com base na chave pública do respondedor e em uma chave privada do iniciador b_I correspondente à chave pública do iniciador B_I. Processar corretamente significa que o processador do iniciador chega ao mesmo valor para k_1 que o respondedor, e que o iniciador encontra o mesmo valor para $\{R\text{-}auth1\}$ computando-se o próprio R-auth1 e por descriptografia com a chave k_1 do valor $\{R\text{ -}auth1\}_{k1}$ recebido na mensagem ARP1.

[175] Opcionalmente, a máquina de estado do iniciador está disposta de modo a ativar o estado de carga inicial ou o estado inicial mediante o recebimento da resposta de autenticação ARP1 e o processador do iniciador processar incorretamente os dados de autenticação unilateral do

respondedor $\{R\text{-}auth1\}_{k1}$. O processamento incorreto pode ser devido a uma chamada má autenticação BA ou quando nenhum dispositivo par for encontrado NP. Nesses casos, a máquina de estado do iniciador pode estar disposta para retornar ao estado de carga inicial BST ou ao estado inicial IST, que pode depender adicionalmente do evento conforme detectado.

[176] Opcionalmente, a máquina de estado do iniciador está disposta de modo a ativar o estado de carga inicial ou o estado inicial mediante o recebimento da resposta de autenticação mútua ARP2 e o processador do iniciador processar incorretamente os dados de autenticação mútua do respondedor $\{R\text{-}auth2\}_{k2}$. O processamento incorreto pode ser devido a uma chamada má autenticação BA ou quando nenhum dispositivo par for encontrado NP. Nesses casos, a máquina de estado do iniciador pode estar disposta para retornar ao estado de carga inicial BST ou ao estado inicial IST (não mostrado), que pode depender adicionalmente do evento conforme detectado.

[177] A Figura 4 mostra um exemplo de uma máquina de estado do respondedor. A máquina de estado do respondedor 400 fornece estados do respondedor de acordo com o protocolo de autenticação dependentes da interação com o usuário e das mensagens recebidas a partir do dispositivo iniciador. Os estados do respondedor podem compreender

[178] - um estado de espera (AWG) para receber mensagens a partir do iniciador;

[179] - um estado de autenticação do respondedor (AR1) para executar a autenticação;

[180] - um estado de autenticação mútua do respondedor (AR2) para possibilitar que o dispositivo respondedor adquira uma chave pública do iniciador a partir do

dispositivo iniciador através de uma ação fora da banda do respondedor;

[181] - um estado autenticado do respondedor (ARD) indicando que a autenticação foi realizada corretamente.

[182] Inicialmente, a máquina de estado do respondedor inicia no estado de espera AWG. O estado pode ser ativado mediante a interação com um usuário, ou qualquer outro evento como ligar o dispositivo respondedor. As setas indicam transições de estado e são marcadas por um acrônimo indicando a mensagem ou evento que corresponde à transição de estado.

[183] A máquina de estado do respondedor pode ser disposta de modo a ativar o estado de autenticação do respondedor AR1 ao receber e processar corretamente o pedido de autenticação ARQ. Os estados AWG e AR1 podem também ser combinados em um único estado.

[184] Processar incorretamente o ARQ pode significar que o respondedor determinou que o verificador do respondedor $H(B_R)$ no ARQ recebido não é o hash de sua chave pública B_R ou que descriptografar o $\{\text{I-nonce} \mid \text{I capabilities}\}_{K1}$ no ARQ recebido leva a um erro. Um exemplo de um algoritmo de criptografia/ descriptografia que é capaz de detectar, durante a descriptografia, que uma chave errada é usada para descriptografar ou que os dados criptografados foram alterados após a criptografia é AES-SIV, consultar [3]. Após o processamento correto de ARQ, a resposta de autenticação ARP1 contendo o estado de andamento mútuo indicativo de que a autenticação mútua está em andamento é transmitida ao iniciador.

[185] A máquina de estado do respondedor fornece e ativa um estado de autenticação mútua do respondedor AR2

quando o dispositivo respondedor adquire uma chave pública do iniciador a partir do dispositivo iniciador através de uma ação fora da banda do respondedor. Após a dita aquisição, também a resposta de autenticação mútua ARP2 é enviada para o iniciador.

[186] Opcionalmente, a máquina de estado do respondedor está disposta de modo a receber e processar a confirmação de espera de autenticação mútua ACF1 que compreende um estado de espera mútuo.

[187] A máquina de estado do respondedor é, então, disposta de modo a ativar somente o estado de autenticação mútua AR2 mediante o recebimento do estado de espera mútuo e a dita ação OOB do respondedor. Se ACF1 não for recebido dentro de um período de interrupção TO predeterminado, o estado permanece o estado de autenticação do respondedor AR1, e o ARP1 pode ser transmitido novamente até um número predeterminado de novas tentativas.

[188] A máquina de estado do respondedor está disposta de modo a ativar o estado autenticado do respondedor ARD mediante o recebimento da confirmação de autenticação mútua ACF2 e após o processador do respondedor processar corretamente os dados de autenticação mútua do iniciador $\{I\text{-}auth2\}_{k2}$ com base na chave pública do iniciador B_I e na chave privada do respondedor b_R.

[189] Opcionalmente, a máquina de estado do respondedor está disposta de modo a ativar o estado autenticado do respondedor ARD mediante o recebimento da confirmação de autenticação mútua ACF2 no estado de autenticação do respondedor AR1 e após o processador do respondedor processar corretamente os dados de autenticação mútua do iniciador {I-

auth2}$_{k2}$. A recepção de ACF2 pode ocorrer após o respondedor, mediante o recebimento do ARQ, enviar a resposta de autenticação mútua ARP2 diretamente ao iniciador, por exemplo, com base no respondedor já possuir a chave pública do iniciador a partir de uma sessão anterior.

[190] Opcionalmente, a unidade de mensagem está disposta de modo a compor, no caso da autenticação unilateral, uma resposta de autenticação unilateral ARP1 que compreende dados de autenticação unilateral do respondedor {R-auth1}$_{k1}$ com base em uma chave privada do respondedor b_R correspondente à chave pública do respondedor B_R e um estado unilateral indicativo da autenticação unilateral estar completa. Além disso, a máquina de estado do respondedor está disposta de modo a, no caso de autenticação unilateral, ativar o estado autenticado do respondedor mediante o recebimento de uma confirmação de autenticação unilateral ACF1 e o processador do respondedor processar corretamente os dados de autenticação unilateral do iniciador {I-auth1}$_{k1}$. Processar corretamente significa que o processador do respondedor chega ao mesmo valor para k_1 que o iniciador, e que o respondedor encontra o mesmo valor para I-auth1 computando-se o próprio I-auth1 e por descriptografia com a chave k_1 do valor {I -auth1}$_{k1}$ recebido na mensagem ACF1.

[191] Opcionalmente, a máquina de estado do respondedor está disposta de modo a ativar o estado de espera mediante o recebimento da confirmação de autenticação mútua ACF2 e após o processador do respondedor processar incorretamente os dados de autenticação mútua do iniciador {I-auth2}$_{k2}$, resultando em um evento de autenticação incorreta BA.

[192] Opcionalmente, a unidade de mensagem do respondedor está disposta adicionalmente de modo a decompor a confirmação de espera de autenticação ACF1 que compreende dados de autenticação unilateral do iniciador $\{I\text{-}auth1\}_{k1}$ e compreendendo um estado de espera mútua. E a máquina de estado do respondedor está disposta de modo a ativar o estado de espera após o processador do respondedor processar incorretamente os dados de autenticação unilateral do iniciador, resultando em um evento de autenticação incorreta BA.

[193] Em geral, a autenticação mútua pode ser acomodada em um protocolo de autenticação que também especifica uma autenticação de sentido único. Na autenticação de sentido único, o (usuário do) respondedor não quer ter certeza de qual dispositivo recebeu o Pedido de Autenticação. O respondedor não adquire uma chave pública B_I do Iniciador fora da banda e, consequentemente, não pode e não envia um hash de B_I na mensagem de resposta de Autenticação ao iniciador. Somente a autenticação unilateral é feita quando o respondedor prova a posse ao iniciador da chave privada b_R que corresponde à chave pública B_R que o Iniciador capturou fora da banda. Por exemplo, com o uso de b_R no modo de Diffie-Hellman, consultar ref [6], para criar uma chave para criptografar uma mensagem ao iniciador. Tal protocolo pode usar dois ou mais pares de chaves para cada parte, por exemplo, um par de chaves para inicializar a confiança entre si e um outro par de chaves a partir do qual uma chave pública é autenticada para operações adicionais.

[194] Quando um usuário executa uma ação que aciona a execução de um protocolo com pedidos e respostas através de Wi-Fi e trocas adicionais de mensagens, o usuário

não gosta de estar esperando muito antes que esta ação com todas as suas trocas seja concluída. Entretanto, cada uma das mensagens pode deixar de ser recebida pela outra parte por várias razões, por exemplo, se uma mensagem for corrompida pela interferência de RF. Então, quando um dispositivo envia um pedido por Wi-Fi, ele ajusta um temporizador para esperar a resposta. Se a resposta não chegar dentro de um tempo de interrupção, ele pode tentar enviar o pedido novamente. Se não foi recebida nenhuma resposta após um número de tentativas, o dispositivo desiste e relata isso ao usuário. As chances de sucesso são aumentadas quando o tempo de espera é mais longo e o número de tentativas possíveis é maior, mas o usuário também tem de esperar mais tempo antes de obter a confirmação de que o protocolo não teve êxito.

[195] Um problema com a autenticação mútua tradicional é que pode demorar mais tempo para o respondedor responder com uma mensagem de Resposta de Autenticação para autenticação mútua do que no caso de autenticação de sentido único, porque o usuário do dispositivo respondedor tem que capturar a chave pública BI primeiro. Além disso, o dispositivo iniciador não sabe se o dispositivo respondedor quer fazer a autenticação mútua ou não. Portanto, ele deve definir o seu tempo de espera e o número de tentativas para acomodar a isto. Isto significa que, no caso de existir um problema com o Wi-Fi, por exemplo, muito ruído ou alguma outra razão para transferências defeituosas entre o iniciador e o respondedor via Wi-Fi, o dispositivo iniciador precisa esperar muito tempo antes de desistir e relatar isso ao seu usuário.

[196] O sistema proposto é eficaz quando é necessária uma interação com o usuário para capturar a chave

pública OOB B_I do iniciador. Exemplos de tal ação OOB do respondedor são:

a. quando B_I é exibida como um código legível por máquina (por exemplo, Código QR ou código de barras) e o usuário tem que usar um leitor de código legível por máquina (como uma câmera ou um scanner a laser) para ler B_I;
b. quando B_I é exibida em formato legível por seres humanos e o usuário tem que inserir um código no dispositivo Respondedor com o uso de algum dispositivo de entrada (teclado, chaves, tela sensível ao toque com teclado virtual, mouse e teclado exibido na tela etc.);
c. quando B_I é transferida mediante o uso de uma etiqueta NFC, consultar ref [5], que o usuário tem que colocar o dispositivo respondedor em contato com um leitor NFC, onde a etiqueta NFC com B_I não pode ser usada para transferir B_R ao dispositivo Iniciador, simultaneamente com a transferência de B_I para o dispositivo respondedor.

[197] Para resolver os problemas acima descritos, no caso de o respondedor querer executar uma autenticação mútua, ele primeiro cria uma primeira Resposta de Autenticação como se ele quisesse executar uma autenticação de sentido único. O respondedor executa todas as ações criptográficas e outras como se quisesse executar uma autenticação de sentido único. No entanto, ele indica em sua resposta que quer realizar uma autenticação mútua mais tarde. Essa indicação pode ser um estado especial, por exemplo, em

vez de "STATUS OK", pode enviar um estado "AUTENTICAÇÃO MÚTUA EM ANDAMENTO" na resposta de autenticação.

[198] Ao receber tal ARP, o dispositivo iniciador obterá uma resposta rápida a seu Pedido de Autenticação quando não houver problemas com o Wi-Fi. O dispositivo Iniciador pode executar verificações de autenticação de sentido único para o dispositivo respondedor, para criar confiança no dispositivo respondedor. Ao se realizar as verificações de autenticação de sentido único, por exemplo, ao se executar uma verificação de integridade no estado retornado com o uso de uma chave de Diffie-Hellman, também se evita que os invasores alterem o código de estado "AUTENTICAÇÃO MÚTUA EM ANDAMENTO" ou outras partes da mensagem de resposta de Autenticação.

[199] O dispositivo Iniciador pode, depois de não ter encontrado nenhum problema com todas as verificações criptográficas na resposta de Autenticação recebida, responder com uma mensagem de Confirmação de Autenticação com um resultado de estado especial "AGUARDANDO RESPOSTA DE AUTENTICAÇÃO MÚTUA".

[200] O (usuário do) dispositivo Respondedor pode então capturar a chave pública B_I a tempo e, quando feito, responder com uma resposta de autenticação mútua contendo o hash da chave pública B_I do Iniciador e um estado adicional "STATUS OK".

[201] Agora, um protocolo de autenticação será descrito com detalhes a seguir. O protocolo possibilita que as chaves públicas sejam usadas fora da banda (OOB), que são exibidas ou transferidas na íntegra, mas não são usadas como tal por meio de Wi-Fi. Em vez disso, por Wi-Fi, os valores

hash das chaves OOB públicas são usados, de modo que essas chaves públicas permaneçam desconhecidas para outras pessoas que estão ouvindo as mensagens Wi-Fi trocadas. Isso é útil, caso as chaves OOB sejam estáticas. As chaves OOB estáticas podem ser usadas por dispositivos que não possuem um meio de saída de dados OOB, como um visor para um código QR. Quando o protocolo requer que o Respondente receba uma chave pública em banda, por meio de Wi-Fi, o Iniciador pode enviar uma chave pública PI adicional e diferente por Wi-Fi.

[202] Para a transferência de chaves públicas, são possíveis modalidades alternativas. Em vez de usar o hash de uma chave pública via Wi-Fi, outras formas de ofuscar um valor podem ser usadas, como exibir/enviar apenas um número limitado de bits da chave pública. Além disso, em vez do valor total, um hash das chaves públicas pode ser exibido/transferido fora da banda - OOB. A vantagem é que o número de bits a exibir ou transferir OOB pode ser menor, portanto, os códigos QR menores ou as etiquetas NFC menores, consultar ref [5], podem ser usados. Nesse caso, o valor total das chaves públicas deve ser enviado dentro da banda, ou seja, através de Wi-Fi. Nesse caso, P_I e B_I podem ser a mesma. As chaves públicas podem ser exibidas/transferidas totalmente com o uso de OOB e por Wi-Fi.

[203] No exemplo de protocolo descrito agora, as chaves públicas OOB são exibidas como um código QR e capturadas por uma câmera, mas outras formas de realização para o canal OOB também são possíveis, veja os exemplos acima.

[204] Em uma primeira fase, o utilizador do dispositivo iniciador pretende estabelecer uma ligação segura entre o dispositivo iniciador e um dispositivo respondedor específico. O usuário inicia o protocolo de autenticação no

dispositivo iniciador. O dispositivo iniciador usa pares de chaves públicas B_I/b_I e P_I/p_I ou gera novos pares de chaves B_I/b_I e P_I/p_I.

[205] Em certas modalidades, o dispositivo respondedor pode ser ativamente configurado em um modo respondedor. Em outras modalidades, o dispositivo respondedor é colocado no modo Respondedor quando ele é ligado pela primeira vez ou após a restauração dos padrões de fábrica. A configuração de R para o modo Respondedor pode ativar a geração de um novo par de chaves públicas B_R/b_R. O dispositivo respondedor tem que estar em modo Respondedor para participar do protocolo. No modo Respondedor, o dispositivo respondedor pode exibir uma chave pública B_R para uso como a chave pública ou uma das chaves públicas no Diffie-Hellman. B_R pode ser estática e estar impressa no dispositivo respondedor ou em seu manual. A chave privada correspondente a B_R é b_R. O par B_R/b_R pode ser gerado de novo para cada nova execução do método Diffie-Hellman ou para cada intervalo de tempo de x minutos. A tela de B_R pode ser em formato legível por humanos ou em formato legível por máquina (código QR, código de barras) ou ambos. Supõe-se que um código legível por computador aqui possa ser lido com uma câmera.

[206] Em uma segunda fase, o utilizador do dispositivo iniciador inicia o protocolo de autenticação e aponta a câmara do dispositivo iniciador para a chave pública B_R legível por máquina do dispositivo respondedor e faz com que o dispositivo iniciador a capture. Essas ações do usuário podem levar algum tempo, é claro.

[207] Em um terceiro estágio, o dispositivo iniciador envia uma Solicitação de Autenticação ao dispositivo

respondedor via Wi-Fi, dirigindo-se ao dispositivo respondedor diretamente se o dispositivo iniciador souber o endereço MAC ou transmitindo-o via Wi-Fi. O Pedido de Autenticação contém o hash da chave pública B_I do dispositivo iniciador e um hash da chave pública B_R do dispositivo respondedor, a chave pública P_I do Iniciador a ser usada na derivação de uma chave de Diffie-Hellman pelo Respondedor e outras informações do Iniciador, por exemplo, um *nonce* do Iniciador, criptografado com uma chave k1 que é derivada com o uso do método Diffie-Hellman que usa B_R e p_I. A criptografia pode ser feita com uma cifra simétrica. Entretanto, quando uma cifra é usada a qual também tem o recurso de verificação da integridade de sua carga útil criptografada e também verificação da integridade de outras partes não criptografadas de sua carga útil, por exemplo, AES SIV (consultar a ref [3]), o dispositivo respondedor pode verificar, durante a descriptografia das "informações do outro Iniciador", se foi gerada a chave correta do Diffie-Hellman e se os valores não criptografados na mensagem, como um código de estado, não foram alterados por um invasor. Se o AES-SIV descriptografa sem erros, o dispositivo respondedor certamente sabe que o dispositivo iniciador usou a chave privada correspondente ao P_I, portanto, o dispositivo Iniciador comprovou a posse da chave privada correspondente ao P_I ao dispositivo Respondedor.

[208] Em uma fase seguinte, o respondedor vê uma mensagem por Wi-Fi com o hash de sua chave pública B_R, de modo que ele sabe que ela foi criada para ele. O respondedor também sabe que o remetente desta mensagem capturou a B_R de sua tela, especialmente quando a B_R foi gerada de novo imediatamente antes desta execução do protocolo de Autenticação. Entretanto,

o dispositivo respondedor não tem ideia de qual dispositivo o remetente é. Portanto, o (usuário do) dispositivo respondedor pode querer uma autenticação adicional, e ali capturar fora da banda a chave pública B_I do dispositivo Iniciador. O usuário do dispositivo respondedor pode configurar seu dispositivo para executar autenticação mútua. O respondedor agora fornece uma rápida retroinformação ao dispositivo Iniciador, desta forma o dispositivo Iniciador tem conhecimento de que o enlace para o Wi-Fi está funcionando, e que tudo está OK agora, com relação à criptografia. A mensagem do respondedor indica que uma resposta de autenticação mútua virá do dispositivo respondedor, mas que esta resposta pode levar algum tempo (desde segundos a dezenas de segundos). Então, o Respondedor imediatamente responde com uma mensagem de Resposta de Autenticação ao Iniciador com o estado "AUTENTICAÇÃO MÚTUA EM ANDAMENTO", enquanto dados adicionais na mensagem são gerados como em uma resposta de autenticação de sentido único. O último significa que, na construção desta mensagem, as "outras informações do Iniciador", por exemplo, o *Nonce* do Iniciador, da Solicitação de Autenticação, são descriptografadas pelo dispositivo Respondedor com o uso de P_I e b_R e usadas na construção da mensagem de Resposta de Autenticação, para que o Iniciador possa verificar se o respondedor realmente usou as "outras informações do Iniciador" corretas, por exemplo, o *Nonce* do Iniciador, e assim comprovou a posse da chave privada b_R que corresponde à chave pública B_R de OOB do Respondedor.

[209] Várias maneiras de usar as outras informações do Iniciador na construção da mensagem de resposta de Autenticação incluem as seguintes:

d. As "outras informações do Iniciador" podem ser deixadas transparentes na mensagem.

e. As "outras informações do Iniciador" podem ser deixadas transparentes na mensagem, ao mesmo tempo em que sua integridade é protegida por uma chave que é derivada com o uso de Diffie-Hellman, e com o uso de "outras informações do Iniciador" como AAD (*Authenticated Associated Data, or Authenticated Additional Data* - Dados Associados Autenticados ou Dados Adicionais Autenticados) com o AES-SIV.

f. As "outras informações do Iniciador" podem ser usadas para derivar uma outra chave, por exemplo, derivar primeiro uma chave com o uso de Diffie-Hellman e com o uso da chave de Diffie-Hellman e as "outras informações do Iniciador" como entrada para uma função de derivação de chave. Se a chave derivada assim for usada com AES SIV, ou se a chave derivada assim for usada para criptografar algo que é conhecido pelo Iniciador, o iniciador pode verificar se o responsável conhece as "outras informações do Iniciador" corretas.

[210] Opcionalmente, o campo de estado também pode ser usado como AAD para AES SIV, de modo que não possa ser violado sem que o dispositivo iniciador descubra.

[211] Em uma fase seguinte, o Iniciador recebe a mensagem de Resposta de Autenticação. Ele executa todas as verificações criptográficas e pode descobrir se o dispositivo descriptografou corretamente as "outras informações do Iniciador", e assim se o dispositivo respondedor possui a chave privada de b_R que corresponde à chave pública B_R OOB que o dispositivo Iniciador capturou com sua câmera do dispositivo respondedor. Se estas verificações falhar, o dispositivo Iniciador aborta o protocolo. Se as verificações forem feitas

corretamente, o dispositivo Iniciador inspeciona o campo de estado. Ele verá o estado "AUTENTICAÇÃO MÚTUA EM ANDAMENTO". O dispositivo Iniciador agora sabe que tem que esperar desde vários segundos até várias dezenas de segundos por uma segunda resposta do dispositivo Respondedor.

[212] Opcionalmente, o dispositivo Iniciador confirma a recepção correta da mensagem de Autenticação de Resposta com uma mensagem de Confirmação de Espera de Autenticação com um estado indicativo de que o Iniciador está esperando a Resposta de Autenticação mútua. A mensagem pode ser construída para autenticação de sentido único.

[213] Em um próximo estágio, o usuário do dispositivo respondedor aponta a câmera do dispositivo respondedor para a chave pública B_I exibida pelo dispositivo iniciador. Quando o hash da chave pública assim capturada do dispositivo iniciador corresponde ao hash da chave pública do dispositivo iniciador recebido via Wi-Fi na mensagem de Solicitação de Autenticação, o dispositivo respondedor pode ter certeza de que irá usar a chave pública correta para executar Diffie-Hellman com o dispositivo iniciador. O dispositivo respondedor saberá com certeza que está se comunicando com o dispositivo de onde ele capturou a B_I, quando, mais tarde no protocolo, o dispositivo iniciador prova a posse da chave privada correspondente b_I.

[214] Em uma fase seguinte, após ter capturado a chave pública B_I, o dispositivo respondedor responde ao dispositivo iniciador com uma mensagem de resposta de autenticação mútua, composta como uma resposta de autenticação mútua. A mensagem pode conter um estado "OK mútuo", ou simplesmente "OK", o hash do B_I e outras informações de

resposta criptografadas com chaves que são derivadas com o uso de chaves públicas P_I recebidas via Wi-Fi na mensagem de Solicitação de Autenticação e Bi obtidas fora da banda a partir do dispositivo iniciador. As "outras informações do Iniciador" enviadas pelo dispositivo Iniciador são descriptografadas pelo dispositivo respondedor, com o uso de sua chave privada b_R e a chave pública recebida P_I, e usadas na construção da mensagem de Resposta de Autenticação, conforme descrito anteriormente, de modo que o dispositivo respondedor possa provar posse da b_R ao dispositivo iniciador. Algumas diferenças com a resposta de Autenticação de sentido único são que o responsável usa também o B_I para derivar uma chave de Diffie-Hellman e a presença do hash da B_I na resposta.

[215] Existem diferentes maneiras nas quais o dispositivo Respondedor pode usar as duas chaves públicas B_I e P_I a partir do Iniciador. Por exemplo, o respondedor pode usar cada uma dessas duas chaves públicas juntamente com uma ou duas chaves privadas para obter duas chaves de Diffie-Hellman com k3 e k4.

[216] Em uma primeira modalidade, o respondedor pode, por exemplo, derivar k3 com o uso de P_I e sua chave privada de b_R ou uma nova chave privada de P_R ou a soma de b_R e p_R. No caso de usar p_R, ele deve incluir a chave pública P_R correspondente na resposta de Autenticação, de modo que o iniciador possa recuperá-la. Isso pode ser feito através do envio de P_R claramente ou criptografada com uma chave que o Iniciador é capaz de derivar, por exemplo, a chave k1 acima.

[217] Em uma segunda modalidade, o respondedor pode, por exemplo, derivar k4 com o uso de B_I e sua chave privada b_R ou uma nova chave privada p_R ou a soma de b_R e p_R.

No caso de usar p_R, ele deve incluir a chave pública P_R correspondente na resposta de Autenticação, de modo que o iniciador possa recuperá-la. Isso pode ser feito através do envio de P_R claramente ou criptografada com uma chave que o Iniciador é capaz de derivar, por exemplo, a chave k1 acima. No caso de a soma das duas chaves privadas ser usada para k3 ou k4, a derivação das outras chaves não precisa usar a soma de p_R e b_R, mas apenas uma dessas chaves. Desta forma, o dispositivo respondedor é capaz de provar a posse das chaves privadas em vez de apenas a soma das chaves privadas b_R e p_R.

[218] Em uma outra modalidade, o respondedor pode usar ambas as chaves k3 e k4, para cada criptografia um valor diferente que o Iniciador sabe, por exemplo, o *nonce* do Iniciador, de modo que o Iniciador possa verificar se o dispositivo respondedor conhece as chaves privadas que o respondedor usou. Além disso, o respondedor criptografa suas próprias "outras informações do Respondedor", por exemplo, um *nonce* do Respondedor, para ser capaz de verificar a mensagem de Confirmação de Autenticação.

[219] Em uma outra modalidade, em vez de usar as chaves k3 e k4 para criptografar valores diferentes, uma delas, a "primeira", pode ser usada para criptografar um primeiro valor enquanto a outra chave, a "segunda chave" é usada para criptografar a concatenação de um outro valor e do primeiro valor criptografado. A segunda chave precisa ser tal que o Respondedor possa gerar essa chave. Os valores criptografados com a segunda chave podem conter informações necessárias para gerar a primeira chave, e assim ajudar a construir a confiança.

[220] Em uma fase seguinte, o Iniciador recebe a mensagem de Resposta de Autenticação, agora com o estado "OK".

O dispositivo iniciador compara hash ali com o hash de sua chave pública B_I. Quando eles correspondem, o dispositivo iniciador também sabe que o dispositivo Respondedor capturou sua chave pública B_I a partir de sua tela. O dispositivo iniciador gera todas as chaves necessárias, para tanto, ele precisa de sua chave privada b_I e p_I, e executa todas as verificações criptográficas. Se todas essas verificações estiverem OK, o dispositivo Iniciador saberá que esteve se comunicando com o dispositivo que possui a chave privada b_R e possivelmente p_R, se este último também tiver sido usado e se o dispositivo Respondedor tiver obtido a B_I corretamente.

[221] Em um próximo estágio, se as verificações no estágio anterior estiverem todas OK, o dispositivo iniciador enviará uma mensagem de resposta de confirmação ao dispositivo respondedor com o estado "OK", onde, entre outras coisas, é usada uma chave derivada no modo Diffie-Hellman de b_I, para que o dispositivo iniciador possa provar a posse de b_I para o dispositivo respondedor. O dispositivo iniciador também usa as "outras informações do Respondedor", por exemplo, o *nonce* do Respondedor, de modo que o Respondedor possa ver que o Iniciador descriptografou-as corretamente.

[222] O sistema acima pode ser implementado em dispositivos portáteis, laptops, calculadores pessoais, pontos de acesso de Wi-Fi, dispositivos entre pares via Wi-Fi, dispositivos com conexão via Bluetooth, dispositivos com conexão ZigBee. No caso de ser usado Wi-Fi, a invenção é tipicamente implementada no software wpa_supplicant, consultar, por exemplo, https://en.wikipedia.org/wiki/wpa_supplicant.

[223] Em uma modalidade, o protocolo de autenticação entre um primeiro e um segundo dispositivos compreende um atributo adicional ou uma mensagem adicional que pode, por exemplo, ser adicionada ao protocolo de autenticação conforme definido no padrão IEEE 802.11, consultar a [ref. 1], que contém uma credencial (por exemplo, uma chave pública) ou um hash de uma credencial ou uma credencial criptografada. O segundo dispositivo tem que incluir tal credencial ou hash de uma credencial ou uma credencial criptografada como parte do intercâmbio de mensagens para o protocolo de autenticação. Para ser simétrico, o primeiro dispositivo também teria que incluir tal credencial, hash de uma credencial ou credencial criptografada. O campo preferencial que contém a credencial ou o hash de uma credencial ou uma credencial criptografada em uma mensagem do protocolo de autenticação é um campo no qual o sinal ou ao menos parte do sinal que transfere aquele campo é usado para medir o tempo de transmissão ou de chegada da mensagem, de modo que seja muito difícil, se não impossível, para outro dispositivo inserir sua credencial ou hash de sua credencial ou sua credencial criptografada em uma mensagem.

[224] Em uma modalidade, o primeiro processador de mensagem é disposto de modo a processar essa credencial ou hash de uma credencial ou credencial criptografada, e verificar se ela corresponde a uma credencial que foi usada anteriormente por um dispositivo com o qual ele executou corretamente a autenticação de dispositivo e estabeleceu confiança mútua, por exemplo, através do uso do protocolo de configuração protegido de Wi-Fi, do protocolo de provisionamento de dispositivo, da troca de chaves de Diffie-Hellman e/ou de handshake de 4 vias WPA2, consultar [1]. Se for encontrada uma correlação, o

primeiro dispositivo pode assumir que o segundo dispositivo pode ser verdadeiro e considerado confiável. Se nenhuma correlação for encontrada, o primeiro dispositivo desconfiará do segundo dispositivo e executará etapas adicionais para verificar a confiabilidade.

[225] Em uma modalidade alternativa, o segundo dispositivo tem que incluir uma credencial ou hash de credencial ou uma credencial criptografada que será usada durante a configuração de uma conexão posterior. O primeiro processador de mensagem é disposto de modo a processar e armazenar a credencial ou hash de credencial ou uma credencial criptografada recebida em conjunto com outros parâmetros do segundo dispositivo, para correlacionar seguramente com o dispositivo específico que se conecta com aquela credencial. Após a configuração da conexão entre o primeiro e o segundo dispositivos, o primeiro dispositivo verifica se a mesma credencial ou uma derivada sua é usada durante a realização da autenticação do dispositivo, por exemplo durante a execução do protocolo de configuração protegido de Wi-Fi, do protocolo de provisionamento de dispositivo, da troca de chaves Diffie Hellman e/ou enquanto é feito o handshake de 4 vias WPA2. Ao fazer isso, o primeiro dispositivo pode determinar que o dispositivo com o qual ele está conectado é o mesmo dispositivo para o qual uma autenticação específica foi feita. Em particular, se a credencial foi uma chave pública e se a configuração da conexão entre o primeiro e o segundo dispositivos incluiu que o segundo dispositivo provasse corretamente ao primeiro dispositivo que ele tem a posse da chave privada que pertence à chave pública como credencial, o

primeiro dispositivo pode ter certeza de que o segundo dispositivo é aquele que ele diz ser e não um impostor.

[226] A Figura 5 mostra um método para um Iniciador. O método é para uso em um dispositivo iniciador para comunicação sem fio com um dispositivo respondedor de acordo com um protocolo de comunicação e um protocolo de autenticação para acomodar autenticação. O protocolo exige estados do iniciador de acordo com o protocolo de autenticação dependente de interação com o usuário e mensagens recebidas a partir do dispositivo respondedor.

[227] O método começa no nó INÍCIO 501. No primeiro estágio, o método estabelece um estado inicial para carga inicial.

[228] Em uma etapa seguinte, o método ACRPK 502 executa a aquisição de uma chave pública B_R a partir do dispositivo respondedor através de uma ação fora da banda do dispositivo iniciador. Após a correta aquisição da B_R, o método, na etapa SARQ 503, aciona um estado de carga inicial indicando que a carga inicial foi realizada corretamente através da aquisição da chave pública do respondedor. Então o método continua mediante a composição de um pedido de autenticação ARQ que compreende um verificador do Iniciador ($H(B_I)$) para verificar uma chave pública do iniciador e um verificador do respondedor ($H(B_R)$) para verificar a chave pública do respondedor. A mensagem ARQ é enviada no estado de carga inicial. Então o método espera receber uma resposta de autenticação. Se não receber a resposta dentro de um tempo predeterminado, o método envia novamente a ARQ conforme indicado pela seta 513.

[229] Em uma fase seguinte RARP1 504, um estado de autenticação para executar a autenticação é acionado. Subsequentemente, o método recebe e se decompõe uma resposta de autenticação ARP1 que compreende dados de autenticação unilateral $\{R\text{-}auth1\}_{k1}$ com base em uma chave privada do dispositivo respondedor b_R correspondente à chave pública do respondedor B_R. O ARP1 tem um estado de andamento mútuo indicativo de que a autenticação mútua está em andamento para possibilitar que o dispositivo respondedor adquira a chave pública do iniciador a partir do dispositivo iniciador através de uma ação fora da banda do respondedor.

[230] Em uma fase seguinte AWMUT 505, um estado de autenticação mútua é acionado após receber o estado de andamento mútuo, para esperar autenticação mútua. Em seguida, uma resposta de autenticação mútua ARP2 é recebida e decomposta. A ARP2 compreende dados de autenticação mútua do respondedor $\{R\text{-}auth2\}_{k2}$ com base na chave pública B_I do iniciador e na chave privada b_R do respondedor.

[231] Em uma fase seguinte MUTC 506, um estado autenticado é acionado indicando que a autenticação foi realizada corretamente. Isso envolve receber a resposta de autenticação mútua ARP2 e processar corretamente os dados de autenticação mútua do respondedor $\{R\text{-}auth2\}_{k2}$ com base na chave pública de respondedor e na chave privada (b_I) do iniciador correspondente à chave pública (B_I) do iniciador. Então o método continua mediante a composição de uma confirmação de autenticação mútua ACF2 que compreende um estado de confirmação mútua indicativo de confirmação da autenticação mútua. O ACF2 também compreende dados de autenticação de iniciador mútuo $\{I\text{-}auth2\}_{k2}$ com base na chave pública do respondedor B_R e uma chave

privada do iniciador b_I correspondente à chave pública B_I do iniciador. O método então termina no nó FIM 507.

[232] A Figura 6 mostra um método para um respondedor. O método é para uso em um dispositivo respondedor para comunicação sem fio com um dispositivo iniciador de acordo com um protocolo de comunicação e um protocolo de autenticação para acomodar a autenticação. O protocolo exige estados do respondedor de acordo com o protocolo de autenticação dependente de interação com o usuário e mensagens recebidas a partir do dispositivo iniciador.

[233] O método começa no nó INÍCIO 601. Em uma primeira fase RARQ 602 o respondedor aciona um estado de espera para receber mensagens a partir do iniciador. Um pedido de autenticação ARQ é recebido e decomposto. O ARQ compreende um verificador iniciador $H(B_I)$ para verificar uma chave pública do iniciador e um verificador do respondedor $H(B_R)$ para verificar a chave pública do respondedor.

[234] Em uma fase seguinte SARP1 603, o método aciona um estado de autenticação do respondedor para executar a autenticação. O estado de autenticação do respondedor é acionado após processar corretamente o pedido de autenticação. Em seguida, é composta uma resposta de autenticação ARP1, compreendendo dados de autenticação unilateral do respondedor $\{R\text{-}auth1\}_{k1}$ com base em uma chave privada b_R do respondedor correspondente à chave pública B_R do respondedor e um estado de andamento mútuo indicativo da autenticação mútua estar em andamento.

[235] Em uma fase seguinte MUTA 604, um estado de autenticação mútua do respondedor é acionado. Agora, o (usuário do) dispositivo respondedor é capaz de adquirir uma

chave pública do iniciador a partir do dispositivo iniciador através de uma ação fora da banda do respondedor. Isto pode levar algum tempo conforme indicado por uma seta 614 reentrando no estado. Depois de adquirir corretamente a chave pública do iniciador, uma resposta de autenticação mútua ARP2 é composta e enviada no estado de autenticação mútua do respondedor. O ARP2 compreende dados de autenticação mútua do respondedor $\{R\text{-}auth2\}_{k2}$ com base na chave pública B_I do iniciador e em uma chave privada do respondedor de b_R correspondente à chave pública B_R do respondedor.

[236] Em uma fase seguinte WMUC 605, um estado autenticado do respondedor é acionado indicando que a autenticação foi realizada corretamente. Uma confirmação de autenticação mútua ACF2 é recebida e decomposta. O ACF2 compreende um estado de confirmação mútua indicando a confirmação da autenticação mútua e os dados de autenticação mútua do iniciador $\{I\text{-}auth2\}_{k2}$ com base na chave pública B_R do respondedor e em uma chave privada b_I do iniciador correspondente à chave pública (B_I) do iniciador. O estado autenticado é acionado após o correto processamento dos dados de autenticação mútua do iniciador com base na chave pública do iniciador (B_I) e na chave privada do respondedor (b_R). O método agora termina no nó FIM 606.

[237] São fornecidos produtos de programa de computador, que podem ser baixados a partir de uma rede e/ou armazenados em uma mídia legível por computador e/ou uma mídia executável por microprocessador, compreendendo instruções de código de programa para implementar os métodos acima quando executados em um computador para proteger informações de localização, conforme elucidado adicionalmente abaixo.

[238] O sistema acima pode ser aplicado, por exemplo, em ambientes internos e externos, em sistemas de comunicação sem fio de curto alcance, onde a autenticação é suportada através de um protocolo de autenticação. Por exemplo, o sistema pode ser aplicado em dispositivos portáteis e dispositivos estacionários que suportam Wi-Fi, Wi-Fi Aware ou Wi-Fi Direct.

[239] Geralmente, cada um dentre o dispositivo iniciador e o dispositivo respondedor de interação compreende um processador que executa softwares adequados armazenados no dispositivo; por exemplo, aquele software pode ter sido baixado e/ou armazenado em uma memória correspondente, por exemplo uma memória volátil, como RAM, ou uma memória não volátil, como Flash (não mostrada). Os dispositivos e servidores podem ser equipados, por exemplo, com microprocessadores e memórias (não mostrados). Alternativamente, os dispositivos e o servidor podem, total ou parcialmente, ser implementados em lógica programável, por exemplo como matriz de portas programável em campo (FPGA - "field-programmable gate array"). Os dispositivos e o servidor podem ser implementados, total ou parcialmente, como um, assim chamado, circuito integrado para aplicação específica (ASIC - "application-specific integrated circuit"), isto é, um circuito integrado (CI) personalizado para seu uso específico. Por exemplo, os circuitos podem ser implementados em CMOS, por exemplo, com o uso de uma linguagem de descrição de hardware como Verilog, VHDL etc.

[240] Muitas formas diferentes de execução do método são possíveis, conforme ficará evidente para o versado na técnica. Por exemplo, a ordem dos estágios ou das etapas pode ser variada ou alguns estágios podem ser executados em

paralelo. Além disso, outras etapas de método podem ser inseridas entre as etapas. As etapas inseridas podem representar modificações no método, conforme aqui descrito, ou podem não estar relacionadas ao método.

[241] Um método, de acordo com a invenção, pode ser executado com o uso de software, que compreende as instruções para fazer com que um sistema de processador execute o respectivo método. O software pode incluir apenas aquelas etapas empregadas por uma subentidade específica do sistema. O software pode ser armazenado em uma mídia de armazenamento adequada, como um disco rígido, um disquete, uma memória, etc. O software pode ser enviado como um sinal por uma rede com fio, ou sem fio, ou com o uso de uma rede de dados, por exemplo a Internet. O software pode ser disponibilizado para download e/ou para uso remoto em um servidor. Um método de acordo com a invenção pode ser executado com o uso de um fluxo de bits disposto de modo a configurar uma lógica programável, por exemplo, uma matriz de portas programável em campo (FPGA), para executar o método. Será reconhecido que o software pode estar sob a forma de código fonte, código objeto, uma fonte de códigos intermediários, um código objeto em formato parcialmente compilado, ou em qualquer outro formato adequado para uso na implementação do método de acordo com a invenção. Uma modalidade relacionada a um produto de programa de computador compreende instruções executáveis por computador que correspondem a cada uma das etapas de processamento de pelo menos um dos métodos apresentados. Essas instruções podem ser subdivididas em sub-rotinas e/ou ser armazenadas em um ou mais arquivos que podem estar estatica ou dinamicamente ligados. Outra modalidade relacionada a um produto de programa

de computador compreende instruções executáveis por computador que correspondem a cada um dos meios de pelo menos um dos sistemas e/ou produtos apresentados.

[242] A Figura 7a mostra uma mídia legível por computador 1000 tendo uma parte gravável 1010 que compreende um programa de computador 1020, sendo que o programa de computador 1020 compreende instruções para fazer com que o sistema processador execute um ou mais dos métodos acima no sistema conforme descrito acima. O programa de computador 1020 pode ser incorporado em uma mídia legível por computador não-transparente 1000 como marcadores físicos ou por meio de magnetização de elementos da mídia legível por computador 1000. Entretanto, qualquer outra modalidade adequada também é concebível. Além disso, deve-se considerar que, embora a mídia legível por computador 1000 seja mostrada aqui como um disco óptico, a mídia legível por computador 1000 pode ser qualquer mídia legível por computador adequada, como um disco rígido, memória de estado sólido, memória Flash etc., e pode ser gravável ou não gravável. O programa de computador 1020 compreende instruções para fazer com que um sistema processador execute os ditos métodos.

[243] A Figura 7b mostra uma representação esquemática de um sistema processador 1100 de acordo com uma modalidade do dispositivo ou do servidor conforme descrito acima. O sistema processador pode compreender um circuito 1110, por exemplo, um ou mais circuitos integrados. A arquitetura do circuito 1110 é esquematicamente mostrada na Figura. O circuito 1110 compreende uma unidade de processamento 1120, por exemplo uma CPU, para executar componentes de programas de computador para executar um método de acordo com uma modalidade e/ou

implementar seus módulos ou unidades. O circuito 1110 compreende uma memória 1122 para armazenar códigos de programação, dados etc. Parte da memória 1122 pode ser apenas de leitura. O circuito 1110 pode compreender um elemento de comunicação 1126, por exemplo, uma antena, conectores ou ambos e similares. O circuito 1110 pode compreender um circuito integrado dedicado 1124 para executar parte ou todo o processamento definido no método. O processador 1120, a memória 1122, o CI dedicado 1124 e o elemento de comunicação 1126 podem ser conectados entre si através de um interconector 1130, como um barramento. O sistema processador 1110 pode ser disposto para comunicação com contato e/ou sem contato, com o uso de uma antena e/ou conectores, respectivamente.

[244] Em resumo, um sistema de comunicação sem fio pode ter um dispositivo iniciador e um dispositivo respondedor dispostos para comunicação sem fio. O sistema de comunicação sem fio possibilita a autenticação unilateral de um dispositivo respondedor por um dispositivo iniciador e a autenticação mútua de ambos os dispositivos. As modalidades do Iniciador podem ter uma unidade de mensagem e uma máquina de estado. O Iniciador inicia ao adquirir uma chave pública do respondedor através de uma ação fora da banda e envia um pedido de autenticação. O Respondedor envia uma resposta de autenticação compreendendo os dados de autenticação do respondedor com base em uma chave privada do respondedor e um estado de andamento mútuo indicativo de que a autenticação mútua está em andamento, para possibilitar que o dispositivo respondedor adquira a chave pública do iniciador através de uma ação fora da banda do respondedor. A máquina de estado do iniciador é disposta de modo a fornecer um estado de

autenticação mútua, acionado mediante o recebimento do estado de andamento mútuo, para esperar autenticação mútua. Assim, evita-se períodos longos de interrupção durante a comunicação sem fio, além de possibilitar que o iniciador relate erros de comunicação ao usuário dentro de um curto período de tempo.

[245] Deve-se entender que a descrição acima, para maior clareza, descreve as modalidades da invenção com referência a diferentes unidades funcionais e processadores. Entretanto, ficará evidente que qualquer distribuição adequada da funcionalidade entre as diferentes unidades funcionais ou os processadores pode ser usada, sem que se desvie do escopo da invenção. Por exemplo, a funcionalidade ilustrada a ser executada por unidades, processadores ou controladores separados pode ser executada pelo mesmo processador ou controlador. Por isso, as referências a unidades funcionais específicas devem ser consideradas apenas como referência a meios adequados de fornecer a funcionalidade descrita, e não como indicadoras de uma estrutura física rígida ou de uma organização lógica ou física estrita. A invenção pode ser implementada em qualquer forma adequada, incluindo hardware, software, firmware ou qualquer combinação dos mesmos.

[246] Deve-se notar que o termo "que compreende" não exclui a presença de elementos ou etapas diferentes daquelas mencionadas, e o artigo indefinido "um" ou "uma" antes de um elemento não exclui a presença de uma pluralidade de tais elementos, que nenhuma referência numérica limita o escopo das reivindicações, que a invenção pode ser implementada tanto por meio de hardware como de software, e que vários "meios" ou "unidades" podem ser representados pelo mesmo item de hardware ou de software, e um processador pode exercer a função de uma

ou mais unidades, possivelmente em cooperação com elementos de hardware. Adicionalmente, a invenção não se limita às modalidades, e a invenção se encontra em toda e qualquer característica inovadora ou combinação de características descritas acima ou mencionadas em reivindicações dependentes mutuamente diferentes.

Documentos de referência:

[247] [1] IEEE Computer Society, "IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," (IEEE Std. 802.11-2016), dezembro de 2016

[248] [2] Wi-Fi Simple Configuration - Technical Specification - Version 2.0.5

[249] "Specification for easy, secure setup and introduction of devices into WPA2-enabled 802.11 networks", Wi-Fi Alliance, 2014.

[250] [3] RFC 5297, Synthetic Initialization Vector (SIV) Authenticated Encryption Using the Advanced Encryption Standard (AES), outubro de 2008, (https://datatracker.ietf.org/doc/rfc5297/)

[251] [4] FIPS180-4, "Secure Hash Standard", United States of America, National Institute of Standards and Technology, Federal Information Processing Standard (FIPS) 180-4

[252] [5] NFC Forum Connection Handover Candidate Technical Specification, dezembro de 2015, (http://nfc-forum.org/product/nfc-forum-connection-handover-candidate-technical-specification-version-1-4/)

[253] [6] Diffie, W.; Hellman, M. (1976), "New directions in cryptography", IEEE Transactions on Information Theory, 22 (6): 644 a 654

[254] [7] Rivest, R.; Shamir, A.; Adleman, L. (fevereiro de 1978). "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of the ACM. 21 (2): 120 a 126.

[255] [8] Koblitz, N. (1987). "Elliptic curve cryptosystems". Mathematics of Computation. 48 (177): 203 a 209.

REIVINDICAÇÕES

1. DISPOSITIVO INICIADOR, caracterizado por ser disposto para comunicação sem fio com um dispositivo respondedor de acordo com um protocolo de comunicação, sendo que o protocolo de comunicação compreende um protocolo de autenticação para acomodar uma autenticação sendo uma dentre:

- autenticação unilateral do dispositivo respondedor pelo dispositivo iniciador e

- autenticação mútua do dispositivo respondedor pelo dispositivo iniciador e do dispositivo iniciador pelo dispositivo respondedor;

sendo que o dispositivo respondedor (120) compreende:

- um transceptor do respondedor disposto para comunicação sem fio de acordo com o protocolo de comunicação e

- um processador do respondedor disposto de modo a processar o protocolo de comunicação,

sendo que o dispositivo iniciador (110) compreende:

- um transceptor do iniciador (111) disposto para comunicação sem fio de acordo com o protocolo de comunicação,

- um processador do iniciador (112) disposto para processar o protocolo de comunicação e tendo:

- uma unidade de mensagem do iniciador (116) para compor mensagens a serem enviadas para o dispositivo respondedor e para decompor mensagens recebidas a partir do dispositivo respondedor de acordo com o protocolo de autenticação; e

- uma máquina de estado do iniciador (117) para fornecer estados do iniciador de acordo com o protocolo de

autenticação dependentes da interação com o usuário e das mensagens recebidas a partir do dispositivo respondedor, sendo que os estados do iniciador compreendem:

um estado inicial (IST) para carga inicial mediante a aquisição de uma chave pública do respondedor a partir do dispositivo respondedor através de uma ação fora da banda do iniciador,

um estado de carga inicial (BST) indicativo de que a carga inicial foi executada corretamente mediante a aquisição da chave pública do respondedor, e

um estado autenticado (ATD) indicativo de que a autenticação foi executada corretamente;

sendo que a unidade de mensagem do iniciador está disposta de modo a compor mensagens que compreendem:

- um pedido de autenticação (ARQ) a ser enviado no estado de carga inicial e que compreende um verificador do iniciador ($H(B_I)$) para verificar uma chave pública do iniciador e um verificador do respondedor ($H(B_R)$) para verificar a chave pública do respondedor;

e disposta de modo a decompor mensagens que compreendem:

- uma resposta de autenticação (ARP1) que compreende dados de autenticação unilateral do respondedor ($\{R\text{-}auth1\}_{k1}$) com base em uma chave privada do respondedor (b_R) correspondente à chave pública do respondedor (B_R) e um estado de andamento mútuo (MPS) indicativo de que a autenticação mútua está em andamento para possibilitar que o dispositivo respondedor adquira a chave pública do iniciador a partir do dispositivo iniciador através de uma ação fora da banda do respondedor; e

sendo que a máquina de estado do iniciador é disposta para fornecer um estado de autenticação mútua, acionado mediante o recebimento do estado de andamento mútuo, para esperar autenticação mútua,

a unidade de mensagem do iniciador é disposta de modo a decompor

- uma resposta de autenticação mútua (ARP2) que compreende dados de autenticação mútua do respondedor ($\{R\text{-}auth2\}_{k2}$ com base na chave pública do iniciador (B_I) e na chave privada do respondedor (b_R);

e disposta de modo a compor

- uma confirmação de autenticação mútua (ACF2) que compreende um estado de confirmação mútua (MCS) que indica a confirmação da autenticação mútua e os dados de autenticação mútua do iniciador ($\{I\text{-}auth2\}_{k2}$ com base na chave pública do respondedor (B_R) e em uma chave privada do iniciador (b_I) correspondente à chave pública do iniciador (B_I).

2. DISPOSITIVO, de acordo com a reivindicação 1, caracterizado pela máquina de estado do iniciador estar disposta de modo a ativar o estado autenticado mediante o recebimento da resposta de autenticação mútua (ARP2) e pelo processador do iniciador processar corretamente os dados de autenticação mútua do respondedor com base na chave pública do respondedor e em uma chave privada do iniciador (b_I) correspondente à chave pública do iniciador (B_I).

3. DISPOSITIVO, de acordo com a reivindicação 1, caracterizado por:

a unidade de mensagem iniciadora estar disposta de modo a decompor, no caso de autenticação unilateral, uma resposta de autenticação unilateral (ARP1) que compreende

dados de autenticação unilateral do respondedor ($\{R\text{-}auth1\}_{k1}$) com base em uma chave privada do respondedor (b_R) correspondente à chave pública do respondedor (B_R) e em um estado unilateral indicativo da autenticação unilateral; e

a máquina de estado do iniciador estar disposta de modo a ativar o estado autenticado no processador do iniciador que processa corretamente os dados de autenticação unilateral do respondedor ({R-auth1} k1) com base na chave pública do respondedor e em uma chave privada do iniciador (p_I) correspondente a uma chave pública do iniciador (P_I).

4. DISPOSITIVO, de acordo com qualquer uma das reivindicações 2 ou 3, caracterizado por:

a máquina de estado do iniciador estar disposta de modo a ativar o estado de carga inicial ou o estado inicial mediante o recebimento da resposta de autenticação (ARP1) e pelo processador do iniciador processar incorretamente os dados de autenticação unilateral do respondedor ($\{R\text{-}auth1\}_{k1}$).

5. DISPOSITIVO, de acordo com a reivindicação 2, caracterizado por:

a máquina de estado do iniciador estar disposta de modo a ativar o estado de carga inicial ou o estado inicial mediante o recebimento da resposta de autenticação mútua (ARP2) e pelo processador do iniciador processar incorretamente os dados de autenticação mútua do respondedor ($\{R\text{-}auth2\}_{k2}$).

6. DISPOSITIVO, de acordo com qualquer uma das reivindicações 2 ou 5, caracterizado por:

a unidade de mensagem do iniciador estar disposta de modo a compor, mediante o recebimento do estado de andamento mútuo, uma confirmação de espera de autenticação (ACF1) que

compreende um estado de espera mútuo (“MAS” - Mutual Awaiting Status).

7. DISPOSITIVO RESPONDEDOR, caracterizado por ser disposto para comunicação sem fio com um dispositivo iniciador de acordo com um protocolo de comunicação, sendo que o protocolo de comunicação compreende um protocolo de autenticação para acomodar uma autenticação sendo uma dentre

- autenticação unilateral do dispositivo respondedor pelo dispositivo iniciador e

- autenticação mútua do dispositivo respondedor pelo dispositivo iniciador e do dispositivo iniciador pelo dispositivo respondedor;

sendo que o dispositivo iniciador (110) compreende:

- um transceptor do iniciador (111) disposto para comunicação sem fio de acordo com o protocolo de comunicação,

- um processador do iniciador (112) disposto de modo a processar o protocolo de comunicação e

sendo que o dispositivo respondedor (120) compreende

- um transceptor do respondedor (121) disposto para comunicação sem fio de acordo com o protocolo de comunicação,

- um processador do respondedor (122) disposto de modo a processar o protocolo de comunicação e que tem

- uma unidade de mensagem do respondedor (126) para compor mensagens a serem enviadas para o dispositivo iniciador e para decompor mensagens recebidas a partir do dispositivo iniciador de acordo com o protocolo de autenticação,

- uma máquina de estado do respondedor (127) para fornecer estados do respondedor de acordo com o protocolo de autenticação dependentes da interação com o usuário e das

mensagens recebidas a partir do dispositivo iniciador, sendo que os estados do respondedor compreendem:

um estado de espera (AWG) para receber mensagens a partir do iniciador, e

um estado autenticado do respondedor (ATD) indicativo de que a autenticação foi feita corretamente;

sendo que a máquina de estado do respondedor é disposta de modo a fornecer um estado de autenticação mútua do respondedor (AR2) para possibilitar que o dispositivo respondedor adquira uma chave pública de iniciador a partir do dispositivo iniciador através de uma ação fora da banda do respondedor; e

sendo que a unidade de mensagem do respondedor é disposta de modo a compor mensagens que compreendem

- uma resposta de autenticação (ARP1) que compreende dados de autenticação unilateral do respondedor ($\{R\text{-}auth1\}_{k1}$ com base em uma chave privada do respondedor (b_R) correspondente à chave pública do respondedor (B_R) e em um estado de andamento mútuo indicativo da autenticação mútua estar em andamento;

e disposta de modo a decompor as mensagens que compreendem

- um pedido de autenticação (ARQ) que compreende um verificador do iniciador $H(B_I)$ para verificar uma chave pública do iniciador e um verificador do respondedor $H(B_R)$ para verificar a chave pública do respondedor;

sendo que a máquina de estado do respondedor está disposta de modo a, após o processador do respondedor processar corretamente os dados de autenticação do iniciador ($\{I\text{-}auth2\}$) com base na chave pública do iniciador (B_I) e na chave privada

do respondedor (b_R), ativar o estado autenticado do respondedor.

8. DISPOSITIVO, de acordo com a reivindicação 7, caracterizado pela unidade de mensagem do respondedor ser disposta de modo a compor

- uma resposta de autenticação mútua (ARP2) a ser enviada no estado de autenticação mútua do respondedor e que compreende dados de autenticação mútua do respondedor ($\{R\text{-}auth2\}_{k2}$) com base na chave pública do iniciador (B_I) e em uma chave privada do respondedor (b_R) correspondente à chave pública do respondedor (B_R);

e disposta de modo a decompor

- uma confirmação de autenticação mútua (ACF2) que compreende um estado de confirmação mútua que indica a confirmação da autenticação mútua e os dados de autenticação mútua do iniciador ($\{I\text{-}auth2\}_{k2}$ com base na chave pública do respondedor (B_R) e em uma chave privada do iniciador (b_I) correspondente à chave pública do iniciador (B_I).

9. DISPOSITIVO, de acordo com qualquer uma das reivindicações 7 ou 8, caracterizado por:

a unidade de mensagem do respondedor estar disposta de modo a compor, no caso de autenticação unilateral, uma resposta de autenticação unilateral (ARP1) que compreende dados de autenticação unilateral do respondedor ($\{R\text{-}auth1\}_{k1}$) com base em uma chave privada do respondedor (b_R) correspondente à chave pública do respondedor (B_R) e em um estado unilateral indicativo da autenticação unilateral; e

pela máquina de estado do respondedor estar disposta de modo a, no caso de autenticação unilateral, ativar o estado autenticado do respondedor mediante o recebimento de uma

confirmação de autenticação unilateral (ACF1) e pelo processador do respondedor processar corretamente os dados de autenticação unilateral do iniciador ($\{I\text{-}auth1\}_{k1}$).

10. DISPOSITIVO, de acordo com a reivindicação 8, caracterizado por:

a máquina de estado do respondedor estar disposta de modo a ativar o estado de espera mediante o recebimento da confirmação de autenticação mútua (ACF2) e pelo processador do respondedor processar incorretamente os dados de autenticação mútua do iniciador ($\{I\text{-}auth2\}_{k2}$.

11. DISPOSITIVO, de acordo com qualquer uma das reivindicações 8 ou 10, caracterizado por:

a unidade de mensagem do respondedor estar disposta de modo a decompor uma confirmação de espera de autenticação mútua (ACF1) que compreende um estado de espera mútuo, e

a máquina de estado do respondedor ser disposta de modo a ativar o estado de autenticação mútua do respondedor (AR2) mediante o recebimento do estado de espera mútua.

12. DISPOSITIVO, de acordo com a reivindicação 11, caracterizado por:

a unidade de mensagem do respondedor estar disposta de modo a decompor adicionalmente a confirmação de espera de autenticação (ACF1) que compreende dados de autenticação unilateral do iniciador ($\{I\text{-}auth1\}_{k1}$), e pela máquina de estado do respondedor estar disposta de modo a ativar o estado de espera após o processador do respondedor processar corretamente os dados de autenticação unilateral do iniciador.

13. DISPOSITIVO, de acordo com qualquer uma das reivindicações 7 a 12, sendo que o dispositivo respondedor é caracterizado por compreender:

- uma interface de usuário do respondedor (123) disposta de modo a acomodar a interação com o usuário para executar a ação fora da banda do respondedor para adquirir a chave pública do iniciador a partir do dispositivo iniciador.

14. SISTEMA DE COMUNICAÇÃO SEM FIO, caracterizado por compreender um dispositivo iniciador (110) conforme definido em qualquer uma das reivindicações 1 a 6, e um dispositivo respondedor (120,120') conforme definido em qualquer uma das reivindicações 7 a 13.

15. MÉTODO DO INICIADOR PARA USO EM UM DISPOSITIVO INICIADOR (11) PARA COMUNICAÇÃO SEM FIO COM UM DISPOSITIVO RESPONDEDOR, de acordo com um protocolo de comunicação, sendo que o protocolo de comunicação compreende um protocolo de autenticação para acomodar uma autenticação sendo uma dentre:

- autenticação unilateral do dispositivo respondedor pelo dispositivo iniciador e

- autenticação mútua do dispositivo respondedor pelo dispositivo iniciador e do dispositivo iniciador pelo dispositivo respondedor;

sendo que o método é caracterizado por compreender

- fornecer estados do iniciador de acordo com o protocolo de autenticação dependentes da interação com o usuário e das mensagens recebidas a partir do dispositivo respondedor, sendo que os estados do iniciador compreendem

um estado inicial para carga inicial mediante a aquisição de uma chave pública do respondedor proveniente do dispositivo respondedor através de uma ação fora da banda do iniciador,

um estado de carga inicial indicativo de que a carga inicial foi executada corretamente mediante a aquisição da chave pública do respondedor, e

um estado autenticado indicativo de que a autenticação foi executada corretamente;

- compor um pedido de autenticação (ARQ) a ser enviado no estado de carga inicial e que compreende um verificador do iniciador ($H(B_I)$) para verificar uma chave pública do iniciador e um verificador do respondedor ($H(B_R)$) para verificar a chave pública do respondedor;

- decompor uma resposta de autenticação (ARP1) que compreende dados de autenticação unilateral do respondedor ($\{R\text{-}auth1\}_{k1}$) com base em uma chave privada do respondedor (b_R) correspondente à chave pública do respondedor (B_R) e em um estado de andamento mútuo indicativo de que a autenticação mútua está em andamento para possibilitar que o dispositivo respondedor adquira a chave pública do iniciador a partir do dispositivo iniciador através de uma ação fora da banda do respondedor;

- fornecer um estado de autenticação mútua, acionado mediante o recebimento do estado de andamento mútuo, para esperar autenticação mútua;

- decompor uma resposta de autenticação mútua (ARP2) que compreende dados de autenticação mútua do respondedor ($\{R\text{-}auth2\}_{k2}$ com base na chave pública do iniciador (B_I) e na chave privada do respondedor (b_R);

- compor uma confirmação de autenticação mútua (ACF2) que compreende um estado de confirmação mútua que indica a confirmação da autenticação mútua e os dados de autenticação mútua do iniciador ($\{I\text{-}auth2\}_{k2}$ com base na chave pública do

respondedor (B_R) e em uma chave privada do iniciador (b_I) correspondente à chave pública do iniciador (B_I); e

- ativar o estado autenticado mediante o recebimento da resposta de autenticação mútua (ARP2) e processar corretamente os dados de autenticação mútua do respondedor com base na chave pública do respondedor e em uma chave privada do iniciador (b_I) correspondente à chave pública do iniciador (B_I).

16. MÉTODO DO RESPONDEDOR PARA USO EM UM DISPOSITIVO RESPONDEDOR PARA COMUNICAÇÃO SEM FIO COM UM DISPOSITIVO INICIADOR DE ACORDO COM UM PROTOCOLO DE COMUNICAÇÃO, sendo que o protocolo de comunicação compreende um protocolo de autenticação para acomodar uma autenticação sendo uma dentre

- autenticação unilateral do dispositivo respondedor pelo dispositivo iniciador e

- autenticação mútua do dispositivo respondedor pelo dispositivo iniciador e do dispositivo iniciador pelo dispositivo respondedor;

sendo que o método é caracterizado por compreender

- fornecer estados do respondedor de acordo com o protocolo de autenticação dependentes da interação com o usuário e das mensagens recebidas a partir do dispositivo iniciador, sendo que os estados do respondedor compreendem

um estado de espera para receber mensagens a partir do iniciador, e

um estado autenticado do respondedor indicativo de que a autenticação foi realizada corretamente;

- compor uma resposta de autenticação (ARP1) que compreende dados de autenticação unilateral do respondedor ($\{R\text{-}auth1\}_{k1}$ com base em uma chave privada do respondedor (b_R)

correspondente à chave pública do respondedor (B_R) e em um estado de andamento mútuo indicativo de que a autenticação mútua está em andamento;

- fornecer um estado de autenticação mútua do respondedor (AR2) para possibilitar que o dispositivo respondedor adquira uma chave pública do iniciador a partir do dispositivo iniciador através de uma ação fora da banda do respondedor;

- compor uma resposta de autenticação mútua (ARP2) a ser enviada no estado de autenticação mútua do respondedor e que compreende dados de autenticação mútua do respondedor ($\{R\text{-}auth2\}_{k2}$) com base na chave pública do iniciador (B_I) e em uma chave privada do respondedor (b_R) correspondente à chave pública do respondedor (B_R);

- decompor um pedido de autenticação (ARQ) que compreende um verificador do iniciador $H(B_I)$ para verificar uma chave pública do iniciador e um verificador do respondedor $H(B_R)$ para verificar a chave pública do respondedor;

- ativar o estado de autenticação do respondedor (AG1) mediante o processamento correto do pedido de autenticação.

17. MÉTODO DO RESPONDEDOR, de acordo com a reivindicação 16, sendo que o método é caracterizado por compreender adicionalmente:

- decompor uma confirmação de autenticação mútua (ACF2) que compreende um estado de confirmação mútua que indica a confirmação da autenticação mútua e os dados de autenticação mútua do iniciador ($\{I\text{-}auth2\}_{k2}$) com base na chave pública do respondedor (B_R) e em uma chave privada do iniciador (b_I) correspondente à chave pública do iniciador (B_I);

- ativar o estado autenticado do respondedor mediante o processamento correto dos dados de autenticação mútua do iniciador com base na chave pública do iniciador (B_I) e na chave privada do respondedor (b_R).

18. PRODUTO DE PROGRAMA DE COMPUTADOR transferível por download a partir de uma rede e/ou armazenado em uma mídia legível por computador e/ou mídia executável por microprocessador, sendo que o produto é caracterizado por compreender instruções de código de programa para implementar um método conforme definido na reivindicação 14 ou um método conforme definido na reivindicação 16, quando executado em um computador.

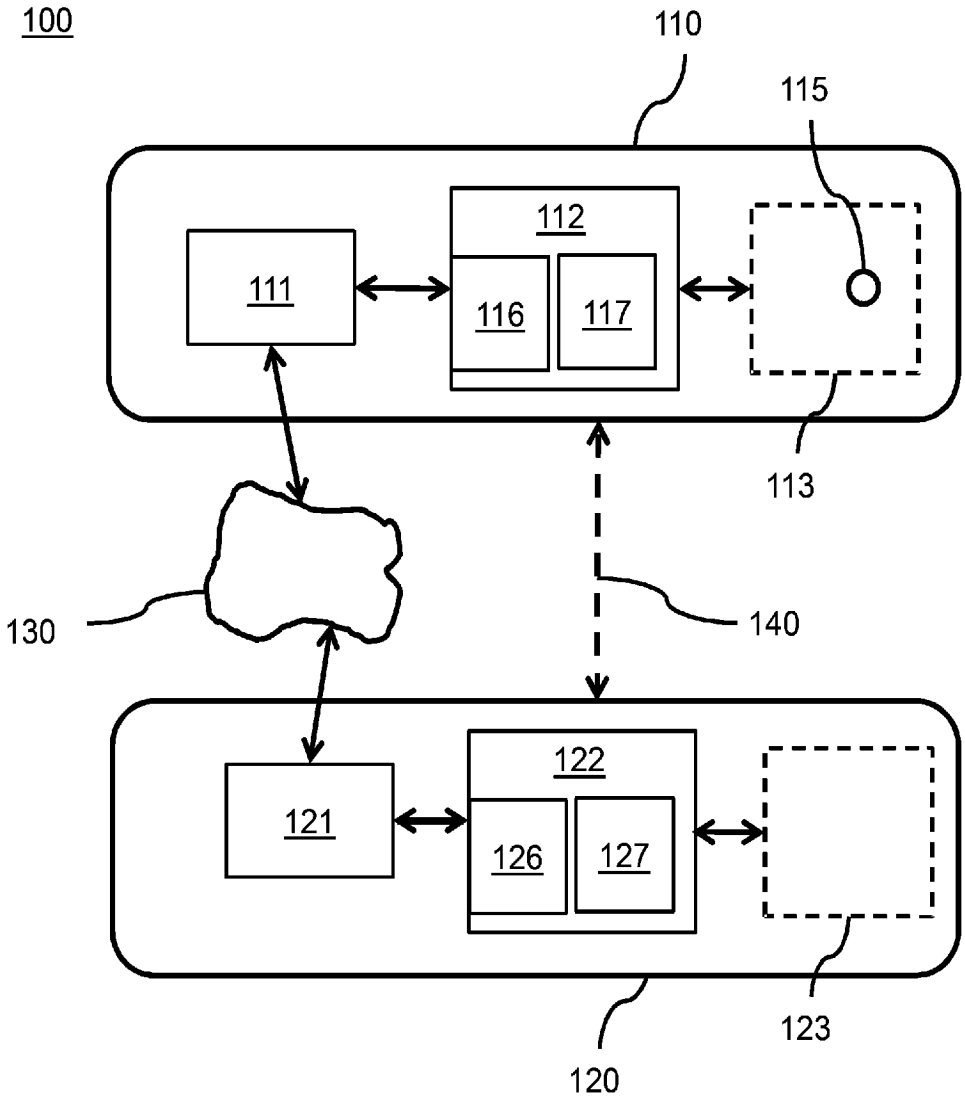


Fig. 1

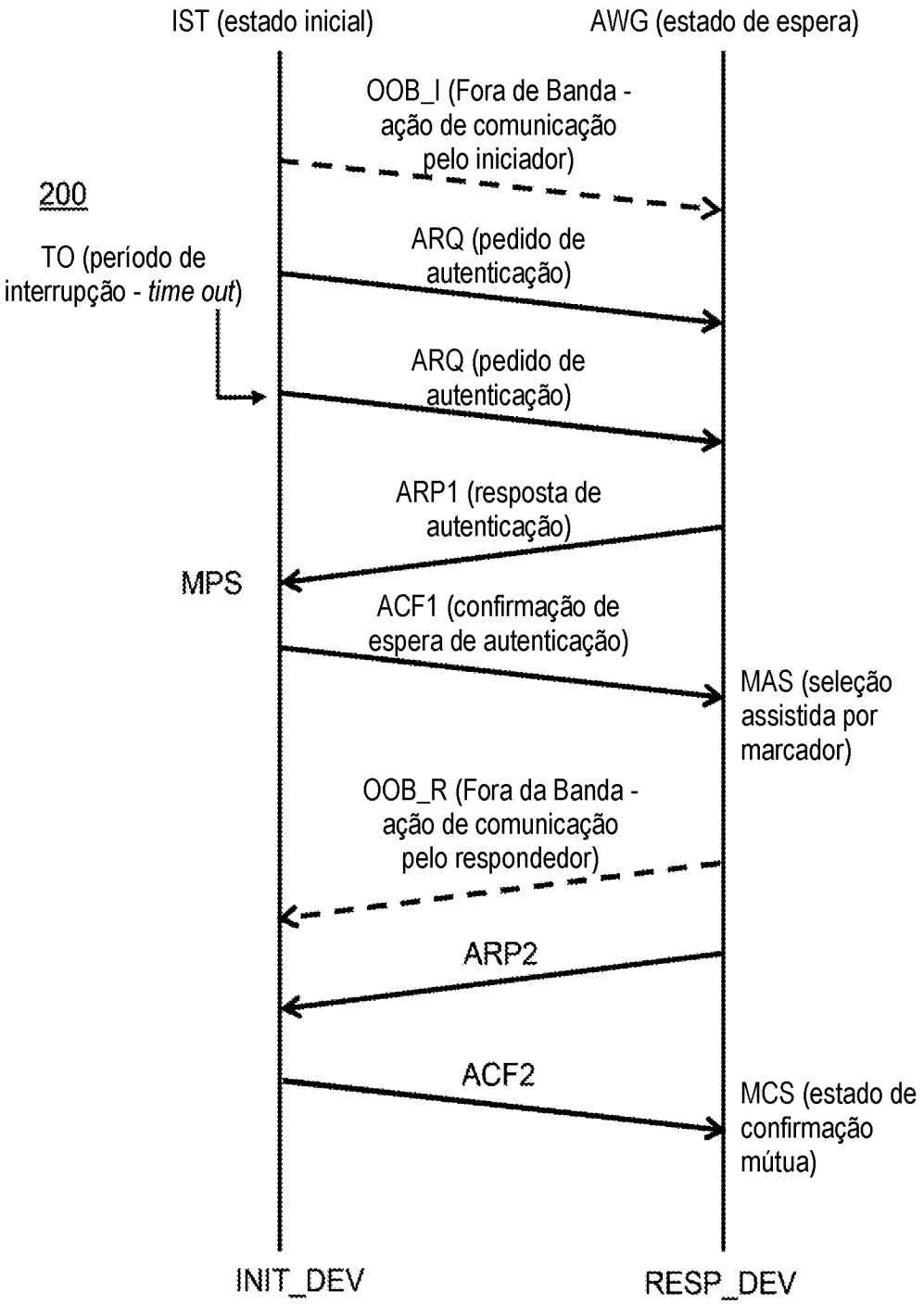

IST (estado inicial)
AWG (estado de espera)
OOB_I (Fora de Banda - ação de comunicação pelo iniciador)
200
TO (período de interrupção - time out)
ARQ (pedido de autenticação)
ARQ (pedido de autenticação)
ARP1 (resposta de autenticação)
MPS
ACF1 (confirmação de espera de autenticação)
MAS (seleção assistida por marcador)
OOB_R (Fora da Banda - ação de comunicação pelo respondedor)
ARP2
ACF2
MCS (estado de confirmação mútua)
INIT_DEV
RESP_DEV

Fig. 2

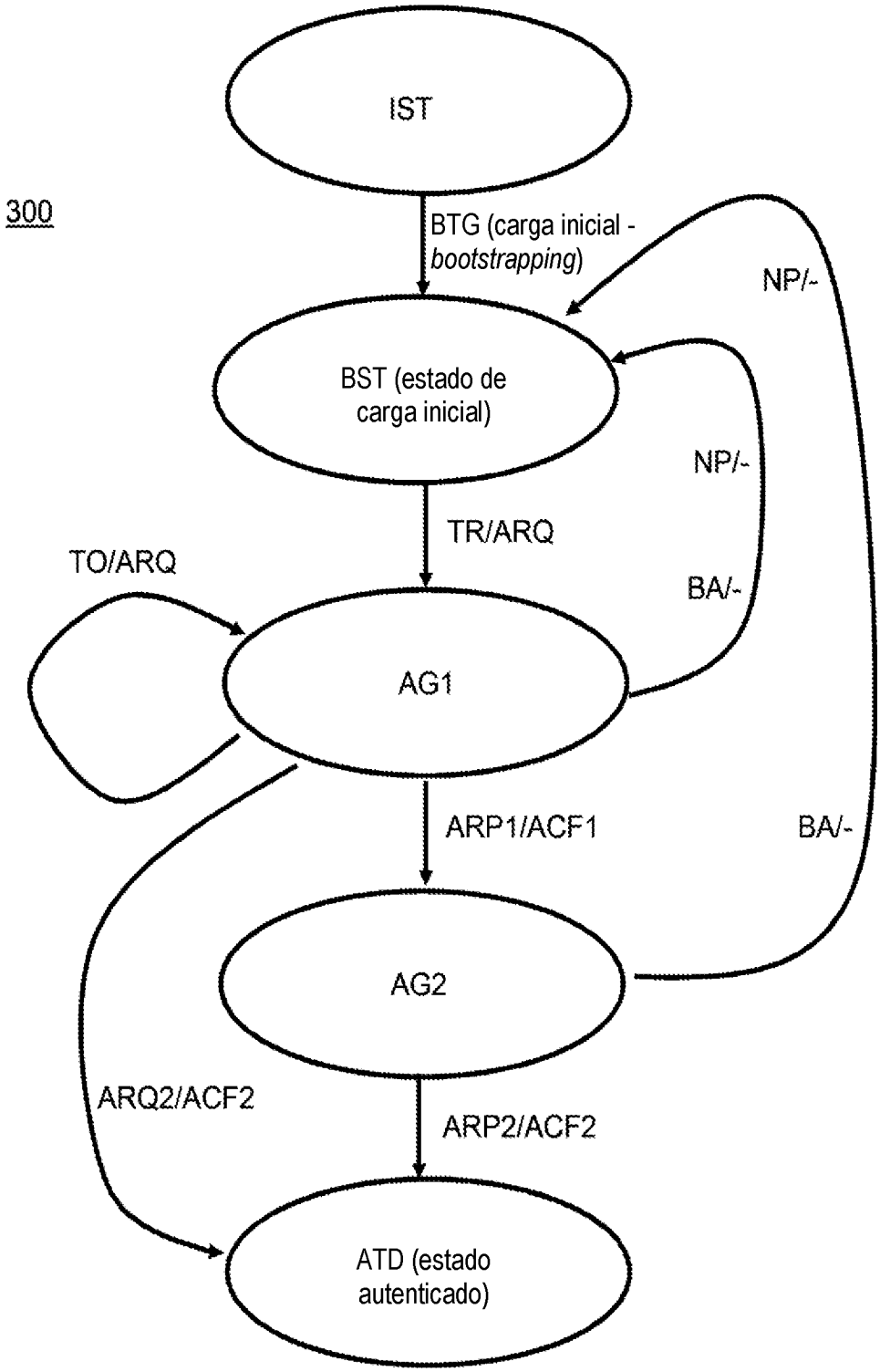

300
IST
BTG (carga inicial - *bootstrapping*)
NP/-
BST (estado de carga inicial)
NP/-
TR/ARQ
TO/ARQ
BA/-
AG1
ARP1/ACF1
BA/-
AG2
ARQ2/ACF2
ARP2/ACF2
ATD (estado autenticado)

Fig. 3

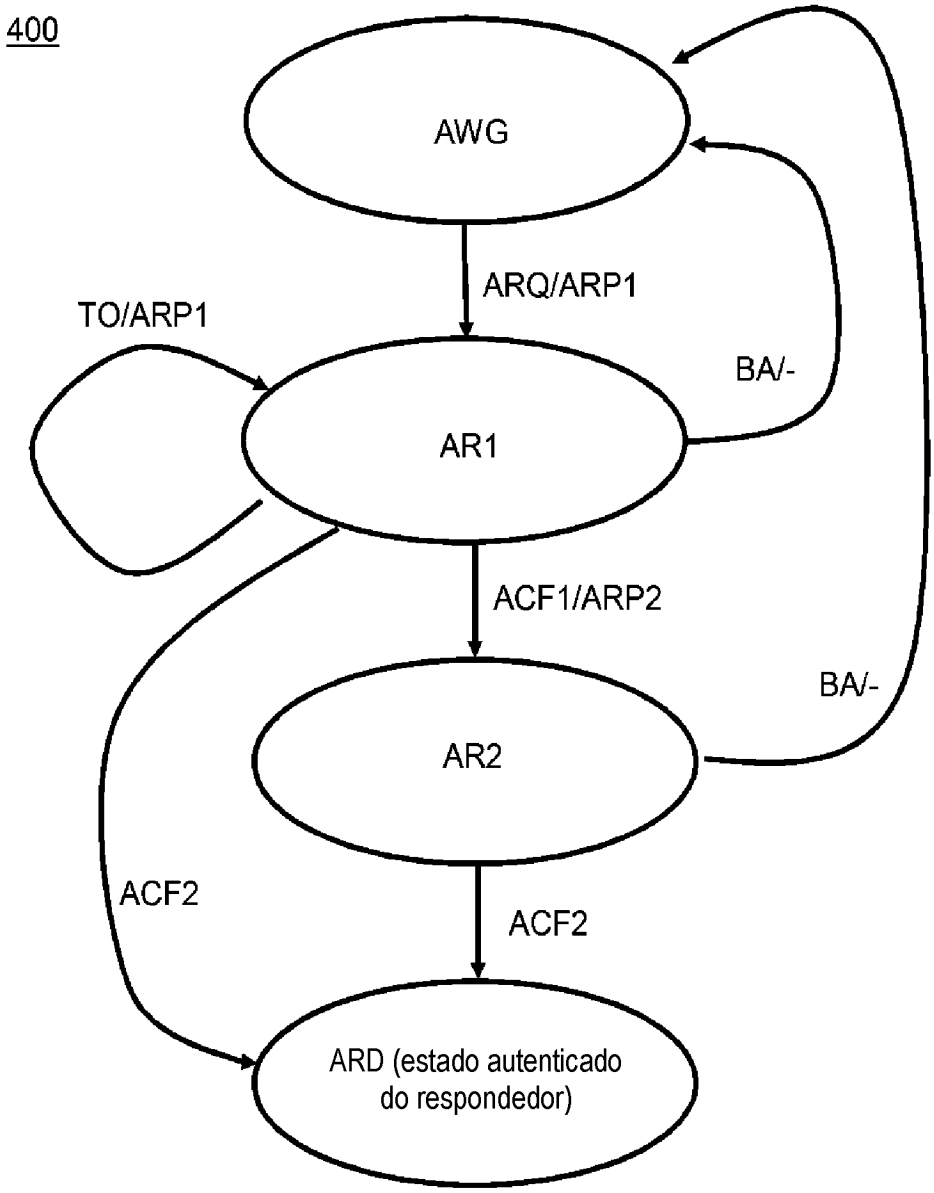

400
AWG
ARQ/ARP1
TO/ARP1
BA/-
AR1
ACF1/ARP2
BA/-
AR2
ACF2
ACF2
ARD (estado autenticado
do respondedor)

Fig. 4

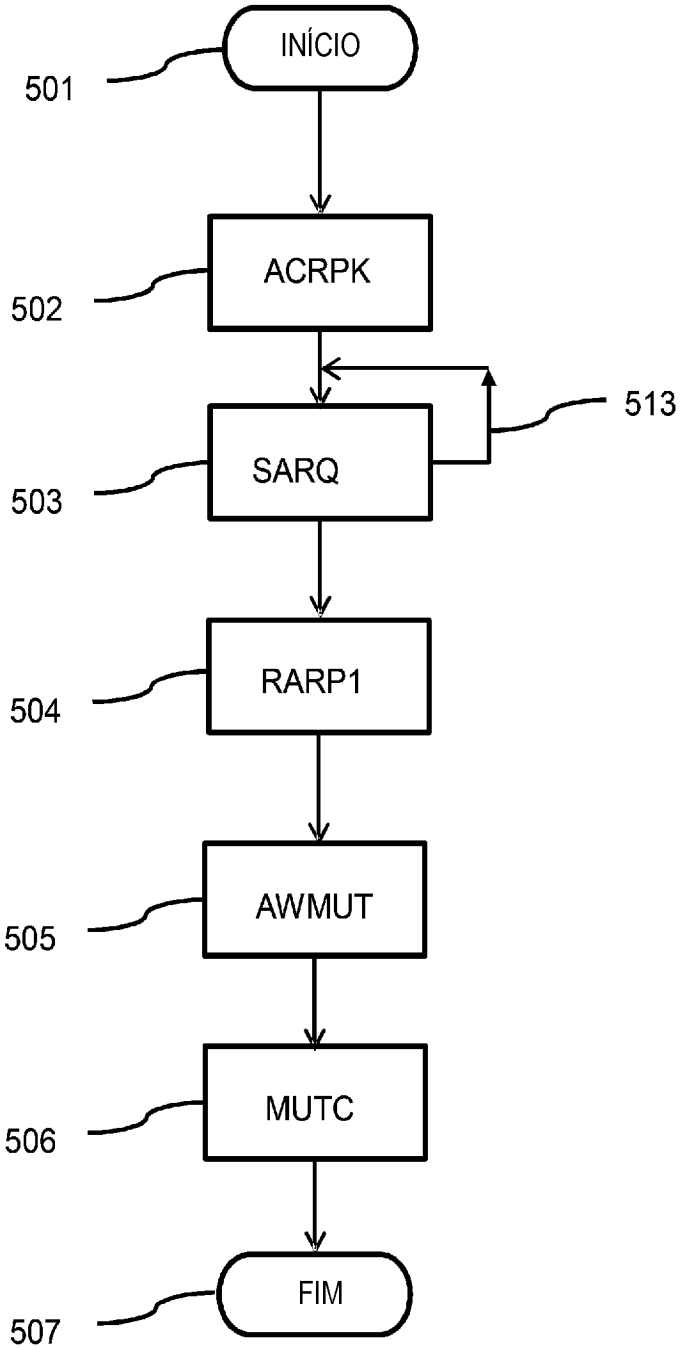

INÍCIO
501
ACRPK
502
SARQ
503
513
RARP1
504
AWMUT
505
MUTC
506
FIM
507

Fig. 5

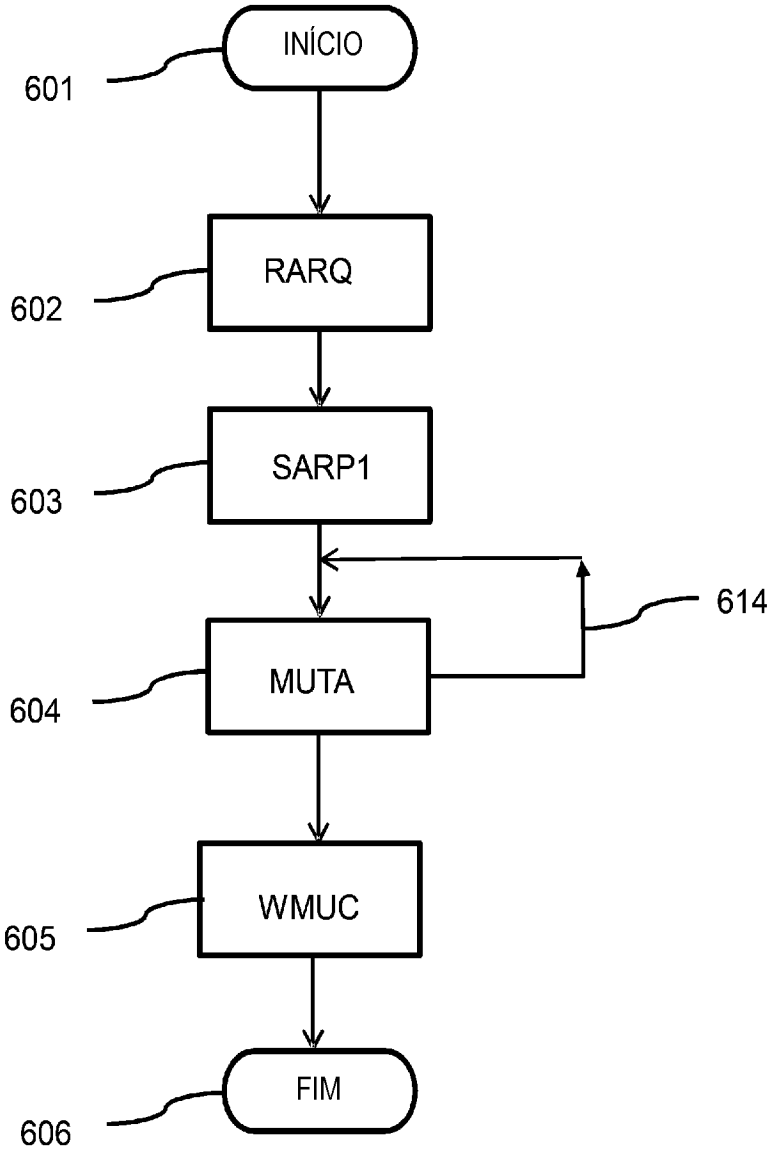


Fig. 6

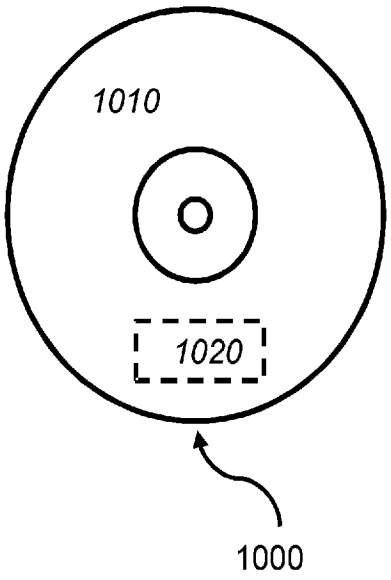


Fig. 7a

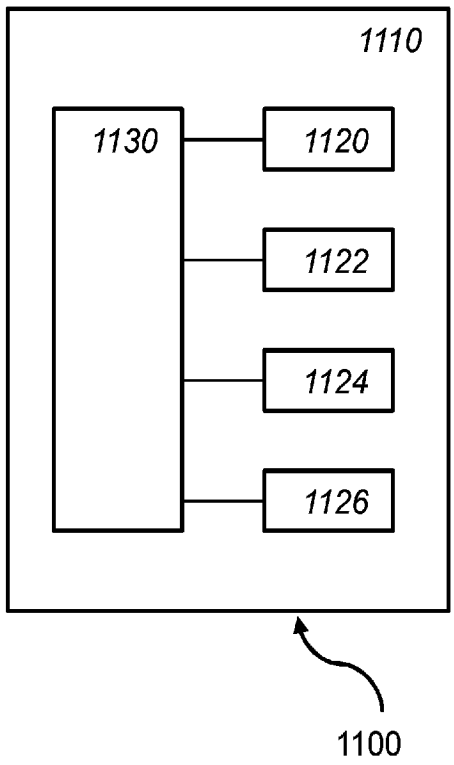


Fig. 7b

RESUMO

DISPOSITIVO INICIADOR, DISPOSITIVO RESPONDEDOR, SISTEMA DE COMUNICAÇÃO SEM FIO, MÉTODO DO INICIADOR PARA USO EM UM DISPOSITIVO INICIADOR PARA COMUNICAÇÃO SEM FIO COM UM DISPOSITIVO RESPONDEDOR, MÉTODO DO RESPONDEDOR PARA USO EM UM DISPOSITIVO RESPONDEDOR PARA COMUNICAÇÃO SEM FIO COM UM DISPOSITIVO INICIADOR DE ACORDO COM UM PROTOCOLO DE COMUNICAÇÃO E PRODUTO DE PROGRAMA DE COMPUTADOR

A presente invenção se refere a um sistema de comunicação sem fio que possibilita a autenticação unilateral de um dispositivo respondedor (210) por um dispositivo iniciador (110) e a autenticação mútua de ambos os dispositivos. As modalidades do iniciador podem ter uma unidade de mensagem (116) e uma máquina de estado (117). O iniciador inicia mediante a aquisição de uma chave pública do respondedor através de uma ação fora da banda e envia um pedido de autenticação. O respondedor envia uma resposta de autenticação compreendendo os dados de autenticação do respondedor com base em uma chave privada do respondedor e um estado de andamento mútuo indicativo de que a autenticação mútua está em andamento, para possibilitar que o dispositivo respondedor adquira a chave pública do iniciador através de uma ação fora da banda do respondedor. A máquina de estado do iniciador é disposta de modo a fornecer um estado de autenticação mútua, acionado mediante o recebimento do estado de andamento mútuo, para esperar autenticação mútua. Assim, evita-se períodos longos de interrupção durante a comunicação sem fio, além de possibilitar que o iniciador relate erros de comunicação ao usuário dentro de um curto período de tempo.