



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

(21) **PI0610430-4 A2**



(22) Data de Depósito: 10/04/2006
(43) Data da Publicação: 22/06/2010
(RPI 2059)

(51) *Int.Cl.:*
H04L 29/06

(54) Título: **MÉTODOS E APARELHOS PARA INTRODUIZIR DISPOSITIVOS COM INTERFACES DE USUÁRIO SIMPLES EM UMA COMUNIDADE DE REDE SEGURA**

(30) Prioridade Unionista: 02/05/2005 EP 05300348.9

(73) Titular(es): THOMSON LICENSING

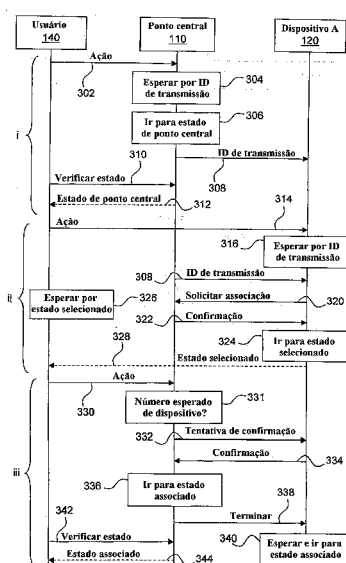
(72) Inventor(es): OLIVIER COURTAY

(74) Procurador(es): Nellie Anne Daniel Shores

(86) Pedido Internacional: PCT EP2006061483 de 10/04/2006

(87) Publicação Internacional: WO 2006/117277 de 09/11/2006

(57) **Resumo:** Um método para introduzir dispositivos (110, 120, 130) com interfaces de usuário simples (115, 125, 135) em uma comunidade de rede (100). Um usuário (140) aperta um botão (116) em um primeiro dispositivo (110) que escuta as mensagens a partir de pontos centrais por dois segundos e, se nenhuma mensagem for recebida, se torna um ponto central e começa a enviar mensagens de ID de transmissão (308). O usuário aperta um botão em um segundo dispositivo (120) para ser inserido, o qual após interação com o ponto central entra em um estado selecionado (403). Percebendo isso na interface de usuário do segundo dispositivo, o usuário aperta o botão no primeiro dispositivo outra vez e após comunicação adicional entre os dispositivos, eles entram em um estado associado (404), o qual pode ser verificado na interface de usuário do primeiro dispositivo. Também são providos um ponto central, um aparelho e um método para configurar um aparelho na rede.



"MÉTODOS E APARELHOS PARA INTRODUIR DISPOSITIVOS
COM INTERFACES DE USUÁRIO SIMPLES EM UMA COMUNIDADE DE REDE
SEGURA"

CAMPO DA INVENÇÃO

5 A presente invenção se refere geralmente às redes seguras, e especificamente à inserção em uma comunidade segura de um ou mais dispositivos com uma interface de usuário simples.

ANTECEDENTES DA INVENÇÃO

10 Um importante problema de segurança com as redes de computadores é que seres humanos estão envolvidos. Administrar tal rede requer conhecimento específico que um usuário comum raramente tem. Por essa razão, um usuário às voltas com interfaces de usuário complicadas freqüentemente opta pelo nível mais baixo de segurança, algumas vezes até mesmo removendo-a completamente. Desse modo pode ser claramente considerado que existe a necessidade de uma forma fácil para facilitar a tarefa do usuário, tanto quanto possível, enquanto mantendo a segurança em um nível aceitável.

20 O Pedido de Patente Europeu EP 1411674 A1 apresenta uma solução onde um ponto central, no simples clique de um botão, limita a cobertura das ondas de rádio que ele transmite. Então o usuário ativa uma função em um dispositivo dentro da área de cobertura reduzida para inserir o mesmo
25 na rede do ponto central. Uma desvantagem com essa solução é que ela é mais propriamente vulnerável aos vários tipos de ataques, tal como, por exemplo, o conhecido ataque de intermediário.

A presente invenção tenta remediar pelo menos algumas das preocupações de segurança relacionadas à técnica anterior, enquanto permitindo que um usuário crie uma comunidade segura de dispositivos que podem ser equipados com interfaces de usuário muito simples.

SUMÁRIO DA INVENÇÃO

Em um primeiro aspecto, a invenção se refere a um método de introduzir pelo menos um dispositivo em uma rede segura que compreende um ponto central instruído para inserir o pelo menos um dispositivo na rede segura. O método é adequado para ser realizado quando o pelo menos um dispositivo e o ponto central não têm conhecimento prévio um do outro. Um usuário instrui o pelo menos um dispositivo a solicitar a inserção na rede segura a partir do ponto central. O pelo menos um dispositivo solicita a partir do ponto central inserção na rede segura, em consequência do que o ponto central verifica se um número esperado de dispositivos solicitou a inserção na rede segura antes de inserir o pelo menos um dispositivo na rede segura.

Em uma modalidade preferida, o ponto central foi instruído pelo usuário a inserir o pelo menos um dispositivo na rede segura.

É vantajoso que a instrução para inserir pelo menos um dispositivo na rede segura compreenda o número de dispositivos a serem inseridos.

Também é vantajoso que a instrução para inserir pelo menos um dispositivo na rede segura tenha sido dada a um dispositivo que mediante essa instrução começou a atuar

como um ponto central. O dispositivo instruído preferivelmente garante que não haja ponto central na rede antes dele começar a atuar como tal. Ele faz isso mediante ação de esperar um tempo predeterminado para uma mensagem a partir do ponto central na rede e decide que não existe ponto central ativo na rede se nenhuma mensagem for recebida durante o tempo predeterminado.

Em outra modalidade preferida, antes da etapa de verificação, o usuário instrui o ponto central a prosseguir com a inserção.

Em uma modalidade preferida adicional, o usuário fornece instruções por intermédio de uma interface de usuário simples.

Em um segundo aspecto, a invenção se refere a um ponto central adaptado para introduzir pelo menos um dispositivo em uma rede segura. O ponto central foi instruído a inserir pelo menos um dispositivo na rede segura, mas não necessariamente tem conhecimento anterior do pelo menos um dispositivo.

Em um terceiro aspecto, a invenção se refere a um aparelho em uma rede segura. O dispositivo é adaptado para, mediante instrução por um usuário, atuar como um ponto central adaptado para inserir pelo menos um dispositivo na rede segura, sem conhecimento prévio do pelo menos um dispositivo, se a rede segura compreende nenhum ponto central ativo e a atuar como um dispositivo se a rede segura compreende um ponto central ativo.

Em um quarto aspecto, o dispositivo se refere a um

método de configurar um aparelho em uma rede segura. Na recepção de uma instrução a partir de um usuário, o dispositivo verifica se há um ponto central na rede segura; e se esse não for o caso, ele começa agir como um ponto central adaptado para inserir pelo menos um dispositivo na rede segura, sem conhecimento prévio do pelo menos um dispositivo.

Em um quinto aspecto, a invenção se refere a um sistema para introduzir pelo menos um dispositivo em uma rede segura compreendendo um ponto central instruído para inserir o pelo menos um dispositivo na rede segura. O pelo menos um dispositivo e o ponto central não precisam ter qualquer conhecimento prévio um do outro. O pelo menos um dispositivo é adaptado para receber uma instrução a partir de um usuário para solicitar a partir do ponto central inserção na rede segura; e para solicitar a partir do ponto central inserção na rede segura. O ponto central é adaptado para inserir o pelo menos um dispositivo na rede segura após ter verificado que um número esperado de dispositivos solicitou a inserção na rede segura.

Em um sexto aspecto, a invenção se refere a um método de introduzir por intermédio de um ponto central um número determinado de dispositivos em uma rede segura. O ponto central é instruído a introduzir um número determinado de dispositivos na rede segura, o ponto central não necessariamente tendo qualquer conhecimento prévio do número determinado de dispositivos. O ponto central recebe uma solicitação para inserção na rede segura a partir de pelo menos um dispositivo, verifica se o número determinado de dispositivos

solicitou inserção na rede segura, e insere o número determinado de dispositivos na rede segura.

O ponto central compreende uma unidade de comunicação adaptada para se comunicar com o pelo menos um dispositivo, e para receber a partir do pelo menos um dispositivo uma solicitação para inserção na rede segura; um processador adaptado para se comunicar com a unidade de comunicação e para inserir o pelo menos um dispositivo na rede segura, e para verificar se um número esperado de dispositivos solicitou inserção na rede segura antes de inserir o pelo menos um dispositivo na rede.

Em uma modalidade preferida, o ponto central é adaptado para receber uma instrução a partir de um usuário para inserir o pelo menos um dispositivo na rede segura.

É vantajoso que a instrução para inserir o pelo menos um dispositivo na rede segura compreenda informação sobre o número de dispositivos a serem inseridos.

Também é vantajoso que o ponto central seja adaptado como um dispositivo antes do recebimento da instrução para inserir o pelo menos um dispositivo na rede segura. É preferível que o processador seja adaptado adicionalmente para garantir que não haja ponto central ativo na rede. Isso é conseguido mediante ação de esperar um tempo predeterminado por uma mensagem a partir de um ponto central na rede e decidir se não existe ponto central ativo na rede se nenhuma mensagem for recebida pela unidade de comunicação durante o tempo predeterminado.

Em outra modalidade preferida, o ponto central

compreende uma interface de usuário adaptada para receber instruções a partir do usuário para prosseguir com a inserção.

É vantajoso que o ponto central compreenda uma interface de usuário adaptada para receber a instrução para inserir o pelo menos um dispositivo na rede.

É vantajoso que a interface de usuário compreenda um botão adaptado para receber as instruções. Também é vantajoso que a interface de usuário compreenda um LED adaptado para sinalizar para o usuário um estado do ponto central.

DESCRIÇÃO RESUMIDA DOS DESENHOS

Características preferidas da presente invenção serão descritas agora, como exemplo, com referência aos desenhos anexos, nos quais:

A Figura 1 ilustra uma comunidade exemplar na qual a invenção é usada;

A Figura 2 ilustra uma interface de usuário, simples, exemplar para uso com a invenção; e

A Figura 3 ilustra um fluxograma do método para inserção de dispositivo de acordo com a invenção; e

A Figura 4 ilustra um diagrama de estado para dois dispositivos, correspondendo a um método ilustrado na Figura 3.

DESCRIÇÃO DETALHADA DE MODALIDADES PREFERIDAS

A Figura 1 ilustra uma comunidade exemplar 100 na qual a invenção é usada. A comunidade 100 compreende um ponto central 110 e um dispositivo B 130. Deve ser observado que em uma modalidade preferida, o ponto central é um dispo-

sitivo atuando como um ponto central durante a inserção somente, após o que ele pára de atuar como um ponto central. O usuário (não mostrado) está para introduzir o dispositivo A 120 na comunidade 100. O ponto central 110, dispositivo A 120 e dispositivo B 130 (todos os quais podem conjuntamente ser referidos como "dispositivo") têm todos, uma interface de usuário 115, 125, 135, respectivamente. A interface de usuário é preferivelmente uma interface de usuário simples que compreende um botão e pelo menos um LED, como descrito adicionalmente na Figura 2.

O ponto central 110 compreende uma unidade de comunicação 119, ilustrada por uma antena, para interação com outros dispositivos. A unidade de comunicação utiliza preferivelmente tecnologia de rádio para comunicação, porém outros meios de comunicação; como, por exemplo, luz infravermelha; também podem ser usados. Além disso, o ponto central 110 compreende uma memória (não mostrada) e um processador 115 para cálculo, verificação, e para controlar o ponto central.

A Figura 2 ilustra uma interface de usuário simples, exemplar para uso com a invenção. A figura mostra a interface de usuário 115 do ponto central 110 e a interface de usuário 125 do dispositivo A 120 durante a inserção do dispositivo A 120 na comunidade 100, após o método descrito na Figura 3. Será suposto para facilitar a ilustração que as duas interfaces de usuário são idênticas. Cada interface de usuário 115, 125 compreende um botão 116, 126 e dois LEDs 117, 118 e 127, 128, respectivamente. O botão 116, 126 pode

ser um botão real, mas ele também pode ser emulado, por exemplo, em uma tela, ou ser ativado por voz; qualquer que seja a sua implementação, ele faz com que uma função específica seja executada quando ativado. As palavras "botão de
5 apertar" devem ser interpretadas como "realizar a ação" que é necessária para causar a execução da função. Como será descrito adicionalmente em seguida, o primeiro LED 117, 127 indica o estado do dispositivo, enquanto que o segundo LED 118, 128 é adaptado para indicar quaisquer erros. Antes do
10 início do método, ambos os LEDs 117, 127 e 118, 128 de ambos os dispositivos 110 e 120, são inativos, o que é indicado pelo número de referência 110.

O método para inserção de um dispositivo em uma comunidade será descrito agora com referência à Figura 2
15 (interfaces de usuário), Figura 3 (fluxograma do método), e Figura 4 (diagrama de estado). Deve ser observado que, ao contrário do exemplo na Figura 1, o Ponto Central 110 é um dispositivo "normal" sem quaisquer conexões com outros dispositivos quando o método começa e que se torna um ponto
20 central durante a execução do método.

Há três partes gerais do processo:

i.A parte de preferência (302-312 na Figura 3): durante essa parte, o ponto central é selecionado.

ii.A parte "alô" (314-326 na Figura 3): a comunicação entre o ponto central e pelo menos um dispositivo a
25 ser inserido é iniciada durante essa parte. Essa parte é repetida para cada dispositivo a ser inserido.

iii.A parte de "verificação" (330-344 na Figura

3): a pelo menos uma associação é confirmada durante essa parte.

O método será descrito em detalhe. O método começa quando o usuário 140 aperta o botão 116 do Ponto Central 110, etapa 302 "Ação" (indicada pela seta 205 na Figura 2). O Ponto Central 110 primeiramente espera um tempo predeterminado, preferivelmente dois segundos, por uma mensagem de ID de Transmissão, etapa 304. Cada ponto central transmite tal mensagem a cada dois segundos, de modo que se o Ponto Central 110 não recebe uma mensagem de ID de Transmissão dentro desse tempo, então não há ponto central (ativo) em suas proximidades. Naturalmente, se os pontos centrais transmitem essas mensagens com outro intervalo do que a cada dois segundos, o tempo predeterminado deve ser conformemente ajustado. Por outro lado, se o Ponto Central 110 recebe uma mensagem de ID de Transmissão, então ele deve ser inserido como um dispositivo normal na comunidade do ponto central que transmite a mensagem, isto é, ele assume o lugar do dispositivo A (e a etapa 302 é na realidade a etapa 314, como será descrito adicionalmente em seguida com referência àquele dispositivo).

Em outras palavras, durante a etapa 304 o dispositivo descobre se ele está ou não na presença de um ponto central. Se esse for o caso, ele atua como um dispositivo simples; se esse não for o caso, ele assume a função do ponto central. Esse arranjo garante que não haja mais do que um único ponto central ativo na rede em um determinado momento.

Após a espera predeterminada, o Ponto Central 110

segue a partir do Estado Inicial (401 na Figura 4) para o Estado de Ponto Central (402 na Figura 4) - indicado por um lento piscar do primeiro LED 117 (faixas diagonais; 220 na Figura 2) - e se torna um ponto central real, etapa 306.

5 Sendo um ponto central, ele começa a transmitir as mensagens de ID de Transmissão 308. As mensagens de Transmissão 308 são ignoradas pelo dispositivo A que nesse ponto está no Estado Inicial 401.

10 O usuário 140 então verifica a interface de usuário 115 do Ponto Central 110, etapa 310, e percebe que ela, corretamente, indica que o Ponto Central 110 está no Estado de Ponto Central 402, etapa 312.

Quando o usuário 140 está satisfeito no sentido de que o Ponto Central 110 está no estado correto, ele vai para 15 o dispositivo A 120, o qual está no Estado Inicial 401, e aperta o botão, etapa 314 (230 na Figura 2).

Quando desse modo ativado, o dispositivo A 120 espera por um tempo predeterminado por uma mensagem de ID de transmissão 308 a partir de um ponto central, etapa 316. 20 Nesse caso, como o usuário 140 fez com que o Ponto Central 110 fosse para o Estado de Ponto Central 402, a mensagem de ID de Transmissão 308 é transmitida e recebida antes do fim do tempo predeterminado.

O dispositivo A 120 então envia uma mensagem de 25 Associação de Solicitação 320 para indicar que ele pretende entrar na comunidade do Ponto Central 110, o qual no recebimento dessa mensagem responde com uma mensagem de Confirmação 322. Quando o dispositivo A 120 recebe a confirmação

322, ele vai para o Estado Seleccionado 403, etapa 324, que é indicado na interface de usuário 125 por um rápido piscar do primeiro LED 117 (328, ilustrado pelas faixas verticais na Figura 2, 240).

5 O usuário 140 que esteve esperando (etapa 326) por essa indicação, agora retorna para o Ponto Central 110 e aperta outra vez o botão 116, etapa 330 (250 na Figura 2). Após ter verificado (etapa 331) que ele recebeu solicitações a partir do número esperado de dispositivos e enviou confir-
10 mações para o número esperado de dispositivos - nesse caso, um - o Ponto Central 110 então envia uma mensagem de tentativa de confirmação 332 para o dispositivo A 120, que responde com uma Confirmação 334. O Ponto Central 110 então vai para o Estado Associado 404 e envia uma mensagem Terminar
15 338 para o dispositivo A 120 para indicar que a associação foi corretamente realizada e que o dispositivo A 120 foi inserido adequadamente na comunidade 100.

 O dispositivo A 120 recebe a mensagem Terminar 338, espera um tempo predeterminado (descrito adicionalmente
20 em seguida) e vai, etapa 340, para o Estado Associado 404. Na Figura 2, número de referência 260 ilustra que tanto o Ponto Central 110 como o dispositivo A 120 indicam por intermédio de suas interfaces de usuário 115, 125 que eles estão no Estado Associado 404 por intermédio de uma luz verde
25 contínua do primeiro LED 117. O usuário 140 verifica o estado do Ponto Central 110, etapa 342, e seu conteúdo para verificar se a inserção do dispositivo A 120 na comunidade 100 do Ponto Central 110 foi bem-sucedida, como indicado (344)

pela interface de usuário.

Embora o método como descrito anteriormente illustre a introdução de um dispositivo em uma comunidade, a invenção também provê a possibilidade de introduzir um número de dispositivos. Não considerando o uso do método como descrito para introduzir um dispositivo de cada vez, também é possível tornar esse processo mais fácil. Deve ser observado que a descrição em seguida pode deixar de fora partes que já foram explicadas anteriormente.

Suponha que o usuário 140 deseje introduzir N dispositivos, 120 e 130, na comunidade 100 do Ponto Central 110, o que como já foi explicado pode ser um dispositivo comum quando o método começa. Para N dispositivos, se pode dizer que o método compreende uma parte de preferência (ligeiramente diferente daquela descrita anteriormente), N partes de alô, e uma parte de verificação. Deve ser observado que se houver um ponto central ativo na comunidade, a parte de escolha já foi realizada e não precisa ser executada outra vez.

O usuário 140 começa seguindo para o Ponto Central (futuro) 110 e apertando o botão 116 N vezes, preferivelmente com menos de dois segundos entre cada ação de apertar. Após a última ação de apertar o botão 116, o Ponto Central 110 espera por uma mensagem de ID de Transmissão durante dois segundos e, se nenhuma tal mensagem for recebida, segue para o Estado de Ponto Central.

O usuário 140 utiliza a interface de usuário 115 para verificar se o Ponto Central 110 atingiu adequadamente

o Estado de Ponto Central. Para cada um dos N dispositivos de cada vez, o usuário então aperta o botão e verifica se o dispositivo entra no Estado Seleccionado. O usuário retorna ao Ponto Central, aperta outra vez o botão, e verifica se o

5 Ponto Central vai para o Estado Associado.

O usuário então introduziu de forma bem-sucedida os N dispositivos na comunidade do Ponto Central.

O Ponto Central 110 conta o número de dispositivos que ele supostamente deve introduzir em sua comunidade, etapa 331, de modo que ele é capaz de verificar se o número de

10 dispositivos introduzidos está correto.

Se houver muitos dispositivos, isso pode significar que um hacker tentou introduzir um ou mais dispositivos na comunidade, e o ponto central vai para o Estado de Erro

15 405 e rejeita cada dispositivo introduzido durante a sessão de introdução atual.

Por outro lado, se houver muito poucos dispositivos, isso pode significar que o usuário se esqueceu de um ou mais dispositivos ou que um dispositivo se comunicou com o

20 ponto central errado. Também nesse caso, o Ponto Central vai para o Estado de Erro 405 e rejeita cada dispositivo introduzido durante a sessão de introdução atual.

Se um dispositivo detecta um problema de segurança, tal como se ele detecta um pacote com o identificador do

25 dispositivo, enviado por outro dispositivo ou se um segundo ponto central foi detectado, ele envia uma mensagem Falhou para o seu Ponto Central. O Ponto Central envia ou encaminha, conforme apropriado, mensagens Falhou para todos os

dispositivos que estão para ser introduzidos no processo atual de introdução. Na recepção ou envio, conforme apropriado, de uma mensagem Falhou, os dispositivos vão para o Estágio de Erro 405, indicado preferivelmente por uma luz vermelha no segundo LED 118, 128.

Há várias formas possíveis para um dispositivo sair do estágio de erro, dos quais dois exemplos serão dados. Um primeiro modo é o de esperar um tempo predeterminado, tal como um minuto e, então, ir para o Estágio Inicial 401. Um segundo modo é o do dispositivo permanecer no Estágio de Erro 405 até que o usuário aperte o botão 116, 126 e somente então seguir para o Estado Inicial 401.

Para que os dispositivos habilitem a autenticação mútua, segura, subsequente, a invenção propõe o seguinte esquema de mensagem, preferido:

Tabela 1: formato e conteúdo da mensagem

	Cabeçalho	Informação de Remetente	Informação de Destino
ID de Transmissão	000	X	-
Solicitar associação	001	Y	X
Confirmação	010	X	Y
Tentativa de confirmação	011	X	-
Confirmação	100	Y	X
Terminar	101	X	-
Falhou	110	X ou Y	-

O cabeçalho distingue o tipo da mensagem. X repre-

senta a identidade provável da chave pública do Ponto Central, tal como um hash de 160 bits da chave pública. Y representa a provável identidade da chave pública do dispositivo, tal como um hash de 160 bits da chave pública.

5 Uma modalidade alternativa utiliza um ponto central dedicado, e dispositivos dedicados. Nesse caso, o método e a interface dos dispositivos podem ser simplificados. Como o ponto central é sempre um ponto central, normalmente não há a necessidade da primeira parte do método, 302-312, 10 onde o dispositivo de outro modo descobriria se deveria agir como um ponto central ou um dispositivo "normal", embora o usuário pudesse ainda verificar se o ponto central estaria no Estado de Ponto Central e não no Estado de Erro. Adicionalmente, o botão e o segundo LED podem ser removidos dos 15 dispositivos, uma vez que uma reinicialização ou ativação de um dispositivo poderia ativar a ação 314 e quaisquer erros podem ser vistos no ponto central.

A invenção, como parcialmente mencionada anteriormente, é resistente aos ataques de hackers. Se um hacker 20 tentar introduzir um dispositivo falso, o ponto central perceberá que o número de dispositivos é incorreto e envia mensagens Falhou. Se um hacker tentar utilizar um ponto central falso para associação com um dispositivo, o dispositivo perceberá que ele recebe as mensagens de ID de Transmissão a 25 partir de dois pontos centrais diferentes e envia uma mensagem Falhou. Mesmo se o ponto central falso reproduzir as mensagens ID de Transmissão a partir do ponto central real, o dispositivo percebe que ele recebe mensagem de ID de

Transmissão a partir de mais do que um ponto central uma vez que as mensagens chegam duas vezes mais freqüentemente do que o esperado. Para neutralizar as mensagens Terminar falsas, o dispositivo espera um tempo predeterminado após recepção de tal mensagem antes de ir para o Estado Associado. Isso proporciona ao Ponto Central tempo para receber a mensagem falsa, perceber que a mensagem é falsa, e enviar uma mensagem Falhou para o dispositivo que ainda não está no Estado Associado.

10 Será considerado que o método é adequado para uso também quando dois dispositivos, um atuando como um ponto central e o outro atuando como um dispositivo, a ser inserido, não tem conhecimento prévio um do outro.

15 Deve ser observado que onde, na descrição e nas reivindicações, é dito que um dispositivo é parte da rede segura embora logicamente ele não seja parte da mesma uma vez que ele está para ser inserido na mesma, as palavras "parte da rede" devem ser interpretadas como "sendo capazes de se comunicar com a rede segura e deduzir se há um ponto
20 central ativo na mesma".

 Desse modo pode ser considerado que a presente invenção é um aperfeiçoamento em relação à técnica anterior mediante provisão de uma forma segura de introduzir dispositivos com interfaces de usuário principalmente simples em
25 uma comunidade.

 Será entendido que a presente invenção foi descrita apenas como exemplo, e modificações de detalhe podem ser feitas sem se afastar do escopo da invenção.

Cada característica revelada na descrição; e (onde apropriado) nas reivindicações e desenhos; pode ser provida independentemente ou em qualquer combinação apropriada. As características podem ser, quando apropriado, implementadas em hardware, software ou uma combinação dos dois. As conexões podem, se aplicável, ser implementadas como conexões sem fio ou cabeadas, não necessariamente conexões diretas ou dedicadas.

Numerais de referência aparecendo nas reivindicações têm apenas a finalidade de ilustração e não devem ter efeito limitador em relação ao escopo das reivindicações.

REIVINDICAÇÕES

1. Método de introduzir pelo menos um dispositivo (120) em uma rede segura (100) compreendendo um ponto central (110) instruído para inserir o pelo menos um dispositivo na rede segura, o método sendo adequado para ser realizado quando o pelo menos um dispositivo (120) e o ponto central (110) não tem conhecimento prévio um do outro, compreendendo as etapas de:

instruir (314) por um usuário (140) o pelo menos um dispositivo para solicitar a partir do ponto central inserção na rede segura;

solicitar (320) por intermédio do pelo menos um dispositivo a partir do ponto central, inserção na rede segura;

inserir (338) por intermédio do ponto central o pelo menos um dispositivo na rede segura;

CARACTERIZADO pelas etapas, antes da etapa de inserção, de:

verificar (331) por intermédio do ponto central se um número esperado de dispositivos solicitou inserção na rede segura.

2. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que o ponto central foi instruído (302) pelo usuário a inserir o pelo menos um dispositivo na rede segura.

3. Método, de acordo com a reivindicação 2, **CARACTERIZADO** pelo fato de que a instrução para inserir pelo menos um dispositivo na rede segura compreende o número de

dispositivos a serem inseridos.

4. Método, de acordo com a reivindicação 2, **CARACTERIZADO** pelo fato de que a instrução (302) para inserir pelo menos um dispositivo na rede segura foi dada a um dispositivo que em decorrência dessa instrução começou a atuar como um ponto central.

5. Método, de acordo com a reivindicação 4, **CARACTERIZADO** por compreender ainda a etapa de garantir (304) por intermédio do dispositivo que não há ponto central ativo na rede antes dele começar a agir como um ponto central.

6. Método, de acordo com a reivindicação 5, **CARACTERIZADO** pelo fato de que a etapa de garantir compreende esperar um tempo predeterminado por uma mensagem a partir de um ponto central na rede e decidir se não existe ponto central ativo na rede se nenhuma mensagem for recebida durante o tempo predeterminado.

7. Método, de acordo com a reivindicação 1, **CARACTERIZADO** por compreender ainda a etapa de, antes da etapa de verificação (331), instruir (330) por intermédio do usuário o ponto central a prosseguir com a inserção.

8. Método, de acordo com as reivindicações 1 a 7, **CARACTERIZADO** pelo fato de que o usuário fornece instruções por intermédio de uma interface de usuário simples.

9. Ponto central (110) adaptado para introduzir pelo menos um dispositivo (120) em uma rede segura (100), o ponto central sendo instruído para inserir pelo menos um dispositivo na rede segura, em que o ponto central não ne-

cessariamente tem qualquer conhecimento prévio do pelo menos um dispositivo, o ponto central compreendendo:

uma unidade de comunicação (119) adaptada para se comunicar com pelo menos um dispositivo, e para receber a
5 partir do pelo menos um dispositivo uma solicitação (320) para inserção na rede segura;

um processador (114) adaptado para se comunicar com a unidade de comunicação e a inserir pelo menos um dispositivo na rede segura; e

10 **CARACTERIZADO** pelo fato de que o processador (114) é adaptado adicionalmente para verificar se um número esperado de dispositivos solicitou inserção na rede segura antes de inserir o pelo menos um dispositivo na rede.

10. Ponto central, de acordo com a reivindicação
15 9, **CARACTERIZADO** pelo fato de que o ponto central é adaptado para receber uma instrução a partir de um usuário (140) para inserir o pelo menos um dispositivo na rede segura.

11. Ponto central, de acordo com a reivindicação
10, **CARACTERIZADO** pelo fato de que a instrução para inserir
20 o pelo menos um dispositivo na rede segura compreende informação sobre o número de dispositivos a serem inseridos.

12. Ponto central, de acordo com a reivindicação
10, **CARACTERIZADO** pelo fato de que o ponto central é adaptado para atuar como um dispositivo antes do recebimento da
25 instrução para inserir o pelo menos um dispositivo na rede segura.

13. Ponto central, de acordo com a reivindicação
12, **CARACTERIZADO** pelo fato de que o processador é adaptado

adicionalmente para garantir que não haja ponto central ativo na rede.

14. Ponto central, de acordo com a reivindicação 13, **CARACTERIZADO** pelo fato de que o processador é adaptado para esperar um tempo predeterminado por uma mensagem a partir de um ponto central na rede e para decidir se não há ponto central ativo na rede se nenhuma mensagem for recebida pela unidade de comunicação durante o tempo predeterminado.

15. Ponto central, de acordo com a reivindicação 9, **CARACTERIZADO** por compreender ainda uma interface de usuário (115) adaptada para receber instruções a partir do usuário para prosseguir com a inserção.

16. Ponto central, de acordo com a reivindicação 10, **CARACTERIZADO** por compreender ainda uma interface de usuário (115) adaptada para receber a instrução para inserir o pelo menos um dispositivo na rede.

17. Ponto central, de acordo com qualquer uma das reivindicações 15 e 16, **CARACTERIZADO** pelo fato de que a interface de usuário compreende um botão (116) adaptado para receber as instruções.

18. Ponto central, de acordo com qualquer uma das reivindicações 15 e 16, **CARACTERIZADO** pelo fato de que a interface de usuário compreende um LED (118) adaptado para sinalizar para o usuário um estado do ponto central.

19. Aparelho em uma rede segura, o aparelho sendo **CARACTERIZADO** pelo fato de ser adaptado para, mediante instrução por um usuário, atuar como um ponto central adaptado para inserir pelo menos um dispositivo na rede segura, sem

conhecimento prévio do pelo menos um dispositivo, se a rede segura não compreender ponto central ativo e para agir como um dispositivo se a rede segura compreender um ponto central ativo.

5 20. Método de configurar um aparelho, em uma rede segura, o método sendo **CARACTERIZADO** por compreender as etapas de:

no recebimento de uma instrução a partir de um usuário, verificar se existe um ponto central na rede; e

10 se esse não for o caso, começar a agir como um ponto central adaptado para inserir pelo menos um dispositivo na rede segura, sem conhecimento prévio do pelo menos um dispositivo.

21. Sistema para introduzir pelo menos um dispositivo (120) em uma rede segura (100) compreendendo um ponto central (110) instruído para inserir o pelo menos um dispositivo na rede segura, em que o pelo menos um dispositivo (120) e o ponto central (110) não precisam ter qualquer conhecimento prévio um do outro:

20 o pelo menos um dispositivo sendo adaptado para:
receber uma instrução (314) a partir de um usuário (140) para solicitar a partir do ponto central inserção na rede segura; e

solicitar (320) a partir do ponto central inserção
25 na rede segura;

o ponto central sendo adaptado para:
inserir (338) o pelo menos um dispositivo na rede segura;

CARACTERIZADO pelo fato de que o ponto central é adaptado adicionalmente para verificar (331) se um número esperado de dispositivos solicitou inserção na rede segura, antes de inserir o pelo menos um dispositivo na rede segura.

5 22. Método de introduzir por intermédio de um ponto central (110) um número determinado de dispositivos (120) em uma rede segura (100), o ponto central sendo instruído para introduzir um número determinado de dispositivos na rede segura, o ponto central não tendo necessariamente qualquer conhecimento prévio do número determinado de dispositivos, o método sendo **CARACTERIZADO** por compreender as etapas,
10 no ponto central, de:

 receber uma solicitação para inserção na rede segura (320) a partir de pelo menos um dispositivo;

15 verificar (331) se o número determinado de dispositivos solicitou inserção na rede segura; e

 inserir (338) o número determinado de dispositivos na rede segura.

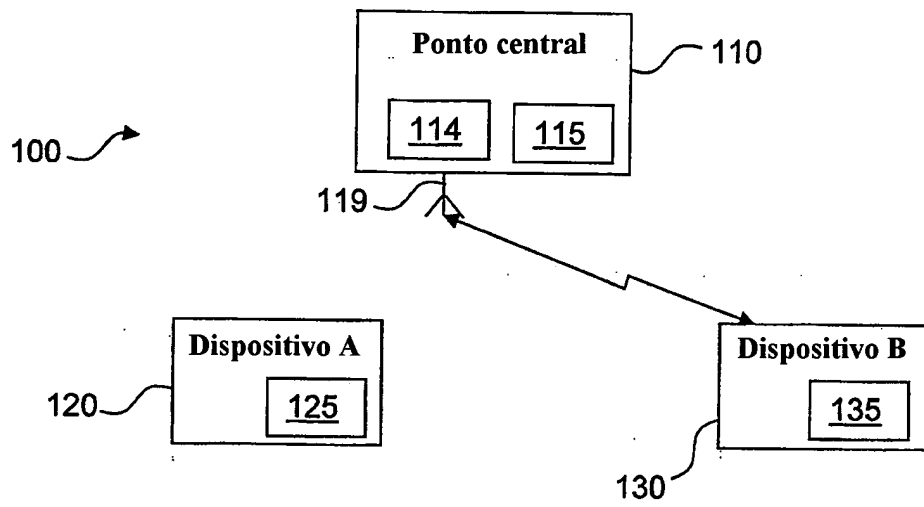


Figura 1

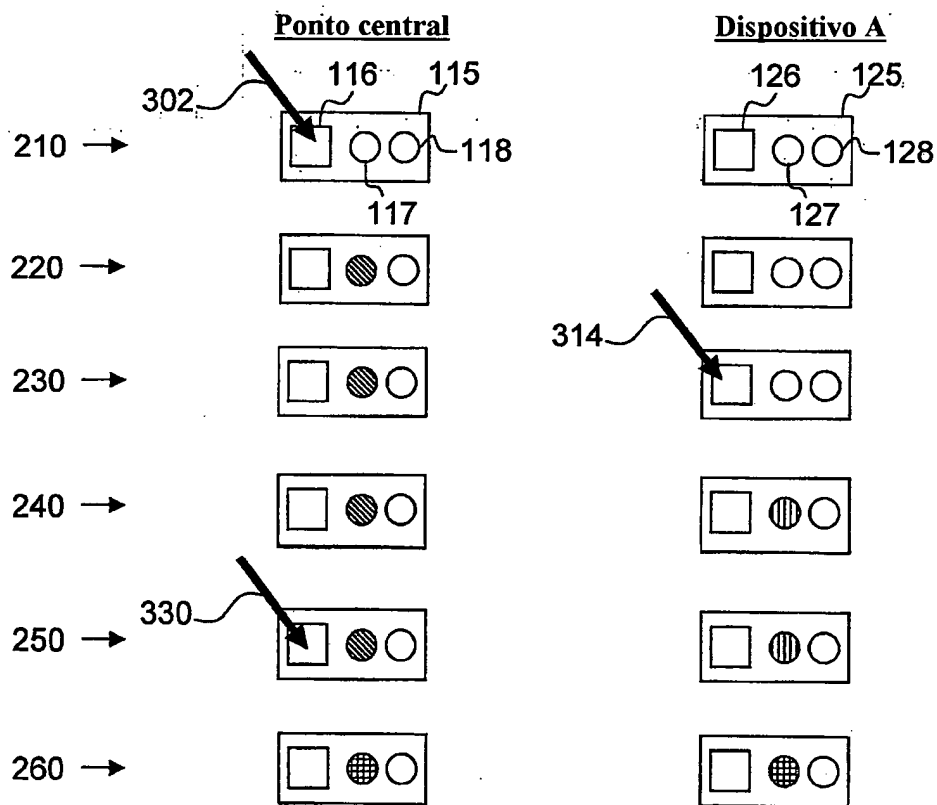


Figura 2

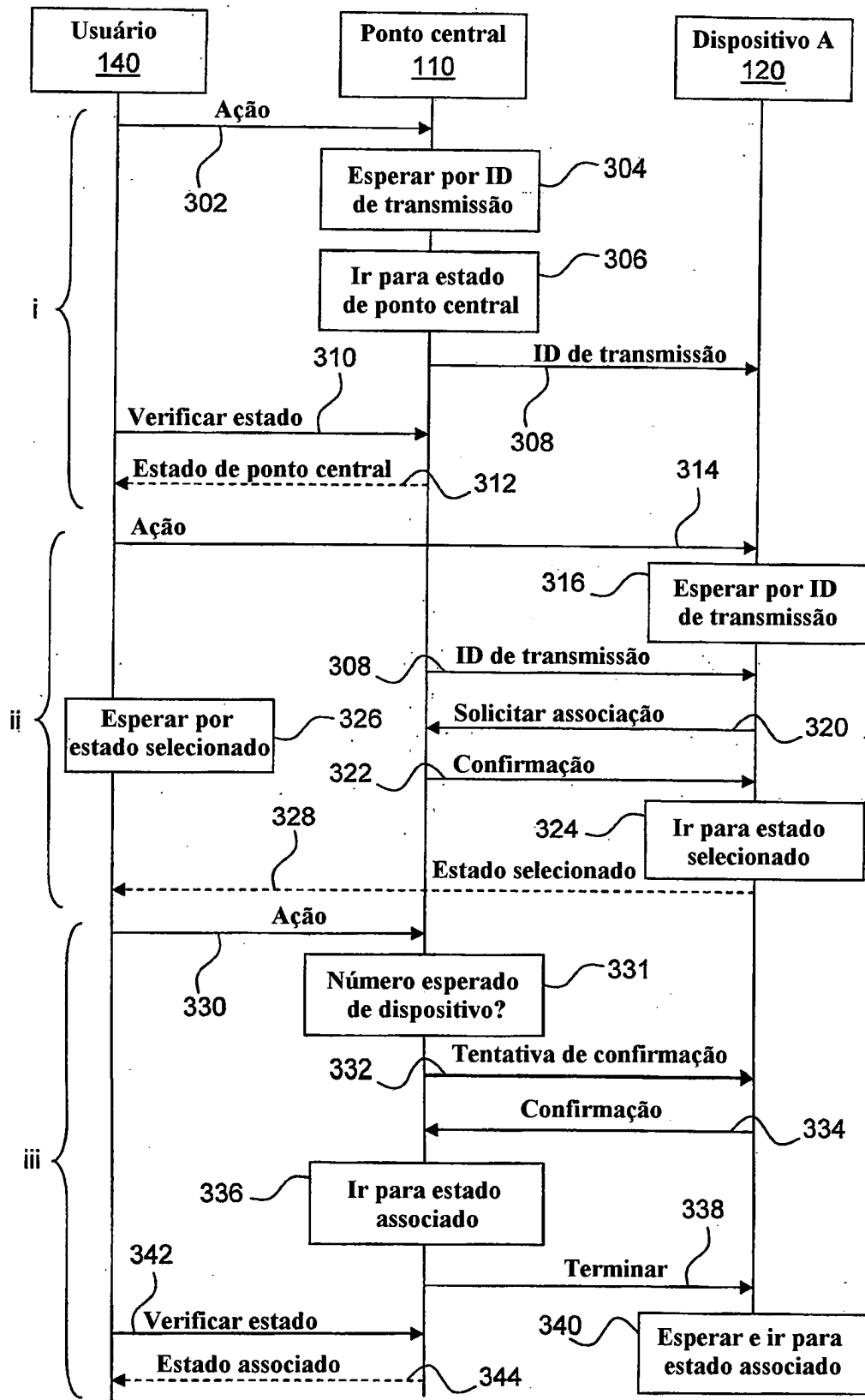


Figura 3

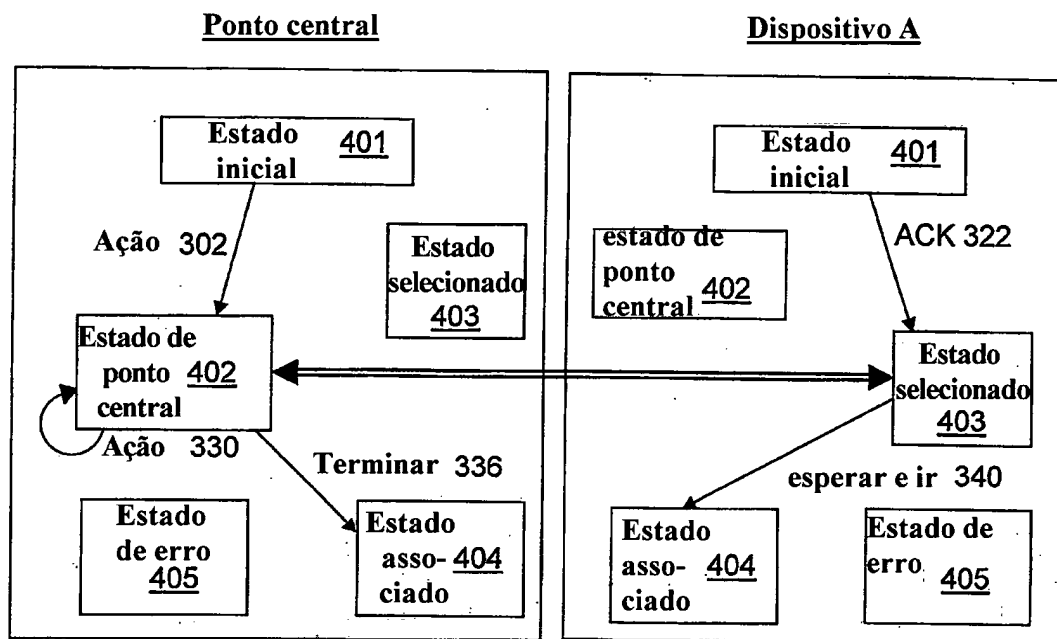


Figura 4

RESUMO

"MÉTODOS E APARELHOS PARA INTRODUIR DISPOSITIVOS COM INTERFACES DE USUÁRIO SIMPLES EM UMA COMUNIDADE DE REDE SEGURA"

5 Um método para introduzir dispositivos (110, 120, 130) com interfaces de usuário simples (115, 125, 135) em uma comunidade de rede (100). Um usuário (140) aperta um botão (116) em um primeiro dispositivo (110) que escuta as mensagens a partir de pontos centrais por dois segundos e,
10 se nenhuma mensagem for recebida, se torna um ponto central e começa a enviar mensagens de ID de transmissão (308). O usuário aperta um botão em um segundo dispositivo (120) para ser inserido, o qual após interação com o ponto central entra em um estado selecionado (403). Percebendo isso na interface de usuário do segundo dispositivo, o usuário aperta
15 o botão no primeiro dispositivo outra vez e após comunicação adicional entre os dispositivos, eles entram em um estado associado (404), o qual pode ser verificado na interface de usuário do primeiro dispositivo. Também são providos um ponto central, um aparelho e um método para configurar um aparelho na rede.
20

PÁGINAS MODIFICADAS
(SUGERIDAS PELA REQUERENTE)

REIVINDICAÇÕES

1. Método de introduzir por intermédio de um primeiro dispositivo (110) um número determinado de dispositivos adicionais (120, 130) em uma rede segura (100), o método
5 compreendendo as etapas, no primeiro dispositivo, de:

receber (320) uma solicitação para inserção na rede segura a partir de cada um de um número de dispositivos adicionais; e

inserir (338) o número determinado de dispositivos
10 adicionais na rede segura, **CARACTERIZADO** por:

antes da etapa de receber uma solicitação, a etapa de receber (302) uma instrução para introduzir um número determinado de dispositivos adicionais na rede segura; e

antes da etapa de inserção, a etapa de verificar
15 (331) se o número de solicitações recebidas é igual ao número determinado de dispositivos adicionais.

2. Método, de acordo com a reivindicação 1, **CARACTERIZADO** por compreender adicionalmente a etapa, antes da etapa de verificação (331), de receber (330) por intermédio do primeiro dispositivo uma instrução para prosseguir com a inserção do número determinado de dispositivos adicionais.
20

3. Método, de acordo com a reivindicação 1 ou 2, **CARACTERIZADO** pelo fato de que as instruções são recebidas
25 por intermédio de uma interface de usuário simples.

4. Primeiro dispositivo (110) adaptado para introduzir um número de dispositivos adicionais (120, 130) em uma rede segura (100), o primeiro dispositivo compreendendo:

uma unidade de comunicação (119) adaptada para se comunicar com dispositivos adicionais, e para receber a partir de cada um de um número de dispositivos uma solicitação (320) para inserção na rede segura;

5 um processador (114) adaptado para se comunicar com a unidade de comunicação e para inserir o número determinado de dispositivos na rede segura;

CARACTERIZADO pelo fato de que:

10 o primeiro dispositivo compreende ainda uma interface (115) adaptada para receber uma instrução para inserir um número determinado de dispositivos adicionais na rede segura; e

15 o processador (114) é adaptado adicionalmente para verificar se o número de solicitações recebidas é igual ao número determinado de dispositivos adicionais.

5. Primeiro dispositivo, de acordo com a reivindicação 4, **CARACTERIZADO** pelo fato de que a interface (115) é adaptada adicionalmente para receber instruções para prosseguir com a inserção.

20 6. Primeiro dispositivo, de acordo com a reivindicação 5, **CARACTERIZADO** pelo fato de que a interface compreende um botão (116) adaptado para receber as instruções.

25 7. Ponto central, de acordo com a reivindicação 5, **CARACTERIZADO** pelo fato de que a interface compreende um LED (118) adaptado para indicar o estado do primeiro dispositivo.

REIVINDICAÇÕES

1. Método de introduzir por intermédio de um primeiro dispositivo (110) um número determinado de dispositivos adicionais (120, 130) em uma rede segura (100), o método
5 compreendendo as etapas, no primeiro dispositivo, de:

receber (320) uma solicitação para inserção na rede segura a partir de cada um de um número de dispositivos adicionais; e

inserir (338) o número determinado de dispositivos
10 adicionais na rede segura, **CARACTERIZADO** por:

antes da etapa de receber uma solicitação, a etapa de receber (302) uma instrução para introduzir um número determinado de dispositivos adicionais na rede segura; e

antes da etapa de inserção, a etapa de verificar
15 (331) se o número de solicitações recebidas é igual ao número determinado de dispositivos adicionais.

2. Método, de acordo com a reivindicação 1, **CARACTERIZADO** por compreender adicionalmente a etapa, antes da etapa de verificação (331), de receber (330) por intermédio do primeiro dispositivo uma instrução para prosseguir
20 com a inserção do número determinado de dispositivos adicionais.

3. Método, de acordo com a reivindicação 1 ou 2, **CARACTERIZADO** pelo fato de que as instruções são recebidas
25 por intermédio de uma interface de usuário simples.

4. Primeiro dispositivo (110) adaptado para introduzir um número de dispositivos adicionais (120, 130) em uma rede segura (100), o primeiro dispositivo compreendendo:

uma unidade de comunicação (119) adaptada para se comunicar com dispositivos adicionais, e para receber a partir de cada um de um número de dispositivos uma solicitação (320) para inserção na rede segura;

5 um processador (114) adaptado para se comunicar com a unidade de comunicação e para inserir o número determinado de dispositivos na rede segura;

CARACTERIZADO pelo fato de que:

10 o primeiro dispositivo compreende ainda uma interface (115) adaptada para receber uma instrução para inserir um número determinado de dispositivos adicionais na rede segura; e

15 o processador (114) é adaptado adicionalmente para verificar se o número de solicitações recebidas é igual ao número determinado de dispositivos adicionais.

5. Primeiro dispositivo, de acordo com a reivindicação 4, **CARACTERIZADO** pelo fato de que a interface (115) é adaptada adicionalmente para receber instruções para prosseguir com a inserção.

20 6. Primeiro dispositivo, de acordo com a reivindicação 5, **CARACTERIZADO** pelo fato de que a interface compreende um botão (116) adaptado para receber as instruções.

25 7. Primeiro dispositivo, de acordo com a reivindicação 4, **CARACTERIZADO** pelo fato de que a interface compreende um LED (118) adaptado para indicar o estado do primeiro dispositivo.