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

(11) BR 112016011293-8 B1

(22) Data do Depósito: 19/11/2014

(45) Data de Concessão: 02/08/2022

(54) Título: TERMINAL, DISPOSITIVO MÓVEL, E MÉTODO PARA A CONDUÇÃO DE UMA TRANSAÇÃO MÓVEL CONVENIENTE E SEGURA, USANDO-SE UM TERMINAL E UM DISPOSITIVO MÓVEL

(51) Int.Cl.: G06Q 30/06; G06Q 20/32.

(30) Prioridade Unionista: 19/11/2013 US 14/083,948.

(73) Titular(es): WAYNE FUELING SYSTEMS LLC.

(72) Inventor(es): WEIMING TANG; JAMES MATTHEW BREWER.

(86) Pedido PCT: PCT US2014066359 de 19/11/2014

(87) Publicação PCT: WO 2015/077307 de 28/05/2015

(85) Data do Início da Fase Nacional: 18/05/2016

(57) Resumo: SISTEMAS E MÉTODOS PARA TRANSAÇÕES MÓVEIS CONVENIENTES E SEGURAS. A presente invenção refere-se sistemas e métodos para a condução de transações móveis convenientes e seguras entre um terminal de paga-mento e um dispositivo móvel, por exemplo, em um ambiente de abastecimento de combustível, que são descritos no presente relatório descritivo. Em algumas modalidades, o terminal de pagamento e o dispositivo móvel conduzem um processo de autenticação mútua que, se bem-sucedido, produz uma chave de sessão, a qual pode ser usada para encriptação de dados sensíveis a serem trocados entre o terminal de pagamento e o dispositivo móvel. A informação de pagamento e de fidelidade pode ser comunicada de forma segura a partir do dispositivo móvel para o terminal de pagamento, usando-se a chave de sessão. Isto pode ser feito automaticamente, sem se esperar que o usuário inicie uma transação, para encurtar o tempo de transação total. A transação também pode ser completada sem qualquer interação de usuário com o dispositivo móvel, aumentando a conveniência do usuário, uma vez que o dispositivo móvel pode ser deixado no bolso do usuário, na bolsa, no veículo, etc..

Relatório Descritivo da Patente de Invenção para **"TERMINAL, DISPOSITIVO MÓVEL, E MÉTODO PARA A CONDUÇÃO DE UMA TRANSAÇÃO MÓVEL CONVENIENTE E SEGURA, USANDO-SE UM TERMINAL E UM DISPOSITIVO MÓVEL".**

REFERÊNCIA CRUZADA A PEDIDOS RELACIONADOS

[001] Este pedido reivindica o benefício da prioridade do Pedido de Patente Não Provisória U.S. Nº de Série 14/083948, conforme depositado em 19 de novembro de 2013, o qual é incorporado aqui como referência em sua totalidade.

CAMPO

[002] O assunto descrito aqui se refere geralmente a sistemas e métodos para transações móveis convenientes e seguras, e, mais particularmente, para um pagamento móvel conveniente e seguro em um ambiente de distribuição de combustível.

ANTECEDENTES

[003] Vários sistemas de pagamento com móvel foram desenvolvidos, nos quais um dispositivo móvel pode ser usado para o pagamento por artigos ou serviços em um terminal de pagamento. Em alguns sistemas, o dispositivo móvel não se comunica diretamente com o terminal de pagamento. Ao invés disso, a transação é conduzida entre uma infraestrutura de pagamento de dispositivo móvel e uma infraestrutura de pagamento de comerciante (por exemplo, de nuvem para nuvem). A integração destas infraestruturas complexas e amplamente divergentes, contudo, frequentemente pode ser proibitiva em termos de custos.

[004] Outros sistemas envolve uma comunicação direta entre o dispositivo móvel e o terminal de pagamento. Nesses sistemas, dados de usuário sensíveis, tal como uma informação de pagamento e fidelidade, são transmitidos como texto claro, dando origem a um grande

número de questões de segurança. Por exemplo, os dados de usuário sensíveis podem ser interceptados por terceiros inescrupulosos. Isto pode ser de preocupação em particular em ambientes de abastecimento de combustível, em que o terminal de pagamento frequentemente está disposto em uma instalação externa automatizada, em que há um risco elevado de espionagem ou violação. Os usuários podem ser desencorajados quanto a usarem esses sistemas por medo que o terminal de pagamento possa ter sido comprometido.

[005] Muitos sistemas de pagamento com móvel existentes também requerem uma interação de usuário com o dispositivo móvel, antes, durante ou após uma transação. Por exemplo, o usuário deve recuperar o dispositivo móvel e abrir um aplicativo de carteira digital ou de outra forma interagir com um software executado no dispositivo móvel para começar uma transação. O usuário também deve ser capaz de levar o dispositivo móvel até o terminal de pagamento para colocar o dispositivo móvel em grande proximidade com o terminal de pagamento.

[006] Os sistemas existentes de pagamento com móvel assim podem ser inseguros e incômodos ou consumirem tempo para o usuário, e existe uma necessidade de sistemas melhorados de pagamento com móvel.

BREVE DESCRIÇÃO

[007] Sistemas e métodos para a condução de transações móveis convenientes e seguras entre um terminal de pagamento e um dispositivo móvel, por exemplo, em um ambiente de abastecimento de combustível, são expostos aqui. Em algumas modalidades, o terminal de pagamento e o dispositivo móvel conduzem um processo de autenticação mútua que, se bem-sucedido, produz uma chave de sessão, a qual pode ser usada para encriptação de dados sensíveis a serem trocados entre o terminal de pagamento e o dispositivo móvel. A informação de pagamento e de fidelidade pode ser comunicada de

forma segura a partir do dispositivo móvel para o terminal de pagamento, usando-se a chave de sessão. Isto pode ser feito automaticamente, sem se esperar que o usuário inicie uma transação, para encurtar o tempo de transação total. A transação também pode ser completada sem qualquer interação de usuário com o dispositivo móvel, aumentando a conveniência do usuário, uma vez que o dispositivo móvel pode ser deixado no bolso do usuário, na bolsa, no veículo, etc. Os dados sensíveis podem ser apagados do terminal de pagamento automaticamente, após uma transação ser concluída ou se uma transação nunca for iniciada.

[008] Em algumas modalidades, um terminal inclui um transceptor sem fio configurado para comunicação de forma sem fio com um dispositivo móvel, um dispositivo de entrada configurado para receber uma entrada a partir de um usuário do terminal, um dispositivo de armazenamento configurado para armazenamento de uma informação de usuário associada a um ou mais usuários, e pelo menos um processador acoplado ao transceptor sem fio, ao dispositivo de entrada e ao dispositivo de armazenamento. O processador é programado para: a condução de um processo de autenticação mútua com um dispositivo móvel para a obtenção de uma chave de sessão, o recebimento de uma informação de usuário a partir do dispositivo móvel através do transceptor sem fio, a referida informação de usuário sendo encriptada pela chave de sessão, o armazenamento de uma informação de usuário no dispositivo de armazenamento, o recebimento de uma requisição para iniciação de uma transação a partir de um usuário através do dispositivo de entrada, o alerta ao usuário quanto a uma informação de autorização, o recebimento de uma informação de autorização a partir do usuário através do dispositivo de entrada, a encriptação da informação de autorização usando-se a chave de sessão, o envio da informação de autorização encriptada para o dispositivo móvel através

do transceptor sem fio, o recebimento de um resultado de validação a partir do dispositivo móvel através do transceptor sem fio, e quando o resultado de validação é positivo, a conclusão de uma transação requisitada pelo usuário usando-se a informação de usuário armazenada.

[009] Em algumas modalidades, um dispositivo móvel inclui um transceptor sem fio configurado para comunicação de forma sem fio com um terminal, um dispositivo de armazenamento configurado para armazenamento de uma informação de usuário associada a um usuário, e pelo menos um processador acoplado ao transceptor sem fio e ao dispositivo de armazenamento. O processador é programado para a execução de uma transação com um terminal por meio de: condução de um processo de autenticação mútua com o terminal, para a obtenção de uma chave de sessão, encriptação da informação de usuário armazenada no dispositivo de armazenamento usando-se a chave de sessão, envio da informação de usuário encriptada para o terminal através do transceptor sem fio, recebimento de uma informação de autorização encriptada a partir do terminal através do transceptor sem fio, a desencriptação da informação de autorização usando-se a chave de sessão, a comparação da informação de autorização com uma informação de autorização mestre para a geração de um resultado de validação, o resultado de validação sendo positivo quando uma combinação for encontrada e sendo negativo quando uma combinação não for encontrada, e o envio do resultado de validação para o terminal através do transceptor sem fio para se facilitar a conclusão da transação pelo terminal.

[0010] Em algumas modalidades, um método para a condução de uma transação móvel conveniente e segura usando-se um terminal e um dispositivo móvel inclui, automaticamente e sem uma interação de usuário com o terminal ou o dispositivo móvel, a condução de um

processo de autenticação mútua, no qual o terminal e o dispositivo móvel autenticam um para cada outro para a obtenção de uma chave de sessão, o recebimento de uma informação de usuário a partir do dispositivo móvel através de um transceptor sem fio do terminal, a referida informação de usuário sendo encriptada pela chave de sessão, e o armazenamento da informação de usuário em um dispositivo de armazenamento do terminal. O método também inclui o recebimento de uma requisição para se iniciar uma transação a partir de um usuário via um dispositivo de entrada do terminal, o alerta ao usuário quanto a uma informação de autorização através de um visor eletrônico do terminal, o recebimento de uma informação de autorização a partir do usuário via o dispositivo de entrada, a encriptação da informação de autorização usando-se a chave de sessão, o envio da informação de autorização encriptada para o dispositivo móvel através do transceptor sem fio, o recebimento de um resultado de validação a partir do dispositivo móvel através do transceptor sem fio, e quando o resultado de validação é positivo, a conclusão da transação requisitada pelo usuário, usando-se a informação de usuário armazenada.

BREVE DESCRIÇÃO DOS DESENHOS

[0011] Estes e outros recursos serão mais prontamente entendidos a partir da descrição detalhada a seguir tomada em conjunto com os desenhos associados, em que:

[0012] a figura 1 é um diagrama esquemático de uma modalidade de exemplo de um ambiente de abastecimento de combustível;

[0013] a figura 2 é um diagrama de sequência de uma modalidade de exemplo de um método para a condução de uma transação segura e conveniente entre um terminal de pagamento, um dispositivo móvel e um usuário;

[0014] a figura 3 é um diagrama esquemático de uma modalidade de exemplo de um sistema de computador;

[0015] a figura 4 é um diagrama esquemático de uma modalidade de exemplo de um terminal de pagamento;

[0016] a figura 5 é um diagrama esquemático de uma modalidade de exemplo de um dispositivo móvel;

[0017] a figura 6 é um fluxograma que descreve o método da figura 2 da perspectiva do terminal de pagamento;

[0018] a figura 7 é um fluxograma que descreve o método da figura 2 da perspectiva do dispositivo móvel;

[0019] a figura 8 é um diagrama esquemático de um certificado de exemplo ou um esquema de chave para a realização de um processo de autenticação mútua; e

[0020] a figura 9 é um diagrama esquemático de outro certificado de exemplo ou esquema de chave para a realização de um processo de autenticação mútua.

[0021] É notado que os desenhos não estão necessariamente em escala. Os desenhos são pretendidos para descreverem apenas aspectos típicos do assunto exposto aqui, e, portanto, não devem ser considerados como limitando o escopo da exposição. Nos desenhos, uma numeração similar representa elementos similares entre os desenhos.

DESCRIÇÃO DETALHADA

[0022] Certas modalidades de exemplo serão descritas, agora, para a provisão de um entendimento geral dos princípios da estrutura, da função, da fabricação e do uso dos dispositivos, sistemas e métodos expostos aqui.

[0023] Os sistemas e métodos para a condução de transações móveis convenientes e seguras entre um terminal de pagamento e um dispositivo móvel, por exemplo, em um ambiente de abastecimento de combustível, são expostos aqui. Em algumas modalidades, o terminal de pagamento e o dispositivo móvel conduzem um processo de

autenticação mútua que, se bem-sucedido, produz uma chave de sessão, a qual pode ser usada para a encriptação de dados sensíveis a serem trocados ente o terminal de pagamento e o dispositivo móvel. Uma informação de pagamento e de fidelidade pode ser comunicada de forma segura a partir do dispositivo móvel para o terminal de pagamento, usando-se a chave de sessão. Isto pode ser feito automaticamente, sem se esperar que o usuário inicie uma transação, para encurtar o tempo de transação total. A transação também pode ser completada sem qualquer interação de usuário com o dispositivo móvel, aumentando a conveniência do usuário, uma vez que o dispositivo móvel pode ser deixado no bolso do usuário, na bolsa, no veículo, etc. Os dados sensíveis podem ser apagados do terminal de pagamento automaticamente, após uma transação ser concluída ou se uma transação nunca for iniciada.

AMBIENTE DE ABASTECIMENTO DE COMBUSTÍVEL

[0024] A figura 1 ilustra uma modalidade de exemplo de um ambiente de abastecimento de combustível 100, no qual um ou mais dos sistemas e métodos expostos aqui podem ser implementados. O ambiente de abastecimento de combustível 100 geralmente inclui um terminal de pagamento 102 e um dispositivo móvel 104 associado a um usuário (por exemplo, um consumidor buscando fazer uma compra usando o terminal de pagamento).

[0025] O terminal de pagamento 102 pode ser integrado com uma bomba de distribuição de combustível 106, a qual pode incluir vários recursos bem entendidos por aqueles versados na técnica, tais como um bocal, uma bomba, botões para a seleção do tipo de combustível, uma tela de visor eletrônico e assim por diante. O terminal de pagamento 102 pode ser ou pode incluir um sistema de computador, conforme descrito abaixo. O terminal de pagamento 102 pode ser configurado para comunicação com várias redes (por exemplo,

diretamente ou através de um servidor de interface interna), tal como uma rede de fidelidade de abastecimento de combustível 108 para a manutenção, a checagem e a atualização de uma informação de fidelidade de consumidor e uma rede de pagamento de abastecimento de combustível 110 para processamento de compra de combustível e outras transações.

[0026] O dispositivo móvel 104 pode ser ou pode incluir um sistema de computador, conforme descrito abaixo. O dispositivo móvel 104 pode ser ou pode incluir qualquer dispositivo que seja configurado para troca de dados por uma rede de comunicações, tais como um telefone móvel, um computador tablet, um computador laptop, uma carteira digital e assim por diante. O dispositivo móvel 104 pode ser um dispositivo portátil que pode ser mantido por um usuário ou armazenado em um bolso do usuário, na bolsa, no veículo, etc. O dispositivo móvel 104 também pode ser integrado com um objeto móvel, tal como um carro, um caminhão, uma motocicleta ou outro veículo.

[0027] Embora um ambiente de abastecimento de combustível 100 seja mostrado na figura 1, será apreciado que os sistemas e métodos expostos aqui podem ser prontamente aplicados em outros cenários, por exemplo, em qualquer cenário no qual um dispositivo móvel é usado para a condução de uma transação com um terminal. As transações podem incluir transações de pagamento, transações de reembolso, transações de serviço, transações de controle ou qualquer outra transação que requeira comunicação. Os terminais podem incluir terminais de pagamento, quiosques e assim por diante, e/ou podem ser parte de um distribuidor (por exemplo, um distribuidor de combustível, um distribuidor de lanche ou bebida, um distribuidor de dinheiro, etc.).

PAGAMENTO COM MÓVEL CONVENIENTE E SEGURO

[0028] A figura 2 ilustra uma modalidade de exemplo de um método de pagamento com móvel conveniente e seguro, por meio do qual um

usuário pode completar uma transação de compra usando o terminal de pagamento 102 e o dispositivo móvel 104. Antes da execução do método ilustrado, um usuário pode habilitar recursos de pagamento com móvel do dispositivo móvel 104, por exemplo, pela instalação de um aplicativo no dispositivo móvel ou pelo carregamento de uma informação de conta de pagamento e de fidelidade no dispositivo móvel. A habilitação do dispositivo móvel 104 para pagamento com móvel pode ser um processo de uma vez, de modo que uma interação de usuário com o dispositivo móvel não seja requerida antes, durante ou após as transações completadas após o dispositivo móvel ser inicialmente habilitado.

[0029] O método ilustrado pode começar com o dispositivo móvel e o terminal de pagamento estabelecendo um enlace de comunicações seguro entre eles. O dispositivo móvel pode usar técnicas baseadas em interrogação ou interrupção para determinar quando um terminal de pagamento está próximo e, quando um terminal de pagamento for detectado, pode iniciar um processo de autenticação de duas vias com o terminal de pagamento. De forma alternativa ou adicional, o terminal de pagamento pode usar técnicas baseadas em interrogação ou interrupção para determinar quando um dispositivo móvel está próximo e, quando um dispositivo móvel for detectado, pode iniciar um processo de autenticação de duas vias com o dispositivo móvel. Em algumas modalidades, o dispositivo móvel periodicamente (por exemplo, a cada 30 segundos) emite um sinal de interrogação, o qual é recebido por quaisquer terminais de pagamento que estejam no alcance e que é usado por esses terminais de pagamento para se iniciar o processo de autenticação de duas vias.

[0030] Se o dispositivo móvel for capaz de autenticar o terminal de pagamento e o terminal de pagamento for capaz de autenticar o dispositivo móvel, o processo de autenticação de duas vias será

completado de forma bem-sucedida com o dispositivo móvel e o terminal de pagamento, cada um possuindo uma chave de sessão (ou respectivas porções de um par de chaves de sessão), a qual pode ser usada para a encriptação e a desencriptação de uma informação a ser comunicada de forma segura entre o dispositivo móvel e o terminal de pagamento. O termo "chave de sessão" pode ser usado de forma intercambiável para referência a uma única chave e para referência a uma ou ambas as porções de um par de chaves de sessão. Se o processo de autenticação se completar de forma bem-sucedida, o dispositivo móvel encriptará uma informação de consumidor associada ao usuário ou ao consumidor (por exemplo, conta ou outra informação de pagamento, informação de fidelidade e assim por diante) usando a chave de sessão. A informação de consumidor encriptada pode ser desencriptada pelo terminal de pagamento usando a chave de sessão e armazenada em uma localização segura no terminal de pagamento, enquanto o terminal de pagamento espera que o usuário inicie uma transação. Os dados de pagamento e fidelidade de usuário assim podem ser pré-carregados no terminal de pagamento, antes de o usuário iniciar uma transação (por exemplo, antes de um consumidor de combustível sair mesmo do seu veículo).

[0031] Um usuário então pode iniciar uma transação com o terminal de pagamento, por exemplo, ao distribuir combustível a partir de uma bomba de combustível acoplada ao terminal de pagamento ou ao pressionar um botão ou atuar algoutro elemento de interface de usuário do terminal de pagamento. O terminal de pagamento pode incluir provisões para se garantir que o usuário que estiver iniciando uma transação esteja autorizado a usar os recursos de pagamento do dispositivo móvel, o que pode evitar o uso desses recursos, quando o dispositivo móvel for roubado ou comprometido de outra forma. Por exemplo, uma vez que uma transação seja iniciada pelo usuário, o

terminal de pagamento pode alertar ao usuário quanto a uma informação de autorização. A informação de autorização pode incluir um número de identificação pessoal (PIN), uma senha, dados biométricos, tal como uma impressão digital ou uma imagem da face, ou qualquer outra informação que possa ser usada para se garantir que um usuário seja um usuário autorizado dos recursos de pagamento do dispositivo móvel. Esta informação de autorização pode ser encriptada, então, pelo terminal de pagamento usando-se a chave de sessão e transmitida para o dispositivo móvel para validação.

[0032] Em alguns casos, uma pluralidade de dispositivos móveis com recursos de pagamento habilitados pode estar no alcance do terminal de pagamento ao mesmo tempo (por exemplo, no caso de uma área de caixa ocupada em um posto de gasolina), e, portanto, o terminal de pagamento pode ter uma pluralidade de conjuntos de informação de consumidor armazenada ali. Assim sendo, o terminal de pagamento também pode alertar ao usuário quanto a uma identificação de usuário (por exemplo, o nome do usuário ou um nome de conta estabelecido pelo usuário), o que pode ter uma referência cruzada com a informação de consumidor recebida pelo terminal de pagamento a partir dos dispositivos móveis em alcance, para se determinar qual dos dispositivos móveis plurais está associado ao usuário que iniciou a transação.

[0033] Em alguns casos, o dispositivo móvel do usuário pode ser configurado com uma informação de pagamento para uma pluralidade de tipos de pagamento (por exemplo, uma informação para múltiplos cartões de crédito ou débito) e/ou uma informação de fidelidade para uma pluralidade de relações de fidelidade, e pode transferir a informação de pagamento para cada um dos tipos de pagamento e uma informação de fidelidade para cada uma das relações de fidelidade para o terminal de pagamento. Assim sendo, o terminal de pagamento

também pode alertar ao usuário quanto a um tipo de pagamento e/ou um tipo de fidelidade a ser usado. Em outras palavras, o terminal de pagamento pode permitir que o usuário selecione qual da pluralidade de tipos de pagamento ou tipos de fidelidade configurados no dispositivo móvel deve ser usado para se completar a transação.

[0034] Uma vez que o usuário introduza a informação requerida, o terminal de pagamento encripta a informação de autorização introduzida usando a chave de sessão e a transmite para o dispositivo móvel para validação. Quando múltiplos dispositivos móveis estão no alcance, o terminal de pagamento pode enviar a informação de autorização encriptada apenas para o dispositivo móvel associado à identificação de usuário provida pelo usuário. Quando múltiplas opções de pagamento ou fidelidade estão disponíveis a partir do dispositivo móvel, o terminal de pagamento pode enviar a seleção do usuário de tipo de pagamento ou fidelidade para o dispositivo móvel com a informação de autorização encriptada. A informação de tipo de pagamento ou fidelidade pode ser enviada na forma encriptada ou não encriptada.

[0035] O dispositivo móvel então desencripta a informação de autorização recebida a partir do terminal de pagamento usando a chave de sessão, e compara a informação de autorização recebida com uma informação de autorização mestre armazenada no dispositivo móvel. Se uma combinação for encontrada, o usuário será um usuário autorizado do dispositivo móvel, e o usuário poderá enviar um resultado de validação positivo para o terminal de pagamento. Se nenhuma combinação for encontrada, o usuário não estará autorizado e o dispositivo móvel poderá enviar um resultado de validação negativo para o terminal de pagamento.

[0036] Quando o terminal de pagamento recebe um resultado de validação positivo a partir do dispositivo móvel, a transação é completada usando-se a informação de consumidor previamente

recebida a partir do dispositivo móvel e agora armazenada no terminal de pagamento. Quando o terminal de pagamento recebe um resultado de validação negativo do dispositivo móvel, o terminal de pagamento pode recusar a transação ou permitir que o usuário tente a informação de autorização de novo, em cujo caso o processo acima é repetido para validação da informação de autorização recém-introduzida com o dispositivo móvel.

[0037] Após a transação ser completada, a informação de usuário armazenada no terminal de pagamento pode ser apagada. O usuário também pode ser alertado quanto a um recibo impresso ou eletrônico, e, se o usuário optar por um recibo eletrônico, o terminal de pagamento poderá transmitir um recibo eletrônico para o dispositivo móvel, em que pode ser subsequentemente recuperado pelo usuário. O recibo pode ser encriptado usando-se a chave de sessão. O terminal de pagamento também pode ser configurado para apagar uma informação de usuário armazenada ali, quando uma comunicação for perdida com o dispositivo móvel (por exemplo, quando o dispositivo móvel deixar o alcance de comunicações do terminal de pagamento), ou quando um tempo predeterminado decorrer sem uma transação ser iniciada (por exemplo, pelo menos em torno de 30 minutos).

[0038] No método acima, o processo de autenticação de duas vias assegura que o dispositivo móvel transfira uma informação de usuário sensível apenas para um terminal de pagamento autenticado de confiança. Esta informação de usuário sensível pode ser encriptada entre o dispositivo móvel e o terminal de pagamento para se evitar uma interceptação por partes maliciosas. De modo similar, o processo de autenticação de duas vias assegura que o terminal de pagamento apenas aceita pagamentos de transação a partir de um dispositivo móvel autenticado de confiança.

[0039] Além disso, a maioria da informação de consumidor (por

exemplo, dados de pagamento e fidelidade) é transferida para o terminal de pagamento automaticamente, sem qualquer interação de usuário com o dispositivo móvel. Assim sendo, o tempo perdido e a inconveniência associados à localização e ao alcance do dispositivo móvel, abertura de aplicativos ou ativação de recursos de pagamento e assim por diante, são eliminados. Um usuário pode completar uma transação inteira sem mesmo tocar ou interagir com o dispositivo móvel. Em outras palavras, uma transação pode ser completada sem qualquer interação física entre o usuário e o dispositivo móvel antes, durante ou após a transação. O processo de pagamento também pode ser expedito, uma vez que uma informação de consumidor de usuário já está armazenada no terminal de pagamento no momento em que o usuário inicia uma transação, poupando tempo que, de outra forma, seria requerido para a autenticação e a transferência da informação.

[0040] Finalmente, o método acima pode alivia preocupações referentes ao uso de dispositivos móveis na proximidade de uma bomba de combustível. Alguns postos de gasolina banem esse uso, uma vez que é alegado que os dispositivos móveis podem gerar eventos elétricos que podem causar um incêndio. O método acima não requer qualquer interação entre o usuário e o dispositivo móvel, e, portanto, o usuário pode deixar o dispositivo móvel no seu bolso, na bolsa, no veículo ou em outra localização e eliminar qualquer preocupação de o dispositivo móvel ser um risco de incêndio.

[0041] Os dispositivos de exemplo ou estruturas para a realização do método acima são discutidos em detalhes abaixo, juntamente com variações do método acima.

SISTEMA DE COMPUTADOR

[0042] A figura 3 ilustra uma arquitetura de exemplo de um sistema de computador 200, o qual pode ser usado para a implementação do terminal de pagamento 102 ou do dispositivo móvel 104 da figura 1.

Embora um sistema de computador 200 de exemplo seja mostrado e descrito aqui, será apreciado que isto é em nome da generalidade e da conveniência. Em outras modalidades, o sistema de computador pode diferir na arquitetura e na operação daquilo mostrado e descrito aqui.

[0043] O sistema de computador 200 pode incluir um processador 202, que controla a operação do sistema de computador 200, por exemplo, pela execução de um sistema operacional (OS), drivers de dispositivo, programas aplicativos e assim por diante. O processador 202 pode incluir qualquer tipo de microprocessador ou unidade de processamento central (CPU), incluindo microprocessadores de finalidade geral ou de finalidade especial e/ou qualquer um de uma variedade de sistemas de processador único ou múltiplo comercialmente disponíveis.

[0044] O sistema de computador 200 também pode incluir uma memória 204, que provê um armazenamento temporário ou permanente para um código a ser executado pelo processador 202 ou para dados que sejam processados pelo processador 202. A memória 204 pode incluir uma memória apenas de leitura (ROM), uma memória flash, uma ou mais variedades de memória de acesso randômico (RAM), e/ou uma combinação de tecnologias de memória.

[0045] Os vários elementos do sistema de computador 200 podem ser acoplados uns aos outros. Por exemplo, o processador 202 pode ser acoplado à memória 204. Os vários elementos do sistema de computador 200 podem ser acoplados diretamente uns aos outros ou podem ser acoplados uns aos outros através de um ou mais componentes intermediários. Na modalidade ilustrada, os vários elementos do sistema de computador 200 são acoplados a um barramento de sistema 206. O barramento de sistema ilustrado 206 é uma abstração que representa linhas / interfaces e/ou conexões de queda múltipla ou de ponto a ponto, conectadas por pontes,

adaptadores e/ou controladores apropriados.

[0046] O sistema de computador 200 também pode incluir uma interface de rede 208, o que permite que o sistema de computador 200 se comunique com dispositivos remotos (por exemplo, outros sistemas de computador) por uma rede. No caso do terminal de pagamento 102, a interface de rede pode facilitar uma comunicação com a rede de fidelidade de abastecimento de combustível 108 e a rede de pagamento de abastecimento de combustível 110, por exemplo, através de uma rede Ethernet, WiFi ou de dados celular.

[0047] O sistema de computador 200 também pode incluir uma interface de entrada / saída (I/O) 210, a qual facilita uma comunicação entre um ou mais dispositivos de entrada, um ou mais dispositivos de saída e vários outros componentes do sistema de computador 200. Os dispositivos de entrada e de saída de exemplo incluem teclados, telas de toque, botões, leitoras de cartão de tarja magnética, luzes, alto-falantes e assim por diante.

[0048] O sistema de computador 200 também pode incluir um dispositivo de armazenamento 212, o qual pode incluir qualquer meio convencional para o armazenamento de dados de uma maneira não volátil e/ou não transiente. O dispositivo de armazenamento 212 assim pode manter dados e/ou instruções em um estado persistente (isto é, o valor é retido, apesar de uma interrupção de potência do sistema de computador 200). O dispositivo de armazenamento 212 pode incluir uma ou mais unidades de disco rígido, unidades flash, unidades USB, unidades óticas, vários discos de mídia ou cartões, tecnologias de memória e/ou qualquer combinação dos mesmos, e pode ser conectado diretamente aos outros componentes do sistema de computador 200 ou conectado remotamente a eles, tal como por uma rede.

[0049] O sistema de computador 200 também pode incluir um controlador de visor 214, o qual pode incluir um processador de vídeo e

uma memória de vídeo, e pode gerar imagens a serem exibidas em um ou mais visores eletrônicos, de acordo com instruções recebidas a partir do processador 202.

[0050] O sistema de computador 200 também pode incluir um elemento seguro 216. O elemento seguro 216 pode ser uma plataforma resistente à violação (por exemplo, um microcontrolador seguro em um chip) capaz de hospedar de forma segura aplicativos e seus dados confidenciais e criptografados (por exemplo, um gerenciamento de chave) de acordo com as regras e as exigências de segurança estabelecidas por um conjunto de autoridades de confiança bem identificadas. O elemento seguro 216 pode ser capaz de prover uma geração de número randômico, uma geração de pares de chave pública / privada específicos de dispositivo, e executar um algoritmo de segurança. Os exemplos conhecidos de algoritmos de segurança incluem, mas não estão limitados a Hash, TDES, AES, RSA, etc. Os elementos seguros 216 de exemplo incluem placas de circuito integrado universais (UICC), elementos seguros embutidos e microcartões digitais seguros (microSD). O elemento seguro 216 pode ser ou pode incluir um dispositivo de armazenamento.

[0051] O sistema de computador 200 também pode incluir uma interface de comunicação segura 218, através da qual o sistema de computador 200 pode conduzir processos de autenticação mútua e se comunicar com outros sistemas de computador. A interface de comunicação segura 218 pode ser sem fio (por exemplo, uma comunicação de campo próximo (NFC), WiFi, Bluetooth, Bluetooth LE, ZigBee e similares) ou com fio (por exemplo, USB ou Ethernet). No caso de NFC, por exemplo, o sistema de computador 200 pode incluir um transceptor de rádio configurado para comunicação com um transceptor de rádio de outro dispositivo usando um ou mais padrões, tais como ISO/IEC 1443, FeliCa, ISO/IEC 18092 e aqueles definidos pelo Fórum

de NFC. As interfaces de comunicação segura 218 do terminal de pagamento 102 e do dispositivo móvel 104 podem ser selecionadas para a provisão do alcance de comunicação desejado. Em algumas modalidades, Bluetooth (por exemplo, um Bluetooth de classe 2 tendo um alcance de 5 a 10 metros) pode ser usado para a interface de comunicação segura 218, para se permitir que o dispositivo móvel 104 permaneça um pouco distante do terminal de pagamento 102 (por exemplo, no bolso de um usuário, na bolsa ou no veículo), enquanto, ao mesmo tempo, limita-se o alcance de comunicação, de modo que partes maliciosas não possam atacar o sistema a partir de uma distância grande e de modo que os dispositivos móveis de motoristas passando ou dispositivos móveis distantes a não serem usados provavelmente para uma transação não sejam autenticados desnecessariamente com o terminal de pagamento.

MÓDULOS GENÉRICOS

[0052] As várias funções executadas pelo terminal de pagamento 102 e pelo dispositivo móvel 104 podem ser logicamente descritas como sendo realizadas por um ou mais módulos ou unidades. Será apreciado que esses módulos podem ser implementados em hardware, software ou uma combinação dos mesmos. Será adicionalmente apreciado que, quando implementados em um software, os módulos podem ser parte de um único programa ou de um ou mais programas em separado, e podem ser implementados em uma variedade de contextos (por exemplo, como parte de um sistema operacional, um driver de dispositivo, um aplicativo independente e/ou combinações dos mesmos). Além disso, um software concretizando um ou mais módulos pode ser armazenado como um programa executável em um ou mais meios de armazenamento que podem ser lidos em computador não transitórios, ou pode ser transmitido como um sinal, uma onda portadora, etc. As funções expostas aqui como sendo realizadas por um

módulo em particular também podem ser realizadas por qualquer outro módulo ou por uma combinação de módulos, e o terminal de pagamento 102 e o dispositivo móvel 104 podem incluir menos ou mais módulos do que o que é mostrado e descrito aqui. Conforme usado aqui, um software se refere a quaisquer instruções de programa executáveis, incluindo um firmware.

MÓDULOS DE TERMINAL DE PAGAMENTO

[0053] A figura 4 é um diagrama esquemático dos módulos de uma modalidade de exemplo do terminal de pagamento 102. Conforme mostrado, o terminal de pagamento 102 pode incluir um módulo de autenticação 402, um módulo de recebimento de informação de usuário 404, um módulo de armazenamento de informação de usuário 406, um módulo de recebimento de requisição de transação 408, uma biblioteca de informação de usuário 410, um módulo de alerta ao usuário 412, um módulo de autorização 414, um módulo de validação 416, um módulo de processamento de transação 418 e um módulo de recibo 420.

[0054] O módulo de autenticação 402 pode ser configurado para execução de um processo de autenticação mútua com o dispositivo móvel 104. Em particular, o módulo de autenticação 402 pode ser configurado para interagir com um módulo de autenticação 502 do dispositivo móvel 104, usando-se a interface de comunicação segura 218 do terminal de pagamento 102 para a execução de um processo de autenticação mútua. Um processo de autenticação mútua de exemplo é descrito em detalhes abaixo.

[0055] O módulo de recebimento de informação de usuário 404 pode ser configurado para receber uma informação de usuário a partir de um dispositivo de pagamento (por exemplo, um dispositivo móvel 104) através da interface de comunicação segura 218 do terminal de pagamento 102. A informação de usuário pode incluir uma informação de pagamento, tais como números de cartão de crédito ou de débito,

datas de validade de cartão, códigos de segurança, nomes de titular, dados EMV® e assim por diante. A informação de usuário também pode incluir uma informação de fidelidade, tais como números de conta de fidelidade, nomes de conta e assim por diante. A informação de usuário recebida pode ser encriptada pelo dispositivo móvel 104, antes de uma transmissão para o terminal de pagamento 102 ocorrer. O módulo de recebimento de informação de usuário 404 pode ser configurado para a desencriptação da informação de usuário recebida usando-se uma chave de sessão gerada durante o processo de autenticação mútua executado pelo módulo de autenticação 402.

[0056] A informação de usuário desencriptada pode ser armazenada pelo módulo de armazenamento de informação de usuário 406 na biblioteca de informação de usuário 410, o que pode ser mantido no elemento seguro 216 ou em outro dispositivo de armazenamento 212 do terminal de pagamento 102. O módulo de armazenamento de informação de usuário 406 pode armazenar uma informação associada a uma pluralidade de usuários, por exemplo, quando uma pluralidade de dispositivos móveis 104 estiver no alcance de ou for autenticado de forma bem-sucedida com o terminal de pagamento 102. O módulo de armazenamento de informação de usuário 406 pode ser configurado para se deletar ou apagar uma informação de usuário, por exemplo, quando uma comunicação entre o terminal de pagamento 102 e o dispositivo móvel 104 cessar (por exemplo, porque uma transação está completada ou porque o dispositivo móvel sai do alcance de comunicação do terminal de pagamento), ou quando um tempo predeterminado decorrer após o recebimento da informação de usuário sem uma transação ser iniciada pelo usuário. Assim, se um dispositivo móvel 104 for autenticado, comunicar uma informação de usuário para o terminal de pagamento 102 e, então, sair do alcance de comunicações do terminal de pagamento, o módulo de armazenamento de informação

de usuário 406 poderá apagar a informação de usuário recebida. De modo similar, se um dispositivo móvel 104 for autenticado, comunicar uma informação de usuário para o terminal de pagamento 102 e, então, um tempo suficiente decorrer sem o usuário iniciar ou completar uma transação, o módulo de armazenamento de informação de usuário 406 poderá apagar a informação de usuário recebida.

[0057] O módulo de recebimento de requisição de transação 408 pode ser configurado para receber uma requisição para iniciar uma transação a partir de um usuário. Por exemplo, o módulo de recebimento de requisição de transação 408 pode detectar uma atuação de usuário de um botão, um teclado, uma tecla virtual, uma tela de toque ou outro elemento de interface de usuário do terminal de pagamento 102, em um esforço para iniciar uma transação (por exemplo, a distribuição e a compra de combustível).

[0058] Quando uma requisição de transação é recebida pelo módulo de recebimento de requisição de transação 408, o módulo de alerta ao usuário 412 pode ser configurado para alertar ao usuário quanto a qualquer informação adicional que seja requerida para se confirmar que o usuário é um usuário autorizado ou para se completar a transação. O módulo de alerta ao usuário 412 pode comandar um visor eletrônico, um alto-falante ou outro dispositivo de saída do terminal de pagamento 102 para e exibição de um alerta para o usuário. Uma informação de exemplo quanto à qual o usuário pode ser alertado inclui uma informação de autorização para se verificar que o usuário é um usuário autorizado do dispositivo móvel 104, uma informação de identificação de usuário para se determinar qual de uma pluralidade de conjuntos de informação de usuário armazenados na biblioteca de informação de usuário 410 pertence ao usuário, e/ou uma informação de tipo de pagamento ou fidelidade para se determinar qual de uma pluralidade de informações de pagamento ou fidelidade armazenadas

em associação ao usuário deve ser usada para se completar a transação. O módulo de alerta ao usuário 412 também pode ser configurado para o recebimento de uma informação quanto à qual o usuário é alertado. Por exemplo, o módulo de alerta ao usuário 412 pode receber uma entrada de usuário provida pela atuação pelo usuário de um botão, um teclado, uma tecla virtual, uma tela de toque, um scanner de impressão digital, uma câmera, etc.

[0059] O módulo de autorização 414 pode ser configurado para a transmissão de vários tipos de informação para o dispositivo móvel 104, usando-se a interface de comunicação segura 218 do terminal de pagamento 102. Por exemplo, uma informação de autorização de usuário alertada e recebida pelo módulo de alerta ao usuário 412 pode ser encriptada pelo módulo de autorização 414 e encaminhada para o terminal de pagamento 102 para validação.

[0060] Quando uma pluralidade de dispositivos móveis 104 está em comunicação com o terminal de pagamento 102, o módulo de autorização 414 pode determinar para qual da pluralidade de dispositivos móveis enviar a informação de autorização com base em uma informação de identificação de usuário sendo recebida pelo módulo de alerta ao usuário 412. Em particular, o módulo de autorização 414 pode comparar a informação de identificação recebida com uma informação de identificação armazenada na biblioteca de informação de usuário 410 em associação com os vários conjuntos de informação de usuário armazenados ali. A informação de autorização assim pode ser enviada apenas para o dispositivo móvel que proveu uma informação de usuário tendo uma identificação de usuário que combine com a identificação de usuário provida pelo usuário requisitando uma transação. Se nenhum dos dispositivos móveis tiver provido uma informação de combinação, um erro poderá ser reportado para o usuário, e o usuário poderá opcionalmente ser alertado quanto a uma

nova informação de autorização e/ou uma nova informação de identificação.

[0061] Quando a informação de usuário associada ao usuário requisitando uma transação incluir dados para uma pluralidade de tipos de pagamento e/ou uma pluralidade de tipos de fidelidade, o módulo de autorização 414 pode transmitir uma indicação de tipo de pagamento ou de fidelidade para o dispositivo móvel 104 juntamente com a informação de autorização. A indicação de tipo de pagamento ou de fidelidade pode ser baseada na seleção de tipo de pagamento ou de tipo de fidelidade recebida pelo módulo de alerta ao usuário 412.

[0062] O módulo de autorização 414 pode ser configurado para encriptar a informação de autorização e/ou a informação de tipo de pagamento ou de fidelidade, antes do envio para o dispositivo móvel 104. Em particular, a autorização e/ou a informação de tipo de pagamento ou fidelidade podem ser encriptadas usando-se uma chave de sessão gerada durante o processo de autenticação mútua conduzido pelo módulo de autenticação 402.

[0063] O módulo de validação 416 pode ser configurado para receber um resultado de validação a partir do dispositivo móvel 104 usando-se a interface de comunicação segura 218 do terminal de pagamento 102 após o dispositivo móvel avaliar a validade da informação provida pelo módulo de autorização 414. Se um resultado de validação positivo for recebido, o módulo de processamento de transação 418 poderá executar a transação requisitada pelo processamento da informação de pagamento e/ou de fidelidade do usuário, conforme armazenado na biblioteca 410 com a rede de pagamento de abastecimento de combustível 110 e/ou a rede de fidelidade de abastecimento de combustível 108 usando técnicas conhecidas. Se um resultado de validação negativo for recebido, o módulo de alerta ao usuário 412 poderá alertar ao usuário para

reintroduzir a informação de autorização ou poderá reportar um erro para o usuário e terminar a transação.

[0064] O módulo de recibo 420 pode ser configurado para a geração de um recibo que indica um ou mais parâmetros da transação. Por exemplo, o módulo de recibo 420 pode controlar uma impressora de recibo do terminal de pagamento 102 para a impressão de um recibo em papel, o qual pode ser recuperado pelo usuário. O módulo de alerta ao usuário 412 também pode perguntar ao usuário se um recibo eletrônico é desejado, em cujo caso o módulo de recibo 420 pode comunicar um recibo eletrônico para o dispositivo móvel 104, usando-se a interface de comunicação segura 218 do terminal de pagamento 102. O usuário então pode recuperar o recibo eletrônico a partir do dispositivo móvel 104 de acordo com a sua conveniência.

MÓDULOS DE DISPOSITIVO MÓVEL

[0065] A figura 5 é um diagrama esquemático dos módulos de uma modalidade de exemplo do dispositivo móvel 104. Conforme mostrado, o dispositivo móvel 104 pode incluir um módulo de autenticação 502, um módulo de transmissão de informação de usuário 504, um armazenamento de dados de informação de usuário 506, um módulo de autorização 508, um módulo de validação 510 e um módulo de recibo 512.

[0066] O módulo de autenticação 502 pode ser configurado para a execução de um processo de autenticação mútua com o terminal de pagamento 102. Em particular, o módulo de autenticação 502 pode ser configurado para interação com o módulo de autenticação 402 do terminal de pagamento 102 usando a interface de comunicação segura 218 do dispositivo móvel 104 para execução de um processo de autenticação mútua. Um processo de autenticação mútua de exemplo é descrito em detalhes abaixo.

[0067] O módulo de transmissão de informação de usuário 504

pode ser configurado para a transmissão de uma informação de usuário para o terminal de pagamento 102 através da interface de comunicação segura 218 do dispositivo móvel 104. A informação de usuário pode incluir uma informação de pagamento, tais como números de cartão de crédito ou débito, datas de validade de cartão, códigos de segurança, nomes de titular, dados de EMV® e assim por diante. A informação de usuário também pode incluir uma informação de fidelidade, tais como números de conta de fidelidade, nomes de conta e assim por diante. A informação de usuário também pode incluir um nome de usuário ou outra identificação de usuário, o que pode ser comparado com uma identificação de usuário introduzida por um usuário do terminal de pagamento 102 para se determinar qual de uma pluralidade de conjuntos de informação de usuário recebidos pelo terminal de pagamento está associada àquele usuário. A informação de usuário transmitida pode ser encriptada pelo dispositivo móvel 104, antes de a transmissão para o terminal de pagamento 102 ocorrer usando-se uma chave de sessão gerada durante o processo de autenticação mútua executado pelo módulo de autenticação 502.

[0068] A informação de usuário pode ser armazenada no armazenamento de dados de informação de usuário 506, o qual pode ser mantido no elemento seguro 216 ou em outro dispositivo de armazenamento 212 do dispositivo móvel 104. Um usuário do dispositivo móvel 104 pode adicionar ou remover uma informação a partir do armazenamento de dados de informação de usuário 506 usando-se um aplicativo executado no dispositivo móvel e um ou mais elementos de interface de usuário do dispositivo móvel. Por exemplo, um usuário pode adicionar um cartão de crédito a um aplicativo de "carteira digital" executado pelo dispositivo móvel 104 para o armazenamento da informação de cartão de crédito no armazenamento de dados de informação de usuário 506.

[0069] O módulo de autorização 508 pode ser configurado para o recebimento de vários tipos de informação a partir do terminal de pagamento 102 através da interface de comunicação segura 218 do dispositivo móvel 104. Por exemplo, uma informação de autorização de usuário, tal como um número de identificação pessoal (PIN), uma senha, dados biométricos, tal como uma impressão digital ou uma imagem de face, ou qualquer outra informação que possa ser usada para se garantir que um usuário seja um usuário autorizado dos recursos de pagamento de dispositivo móvel possam ser recebidos a partir do terminal de pagamento 102.

[0070] Quando a informação de usuário enviada para o terminal de pagamento 102 inclui dados para uma pluralidade de tipos de pagamento e/ou uma pluralidade de tipos de fidelidade, o módulo de autorização 508 pode receber uma indicação de tipo de pagamento ou de fidelidade a partir do terminal de pagamento juntamente com a informação de autorização. A indicação de tipo de pagamento ou de fidelidade pode ser usada pelo módulo de validação 510, conforme discutido abaixo. O módulo de autorização 508 pode ser configurado para desencriptar a informação de autorização e/ou a informação de tipo de pagamento ou de fidelidade recebida a partir do terminal de pagamento 102. Em particular, a autorização e/ou a informação de tipo de pagamento ou de fidelidade podem ser desencriptadas usando-se a chave de sessão gerada durante o processo de autenticação mútua conduzido pelo módulo de autenticação 502.

[0071] O módulo de validação 510 pode ser configurado para a geração de um resultado de validação e a transmissão do resultado de validação para o terminal de pagamento 102, usando-se a interface de comunicação segura 218 do dispositivo móvel 104. Em particular, o módulo de validação 510 pode comparar a informação de autorização recebida pelo módulo de autorização 508 com uma informação de

autorização válida ou mestre armazenada no dispositivo móvel 104, por exemplo, no elemento seguro 216 do dispositivo móvel. Quando múltiplos tipos de pagamento e/ou fidelidade são armazenados no dispositivo móvel 104, o módulo de validação 510 pode determinar qual informação de autorização válida de pagamento ou de fidelidade deve ser usada para a comparação, com base na indicação de tipo de pagamento ou de fidelidade recebida pelo módulo de autorização 508. Quando a informação de autorização recebida combina com a informação de autorização válida, um resultado de validação positivo é gerado e transmitido para o terminal de pagamento 102. Quando a informação de autorização recebida não combina com a informação de autorização válida, um resultado de validação negativo é gerado e transmitido para o terminal de pagamento 102.

[0072] O módulo de recibo 512 pode ser configurado para receber um recibo eletrônico a partir do terminal de pagamento 102 através da interface de comunicação segura 218 do dispositivo móvel 104 (por exemplo, mediante a conclusão bem-sucedida de uma transação). O módulo de recibo 512 também pode ser configurado para a exibição do recibo para um usuário usando um visor eletrônico do dispositivo móvel 104, ou para a transmissão do recibo eletronicamente via e-mail, mensagem de texto ou outras técnicas.

OPERAÇÃO

[0073] Um método de exemplo de condução de uma transação de pagamento com móvel segura e conveniente é ilustrado esquematicamente nas figuras 6 a 7. A figura 6 provê uma visão geral do método da perspectiva do terminal de pagamento 102. Inicialmente, na etapa 602, o terminal de pagamento 102 inicia e completa um processo de autenticação mútua com o dispositivo móvel 104 que está ao alcance, ou completa um processo de autenticação mútua iniciado pelo dispositivo móvel 104. Em particular, o módulo de autenticação 402

do terminal de pagamento 102 coopera com o módulo de autenticação 502 do dispositivo móvel 104 para completar um processo de autenticação mútua. Na etapa 604, o módulo de recebimento de informação de usuário 404 do terminal de pagamento 102 recebe uma informação de usuário encriptada a partir do módulo de transmissão de informação de usuário 504 do dispositivo móvel 104. Na etapa 606, o terminal de pagamento 102 desencripta a informação de usuário usando uma chave de sessão gerada na etapa 602. A informação de usuário então é armazenada na etapa 608 na biblioteca de informação de usuário 410 do terminal de pagamento 102. Se nenhuma requisição de transação for recebida em um período de tempo predeterminado, ou se uma comunicação cessar entre o dispositivo móvel 104 e o terminal de pagamento 102, a informação de usuário armazenada no terminal de pagamento poderá ser apagada.

[0074] Na etapa 610, o módulo de recebimento de requisição de transação 408 do terminal de pagamento 102 recebe uma requisição de transação a partir de um usuário. Se múltiplos conjuntos de informação de usuário forem armazenados na biblioteca 410 na etapa 612, o módulo de alerta ao usuário 412 alertará ao usuário quanto a uma identificação de usuário na etapa 614 e receberá a identificação de usuário na etapa 616. Se múltiplos tipos de pagamento e/ou de fidelidade estiverem armazenados para o usuário na etapa 618, o módulo de alerta ao usuário 412 alertará ao usuário quanto a uma indicação de tipo de pagamento ou de fidelidade na etapa 620, e receberá a indicação de tipo de pagamento ou de fidelidade na etapa 622. Na etapa 624, o módulo de alerta ao usuário 412 alerta ao usuário quanto a uma informação de autorização e recebe a informação de autorização na etapa 626. O módulo de autorização 414 então encripta a informação de autorização e a envia para o módulo de autorização 508 do dispositivo móvel 104 na etapa 628. Na etapa 630, o módulo de

validação 416 do terminal de pagamento 102 recebe um resultado de validação a partir do módulo de validação 510 do dispositivo móvel 104. Se o resultado de validação for positivo na etapa 632, o módulo de processamento de transação 418 do terminal de pagamento 102 completará a transação nível de água estático etapa 634. Se o resultado de validação for negativo na etapa 632, o módulo de processamento de transação 418 negará a transação ou tentará de novo o processo de autenticação na etapa 636. Quando uma transação é concluída, o módulo de recibo 420 pode gerar um recibo na etapa 638 e a informação de usuário armazenada no terminal de pagamento 102 pode ser apagada na etapa 640.

[0075] A figura 7 provê uma visão geral do método da perspectiva do dispositivo móvel 104. Inicialmente, na etapa 702, o dispositivo móvel 104 inicia e completa um processo de autenticação mútua com um terminal de pagamento 102 que está no alcance, ou completa um processo de autenticação mútua iniciado pelo terminal de pagamento 102. Em particular, o módulo de autenticação 502 do dispositivo móvel 104 coopera com o módulo de autenticação 402 do terminal de pagamento 102 para se completar um processo de autenticação mútua. Na etapa 704, o módulo de transmissão de informação de usuário 504 encripta uma informação de usuário armazenada no armazenamento de dados de informação de usuário 506 do dispositivo móvel 104 usando uma chave de sessão gerada na etapa 702. O módulo de transmissão de informação de usuário 504 envia a informação de usuário encriptada para o módulo de recebimento de informação de usuário 404 do terminal de pagamento 102 na etapa 706. Na etapa 708, o módulo de autorização 508 do dispositivo móvel 104 recebe uma informação de autorização a partir do módulo de autorização 414 do terminal de pagamento 102. A informação de autorização é desencriptada na etapa 710 usando-se a chave de sessão gerada na etapa 702. Se múltiplos

tipos de pagamento e/ou tipos de fidelidade forem armazenados no armazenamento de dados de informação de usuário 506 na etapa 712, o módulo de autorização 508 do dispositivo móvel 104 receberá uma indicação de tipo de pagamento ou de fidelidade a partir do módulo de autorização 414 do terminal de pagamento 102 na etapa 714. Na etapa 716, o módulo de validação 510 do dispositivo móvel 104 compara a informação de autorização recebida com uma informação de autorização armazenada para o tipo indicado de pagamento ou de fidelidade. Se uma combinação não for encontrada, o módulo de validação 510 do dispositivo móvel 104 enviará um resultado de validação positivo para o 416 do terminal de pagamento 102 na etapa 718. Se nenhuma combinação for encontrada, o módulo de validação 510 do dispositivo móvel 104 enviará um resultado de validação negativo para o módulo de validação 416 do terminal de pagamento 102 na etapa 718. Quando uma transação é completada de forma bem-sucedida, ou em qualquer outra situação na qual um recibo é gerado, o recibo pode ser recebido pelo módulo de recibo 512 do dispositivo móvel 104 na etapa 720 e exibido para o usuário na etapa 722.

[0076] O método das figuras 6 a 7 assim pode permitir que o terminal de pagamento 102 e o dispositivo móvel 104 da figura 1 se engajem e completem uma transação de pagamento com móvel segura e conveniente.

PROCESSO DE AUTENTICAÇÃO MÚTUA

[0077] Em um ou mais dos sistemas e métodos descritos acima, um processo de autenticação de duas vias ou mútuo é usado para se garantir que o dispositivo móvel transfira uma informação de consumidor sensível apenas para um terminal de pagamento autenticado de confiança e para se garantir que o terminal de pagamento apenas aceite pagamentos de transação a partir de um dispositivo móvel autenticado de confiança. Uma informação de consumidor sensível pode ser

encriptada entre o dispositivo móvel e o terminal de pagamento para a provisão de uma interceptação por partes maliciosas.

[0078] Qualquer um de uma variedade de processos de autenticação mútua pode ser usado para a obtenção deste resultado. O processo de autenticação mútua em algumas modalidades pode envolver apenas uma única troca entre o terminal de pagamento 102 e o dispositivo móvel 104 (por exemplo, uma requisição de autenticação transmitida a partir do dispositivo móvel 104 para o terminal de pagamento 102 e uma resposta de autenticação transmitida a partir do terminal de pagamento 102 para o dispositivo móvel 104). Para começar este processo, o dispositivo móvel 104 envia uma requisição de autenticação para o terminal de pagamento 102. A requisição de autenticação pode incluir uma chave pública específica de dispositivo encriptada do dispositivo móvel 104 e um número randômico R1 encriptado pela chave privada do dispositivo móvel. A requisição também pode incluir um identificador único que especifica a cadeia de chaves públicas em uma hierarquia de confiança requerida para a desencriptação da chave pública do dispositivo móvel 104.

[0079] Mediante o recebimento da requisição de autenticação, o terminal de pagamento 102 pode usar um conjunto de chaves públicas pré-autenticadas para a desencriptação da chave pública do dispositivo móvel 104, o que então pode ser usado para a desencriptação o número randômico R1. Caso contrário, o terminal de pagamento 102 pode usar chaves públicas mais altas na hierarquia de confiança ou tentar obter a chave pública requisitada (por exemplo, por uma rede). O terminal de pagamento 102 então pode gerar uma chave de sessão Si com base no número randômico R1 e um número randômico R2 gerado pelo terminal de pagamento, bem como uma soma de verificação CHKS1 da chave de sessão. A chave de sessão Si pode ser encriptada pela chave pública do dispositivo móvel, de modo que apenas a chave privada armazenada

no elemento seguro 216 do dispositivo móvel possa ser usada para a desencriptação e a obtenção da chave de sessão Si. A soma de verificação CHKS1 pode ser encriptada usando-se a chave privada específica do próprio dispositivo do terminal de pagamento. O terminal de pagamento 102 então pode enviar uma resposta de autenticação para o dispositivo móvel 104 que inclui uma chave pública específica de dispositivo encriptada do terminal de pagamento 102 e a chave de sessão encriptada Si e a soma de verificação CHKS1. A requisição também pode incluir um identificador único que especifica a cadeia de chaves públicas requeridas para a desencriptação da chave pública do terminal de pagamento 102.

[0080] Mediante o recebimento da resposta de autenticação, o dispositivo móvel 104 pode usar um conjunto de chaves públicas pré-autenticadas para a desencriptação da chave pública do terminal de pagamento 102, o que então pode ser usado para a desencriptação da soma de verificação CHKS1. Caso contrário, o dispositivo móvel 104 pode usar as chaves públicas mais altas na hierarquia de confiança ou tentar obter a chave pública requisitada (por exemplo, por uma rede). O dispositivo móvel 104 também pode desencriptar a chave de sessão Si usando sua chave privada específica de dispositivo própria. Se a soma de verificação CHKS1 e a chave de sessão Si combinarem, o dispositivo móvel 104 e o terminal de pagamento 102 estarão de posse da chave de sessão acordada Si, e o processo de autenticação mútua é concluído. A chave de sessão Si então pode ser usada para a encriptação e a desencriptação de dados de usuário transmitidos entre o dispositivo móvel 104 e o terminal de pagamento 102.

[0081] Um processo de autenticação mútua de exemplo, o qual pode ser usado nos sistemas e métodos expostos aqui é detalhado no Pedido U.S. Nº 13/890.734, depositado em 9 de maio de 2013 e intitulado SYSTEMS AND METHODS FOR SECURE

COMMUNICATION, o qual é desse modo incorporado aqui como referência em sua totalidade.

[0082] A figura 8 ilustra uma hierarquia de confiança de exemplo 800, a qual pode ser usada no processo de autenticação mútua descrito acima. Conforme mostrado, a hierarquia 800 pode incluir um certificado de raiz 802 que indica uma autoridade de certificado de raiz padrão da indústria (CA de Raiz). Os CAs de Raiz de exemplo incluem VeriSign, GlobalSign, DigiCert e similares. O certificado de raiz 802 forma a raiz de confiança para a hierarquia de certificado 800, e pode ser um certificado de chave pública não assinado ou um certificado autoassinado. O valor de confiança do certificado de raiz 802 pode ser estabelecido por uma distribuição física segura, por exemplo, durante a produção do terminal de pagamento 102. Por conveniência de descrição, o certificado de raiz 802 é referido aqui como um certificado de nível 1 ou "L1". Será apreciado que a hierarquia 800 pode incluir uma pluralidade de certificados de L1, por exemplo, emitidos a partir de uma pluralidade de CAs de Raiz diferentes.

[0083] A hierarquia de certificado também pode incluir um ou mais níveis de certificados subordinados, os quais são assinados por uma autoridade de certificado superior e, desse modo, herdam o valor de confiança da autoridade de certificado superior. Na modalidade ilustrada, por exemplo, a hierarquia 800 inclui um ou mais certificados de rede de terminal de pagamento 804 emitidos a partir de redes de pagamento, tais como bancos de emissão de cartão, adquirentes ou outros processadores de pagamento. A hierarquia ilustrada 800 também inclui um ou mais certificado de concessionária de móvel 806 emitidos a partir de concessionárias de móveis. Por conveniência de descrição, os certificados de rede de terminal de pagamento 804 e os certificados de concessionária de móvel 806 são referidos aqui como certificado de nível 2 ou "L2". Os certificados de L2 são imediatamente subordinados

aos certificados de L1, e, portanto, podem ser assinados pela CA de Raiz para herdarem o valor de confiança do CA de Raiz.

[0084] A hierarquia também pode incluir certificados os quais são subordinados aos certificados de L2. Na modalidade ilustrada, por exemplo, a hierarquia 800 inclui um ou mais certificados de vendedor de terminal de pagamento 808 emitidos a partir dos fabricantes ou distribuidores de terminais de pagamento. A hierarquia 800 também pode incluir um ou mais certificados de vendedor de dispositivo móvel 810 emitidos a partir de fabricantes ou distribuidores de dispositivos móveis. Por conveniência de descrição, os certificados de vendedor de terminal de pagamento 808 e os certificados de vendedor de dispositivo móvel 810 são referidos aqui como certificados de nível 3 ou "L3". Os certificados de L3 são subordinados imediatamente aos certificados de L2, e, portanto, podem ser assinados por uma autoridade de certificado de L2 para herdarem o valor de confiança da autoridade de certificado de L2.

[0085] A hierarquia 800 também pode incluir um certificado específico de dispositivo 812 único para o terminal de pagamento individual e um certificado específico de dispositivo 814 único para o dispositivo móvel individual. Por conveniência de descrição, os certificados específicos de dispositivo são referidos aqui como certificados de nível 4 ou "L4". Os certificados de L4 podem ser assinados por uma autoridade de certificado de L3, para herdarem um valor de confiança de autoridade de certificado de L3.

[0086] Os certificados de raiz 802, os certificados de rede de terminal de pagamento 804, os certificados de vendedor de terminal de pagamento 808 e o certificado de terminal de pagamento 812 podem ser referidos como certificados de "lado de terminal". Os certificados de raiz 802, os certificados de concessionária de móvel 806, os certificados de vendedor de dispositivo móvel 810 e o certificado de dispositivo

móvel 814 podem ser referidos como certificados de "lado de móvel". Os certificados podem ser referidos como "certificados superiores", "certificados mais superiores", "certificados inferiores", "certificados mais inferiores", e assim por diante, com base em sua posição na hierarquia 800 e no certificado cuja perspectiva está sendo descrita. Por exemplo, a partir da perspectiva de um certificado de L4, um certificado de L3 pode ser referido como um certificado superior, e um certificado de L2 pode ser referido como um certificado mais superior. Da mesma forma, da perspectiva de um certificado de L4, um certificado de L2 pode ser referido como um certificado superior e um certificado de L1 pode ser referido como um certificado mais superior. Embora uma hierarquia de certificado de quatro níveis 800 seja mostrada e descrita aqui, será apreciado que a hierarquia pode incluir qualquer número de níveis.

[0087] Em algumas modalidades, a hierarquia de certificado 800 pode ser parte de uma infraestrutura de chave pública (PKI), por exemplo, de acordo com o padrão da indústria X.509. Uma PKI usa pares de chave pública / chave privada para encriptar e desencriptar de forma segura uma informação. Uma chave pública pode ser distribuída livremente e pode ser usada para a encriptação da informação. Para a desencriptação da informação, contudo, uma parte deve possuir uma chave privada associada à chave pública. Um algoritmo de encriptação de chave pública / chave privada de exemplo é o sistema de criptografia RSA. Um certificado digital pode incluir uma chave pública e uma assinatura digital. A assinatura digital é criada usando-se uma chave privada de uma parte, de modo que qualquer um com acesso à chave pública da parte possa provar que o signatário teve acesso a chave privada da parte e, portanto, que a assinatura é autêntica.

[0088] Assim, no exemplo acima, a CA de Raiz armazena uma chave privada em uma localização altamente segura. O certificado de raiz 802 inclui a chave pública que corresponde à chave privada e a

assinatura digital assinada pela CA de Raiz usando a chave privada. Um certificado de raiz bom conhecido 802 pode ser instalado em um ambiente controlado (por exemplo, durante a fabricação), de modo que o certificado possa ser de confiança. Outros certificados no sistema podem ser de confiança ou autenticados com base em um sistema hierárquico de chaves criptográficas e assinaturas digitais que fazem um rastreamento de volta para o certificado de raiz, conforme será apreciado por aqueles versados na técnica.

[0089] No processo de autenticação mútua acima, cada parte pode verificar a chave pública da outra usando a hierarquia de certificado que faz um rastreamento de volta para uma autoridade de confiança de raiz comum. Em particular, o terminal de pagamento 102 e o dispositivo móvel 104 podem trocar suas respectivas chaves públicas no tempo de rodada, desde que ambos os lados possam fazer um rastreamento da dada hierarquia de certificado para um CA de Raiz de confiança comum.

[0090] A figura 9 ilustra uma hierarquia de confiança alternativa 900, a qual pode ser usada em algumas modalidades do processo de autenticação mútua. Na modalidade da figura 9, o terminal de pagamento 102 e o dispositivo móvel 104 pode eliminar a hierarquia de certificado PKI pelo pré-carregamento da hierarquia de chave pública de confiança, ao invés disso. Em particular, ao invés de se manter a hierarquia CA, cada lado tem seu próprio sistema de gerenciamento de segurança 902, 904 alojado, e é responsável pela assinatura da chave pública específica de dispositivo única (a chave pública específica para o terminal de pagamento individual 102 ou a chave pública específica para o terminal de pagamento individual 102) usando sua própria chave de raiz. Ambos o vendedor / fabricante de terminal de pagamento e o vendedor / fabricante de dispositivo móvel podem trocar sua chave pública de raiz por uma rede 906 (por exemplo, a Internet), por exemplo, após o terminal de pagamento 102 e o dispositivo móvel 104 terem

detectado cada outro no alcance de comunicações, e pré-carregar a(s) dada(s) chave(s) pública(s) para a unidade (terminal de pagamento ou dispositivo móvel) em uma preparação para uma transação eventual. No tempo de rodada (ou quando o consumidor estiver iniciando a transação no terminal de pagamento), o terminal de pagamento pode simplesmente autenticar a dada chave pública assinada com a dada chave pública de raiz. Em algumas modalidades, o sistema de chave pública PKI pré-carregada 900 da figura 9 pode ser menos dispendioso de manter do que a hierarquia de certificado PKI completa 900 da figura 8.

VANTAGENS / EFEITOS TÉCNICOS

[0091] Os sistemas e métodos expostos aqui podem produzir várias vantagens e/ou efeitos técnicos.

[0092] Por exemplo, em algumas modalidades, um processo de autenticação mútua assegura que o dispositivo móvel transfira uma informação de usuário sensível apenas para um terminal de pagamento autenticado de confiança, e que o terminal de pagamento apenas aceite pagamentos de transação a partir de um dispositivo móvel autenticado de confiança. Uma informação de usuário sensível pode ser encriptada entre o dispositivo móvel e o terminal de pagamento, para se evitar uma interceptação por partes maliciosas.

[0093] A título de exemplo adicional, em algumas modalidades, a informação de consumidor (por exemplo, dados de pagamento e fidelidade) é transferida para o terminal de pagamento automaticamente, sem qualquer interação de usuário com o dispositivo móvel. Assim sendo, o tempo perdido e a inconveniência associados à localização e ao alcance do dispositivo móvel, a abertura de aplicativos ou a ativação de recursos de pagamento e assim por diante são eliminados. Um usuário pode completar uma transação inteira sem mesmo tocar ou interagir com o dispositivo móvel. Em outras palavras,

uma transação pode ser completada sem qualquer interação física entre o usuário e o dispositivo móvel antes, durante ou após a transação. O processo de pagamento também pode ser expedito, uma vez que uma informação de consumidor de usuário já está armazenada no terminal de pagamento no momento em que o usuário inicia uma transação, poupando tempo que, de outra forma, seria requerido para a autenticação e a transferência da informação.

[0094] Como ainda outro exemplo, em algumas modalidades, preocupações referentes ao uso de dispositivos móveis nas proximidades de um posto de combustível podem ser aliviadas, uma vez que o dispositivo móvel pode ser mantido em um lugar seguro por toda uma transação de abastecimento de combustível.

[0095] Embora vários métodos expostos aqui possam ser mostrados em relação a fluxogramas ou diagramas de sequência, deve ser notado que qualquer ordenação de etapas de método implicadas por esses fluxogramas, diagramas de sequência ou a descrição dos mesmos não é para ser construída como limitando o método para execução das etapas naquela ordem. Ao invés disso, as várias etapas de cada um dos métodos expostos aqui podem ser executadas em qualquer uma de uma variedade de sequências. Além disso, como os fluxogramas ilustrados e os diagramas de sequência são meramente modalidades de exemplo, vários outros métodos que incluem etapas adicionais ou incluir menos etapas do que ilustrado também estão no escopo da presente exposição.

[0096] Esta descrição por escrito usa exemplos para exposição da invenção, incluindo o melhor modo, e também para se permitir que qualquer pessoa versada na técnica pratique a invenção, incluindo fazer e usar quaisquer dispositivos ou sistemas e executando quaisquer métodos incorporados. O escopo patenteável da invenção é definido pelas reivindicações, e pode incluir outros exemplos que ocorrem

àqueles versados na técnica. Pretende-se que esses outros exemplos estejam no escopo das reivindicações, se eles tiverem elementos estruturais que não diferem da linguagem literal das reivindicações, ou se eles incluírem elementos estruturais equivalentes com diferenças não substanciais a partir das linguagens literais das reivindicações.

REIVINDICAÇÕES

1. Terminal caracterizado pelo fato de compreender:

um transceptor sem fio configurado para comunicação de forma sem fio com o dispositivo móvel (104);

um dispositivo de entrada configurado para receber uma entrada a partir de um usuário do terminal;

um dispositivo de armazenamento (212) configurado para armazenamento de uma informação de usuário associada a um ou mais usuários; e

pelo menos um processador acoplado ao transceptor sem fio, ao dispositivo de entrada e ao dispositivo de armazenamento (212), o processador sendo programado para:

a condução de um processo de autenticação mútua com um dispositivo móvel (104) para a obtenção de uma chave de sessão;

o recebimento de uma informação de usuário a partir do dispositivo móvel (104) através do transceptor sem fio, a referida informação de usuário sendo encriptada pela chave de sessão;

o armazenamento de uma informação de usuário recebida no dispositivo de armazenamento (212);

após o processo de autenticação mútua ser conduzido e após a informação de usuário recebida ser armazenada no dispositivo de armazenamento (212):

- o recebimento de uma requisição para iniciação de uma transação a partir de um usuário através do dispositivo de entrada;

- o alerta ao usuário quanto a uma informação de autorização;

- o recebimento de uma informação de autorização a partir do usuário através do dispositivo de entrada;

- a encriptação da informação de autorização usando-se a chave de sessão;

- o envio da informação de autorização encriptada para o dispositivo móvel (104) através do transceptor sem fio;

- o recebimento de um resultado de validação a partir do dispositivo móvel (104) através do transceptor sem fio; e

- quando o resultado de validação é positivo, a conclusão de uma transação requisitada pelo usuário usando-se a informação de usuário armazenada.

2. Terminal, de acordo com a reivindicação 1, caracterizado pelo fato de a informação de usuário ser recebida automaticamente, sem qualquer interação entre o usuário e o dispositivo móvel (104).

3. Terminal, de acordo com a reivindicação 1, caracterizado pelo fato de a interação de usuário com o dispositivo móvel (104) não ser requerida, antes, durante ou depois de concluir a transação.

4. Terminal, de acordo com a reivindicação 1, caracterizado pelo fato de o terminal compreender um terminal de ponto de venda.

5. Terminal, de acordo com a reivindicação 1, caracterizado pelo fato de o processador ser programado para enviar um recibo eletrônico para o dispositivo móvel (104) através do transceptor sem fio, o recibo eletrônico sendo encriptado usando-se a chave de sessão.

6. Terminal, de acordo com a reivindicação 1, caracterizado pelo fato de o processador ser programado para apagar uma informação de usuário recebida a partir do dispositivo móvel (104), se o terminal perder uma comunicação com o referido dispositivo móvel (104) ou se um tempo predeterminado decorrer sem um usuário do referido dispositivo móvel (104) iniciar uma transação.

7. Terminal, de acordo com a reivindicação 1, caracterizado pelo fato de o processador ser programado para receber uma identificação de usuário a partir do usuário e para enviar a informação de autorização encriptada apenas para um dispositivo móvel (104) associado ao dispositivo de armazenamento (212) com a referida

identificação de usuário.

8. Terminal, de acordo com a reivindicação 1, caracterizado pelo fato de o processador ser programado para receber pelo menos uma dentre uma indicação de tipo de pagamento e uma indicação de tipo de fidelidade e para enviar a referida indicação para o dispositivo móvel (104) com a informação de autorização encriptada.

9. Terminal, de acordo com a reivindicação 1, caracterizado pelo fato de uma chave criptográfica de um CA de Raiz com o qual o dispositivo móvel (104) e o terminal têm uma relação de confiança ser armazenada no dispositivo de armazenamento (212).

10. Terminal, de acordo com a reivindicação 1, caracterizado pelo fato de uma chave criptográfica de um vendedor móvel com o qual o dispositivo móvel (104) tem uma relação de confiança ser armazenada no dispositivo de armazenamento (212).

11. Dispositivo móvel (104) caracterizado pelo fato de compreender:

um transceptor sem fio configurado para comunicação de forma sem fio com um terminal;

um dispositivo de armazenamento (212) configurado para armazenamento de uma informação de usuário associada a um usuário; e

pelo menos um processador acoplado ao transceptor sem fio e ao dispositivo de armazenamento (212), o processador sendo programado para a execução de uma transação com um terminal por meio de:

- condução de um processo de autenticação mútua com o terminal, para a obtenção de uma chave de sessão;
- encriptação da informação de usuário armazenada no dispositivo de armazenamento (212) usando-se a chave de sessão;
- envio da informação de usuário encriptada para o terminal

através do transceptor sem fio;

- após condução do processo de autenticação mútua e após envio da informação de usuário encriptada para o terminal:

recebimento de uma informação de autorização encriptada a partir do terminal através do transceptor sem fio;

a desencriptação da informação de autorização usando-se a chave de sessão;

a comparação da informação de autorização com uma informação de autorização mestre para a geração de um resultado de validação, o resultado de validação sendo positivo quando uma combinação for encontrada e sendo negativo quando uma combinação não for encontrada; e

o envio do resultado de validação para o terminal através do transceptor sem fio para se facilitar a conclusão da transação pelo terminal.

12. Dispositivo móvel (104), de acordo com a reivindicação 11, caracterizado pelo fato de o processador ser programado para enviar a informação de usuário para o terminal automaticamente, sem qualquer interação entre um usuário e o dispositivo móvel (104).

13. Dispositivo móvel (104), de acordo com a reivindicação 11, caracterizado pelo fato de uma interação de usuário com o dispositivo móvel (104) não ser requerida, antes, durante ou depois de concluir a transação.

14. Dispositivo móvel (104), de acordo com a reivindicação 11, caracterizado pelo fato de o processador ser programado para receber pelo menos uma indicação de tipo de pagamento e uma indicação de tipo de fidelidade a partir do terminal através do transceptor sem fio, e para selecionar uma informação de autorização mestre para a referida comparação, com base na indicação.

15. Dispositivo móvel (104), de acordo com a reivindicação

11, caracterizado pelo fato de uma chave criptográfica de um CA de Raiz, com o qual o dispositivo móvel (104) e o terminal têm uma relação de confiança, ser armazenada no dispositivo de armazenamento (212).

16. Dispositivo móvel (104), de acordo com a reivindicação 11, caracterizado pelo fato de uma chave criptográfica de um vendedor de terminal, com o qual o terminal tem uma relação de confiança, ser armazenada no dispositivo de armazenamento (212).

17. Método para a condução de uma transação móvel conveniente e segura, usando-se um terminal e um dispositivo móvel (104), caracterizado pelo fato de compreender:

automaticamente e sem uma interação de usuário com o terminal ou o dispositivo móvel (104),

a condução de um processo de autenticação mútua, no qual o terminal e o dispositivo móvel (104) autenticam um para cada outro para a obtenção de uma chave de sessão;

o recebimento de uma informação de usuário a partir do dispositivo móvel (104) através de um transceptor sem fio do terminal, a referida informação de usuário sendo encriptada pela chave de sessão; e

o armazenamento da informação de usuário em um dispositivo de armazenamento (212) do terminal;

após condução do processo de autenticação mútua e após armazenamento da informação de usuário no dispositivo de armazenamento (212);

- o recebimento de uma requisição para se iniciar uma transação a partir de um usuário via um dispositivo de entrada do terminal;

- o alerta ao usuário quanto a uma informação de autorização através de um visor eletrônico do terminal;

- o recebimento de uma informação de autorização a partir

do usuário via o dispositivo de entrada;

- a encriptação da informação de autorização usando-se a chave de sessão;

- o envio da informação de autorização encriptada para o dispositivo móvel (104) através do transceptor sem fio;

- o recebimento de um resultado de validação a partir do dispositivo móvel (104) através do transceptor sem fio; e

quando o resultado de validação é positivo, a conclusão da transação requisitada pelo usuário, usando-se a informação de usuário armazenada.

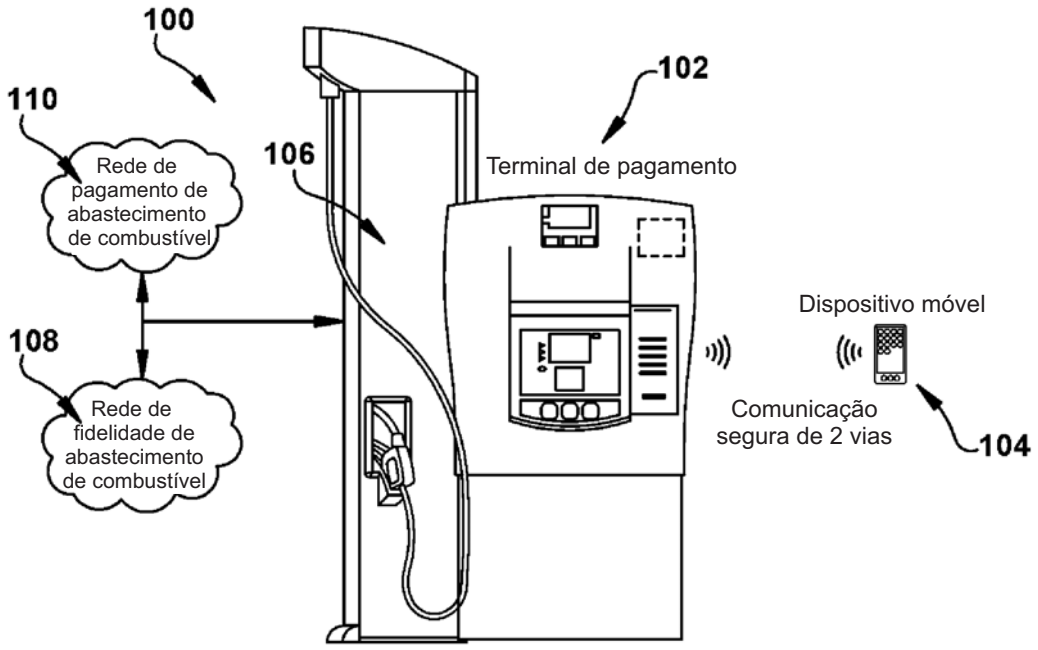
100
110
Rede de pagamento de abastecimento de combustível
108
Rede de fidelidade de abastecimento de combustível
106
102
Terminal de pagamento
Dispositivo móvel
Comunicação segura de 2 vias
104

FIG. 1

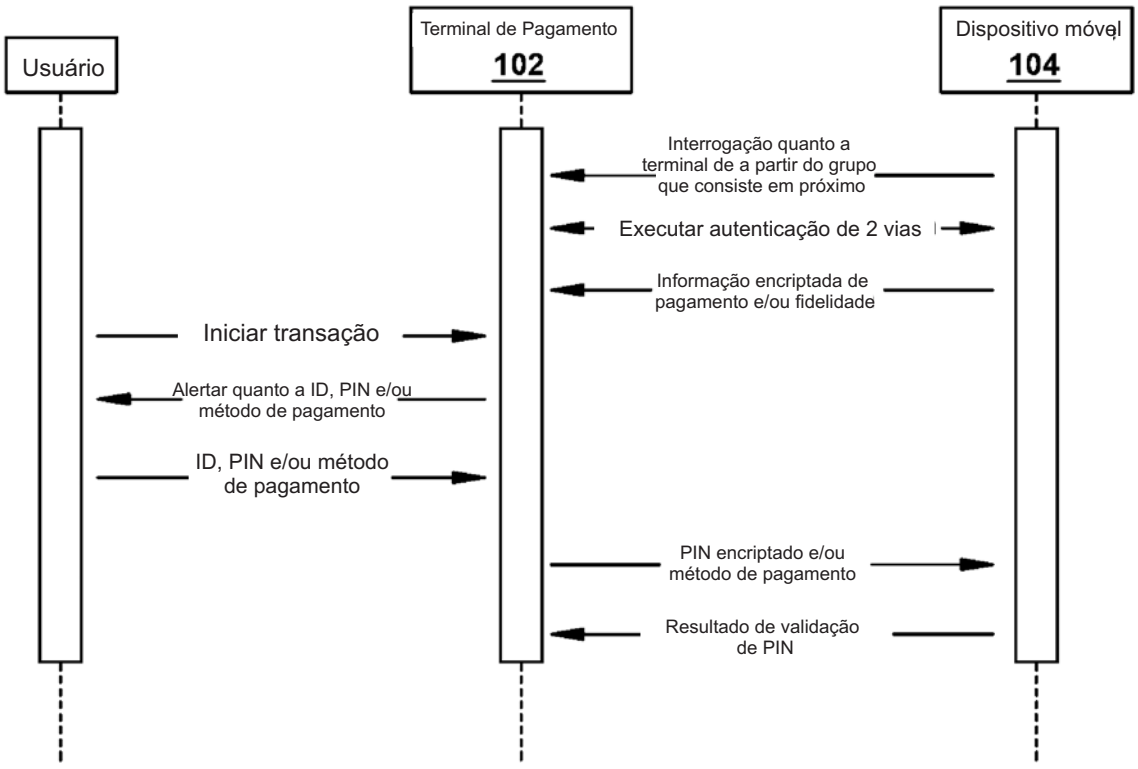
Usuário
Terminal de Pagamento
102
Dispositivo móvel
104
Interrogação quanto a terminal de a partir do grupo que consiste em próximo
Executar autenticação de 2 vias
Informação encriptada de pagamento e/ou fidelidade
Iniciar transação
Alertar quanto a ID, PIN e/ou método de pagamento
ID, PIN e/ou método de pagamento
PIN encriptado e/ou método de pagamento
Resultado de validação de PIN

FIG. 2

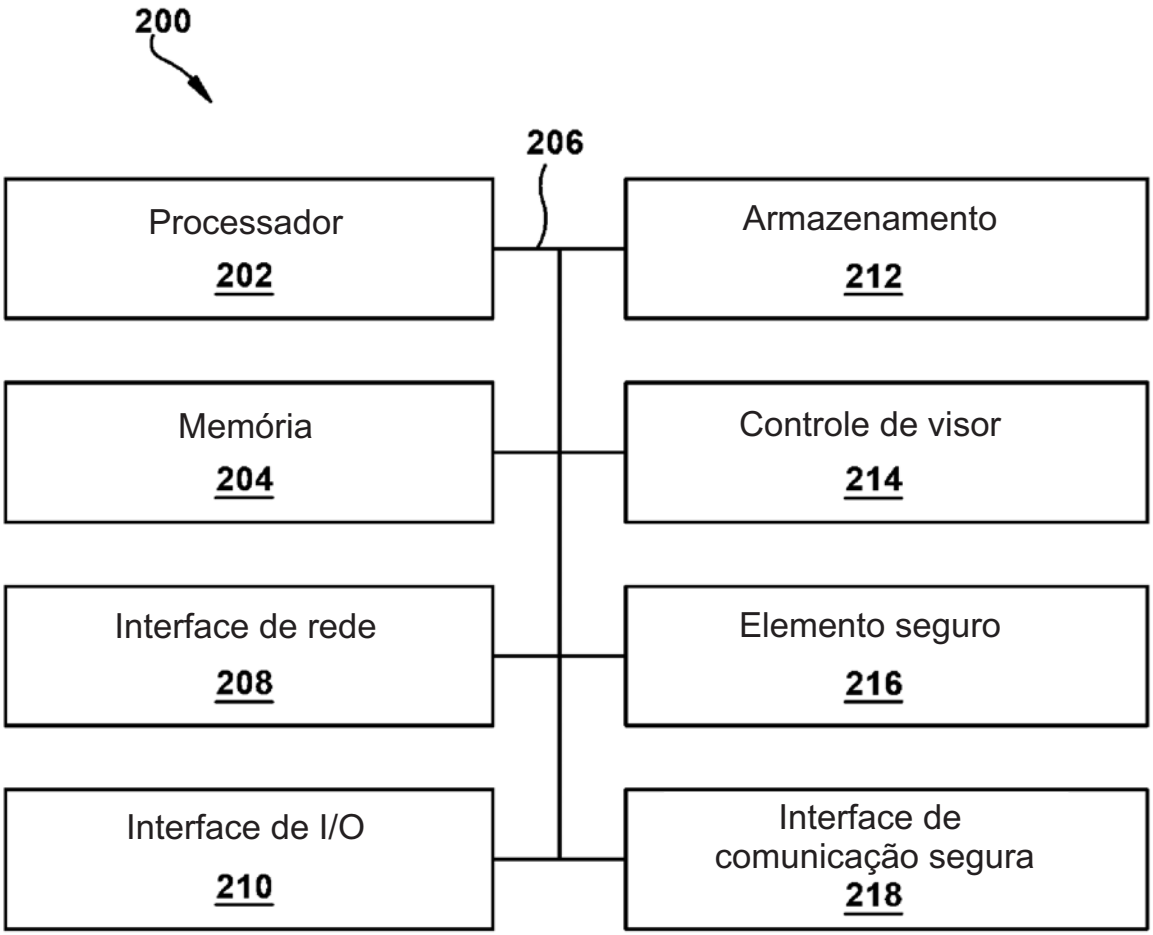
200
206
Processador
202
Armazenamento
212
Memória
204
Controle de visor
214
Interface de rede
208
Elemento seguro
216
Interface de I/O
210
Interface de comunicação segura
218

FIG. 3

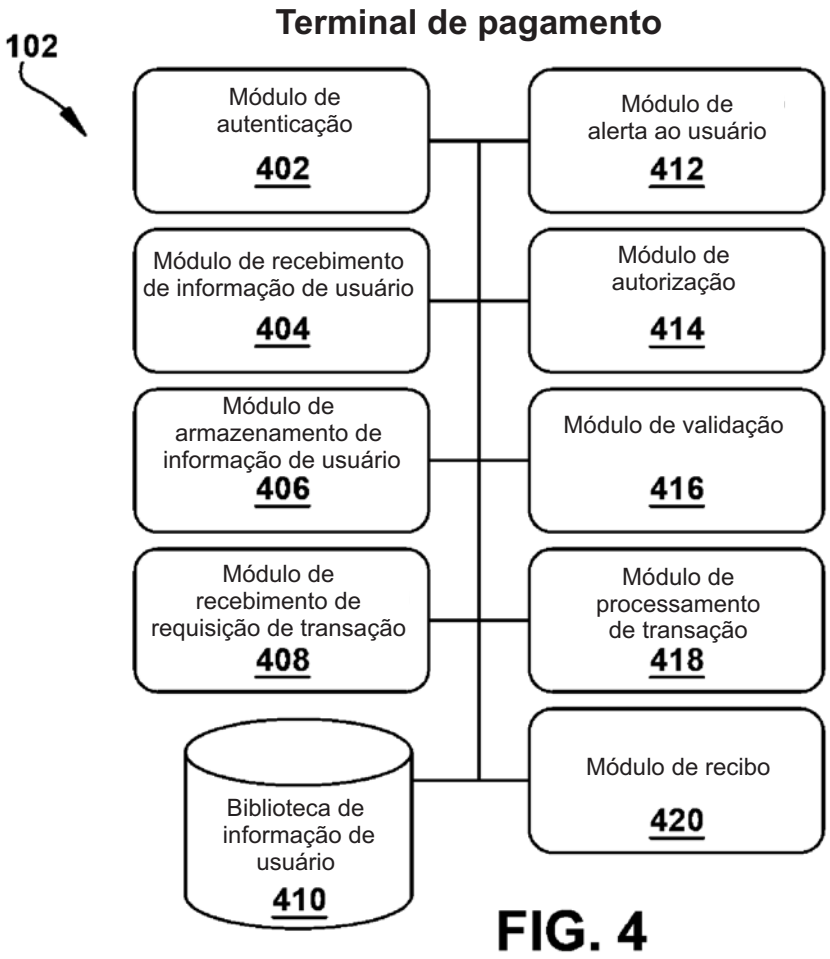
Terminal de pagamento
102
Módulo de autenticação
402
Módulo de recebimento de informação de usuário
404
Módulo de armazenamento de informação de usuário
406
Módulo de recebimento de requisição de transação
408
Biblioteca de informação de usuário
410
Módulo de alerta ao usuário
412
Módulo de autorização
414
Módulo de validação
416
Módulo de processamento de transação
418
Módulo de recibo
420

FIG. 4

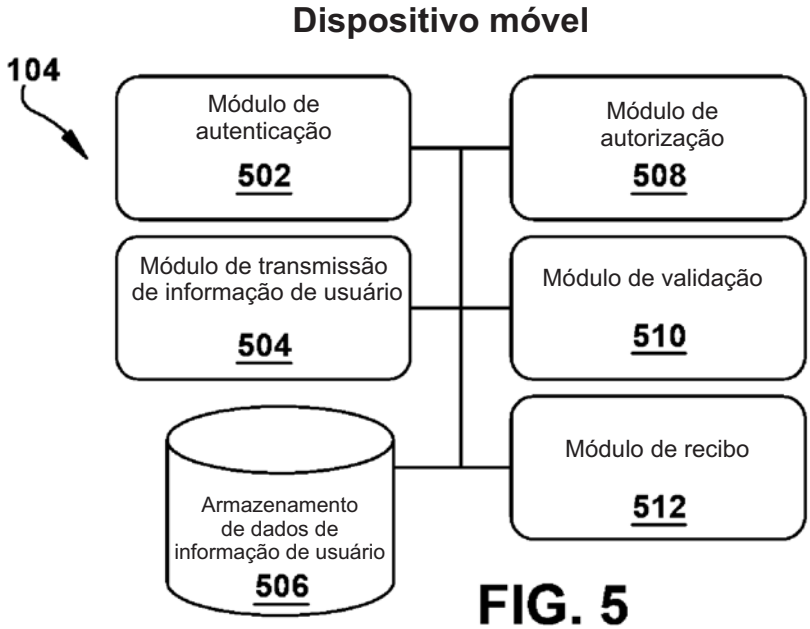
Dispositivo móvel
104
Módulo de autenticação
502
Módulo de transmissão de informação de usuário
504
Armazenamento de dados de informação de usuário
506
Módulo de autorização
508
Módulo de validação
510
Módulo de recibo
512

FIG. 5

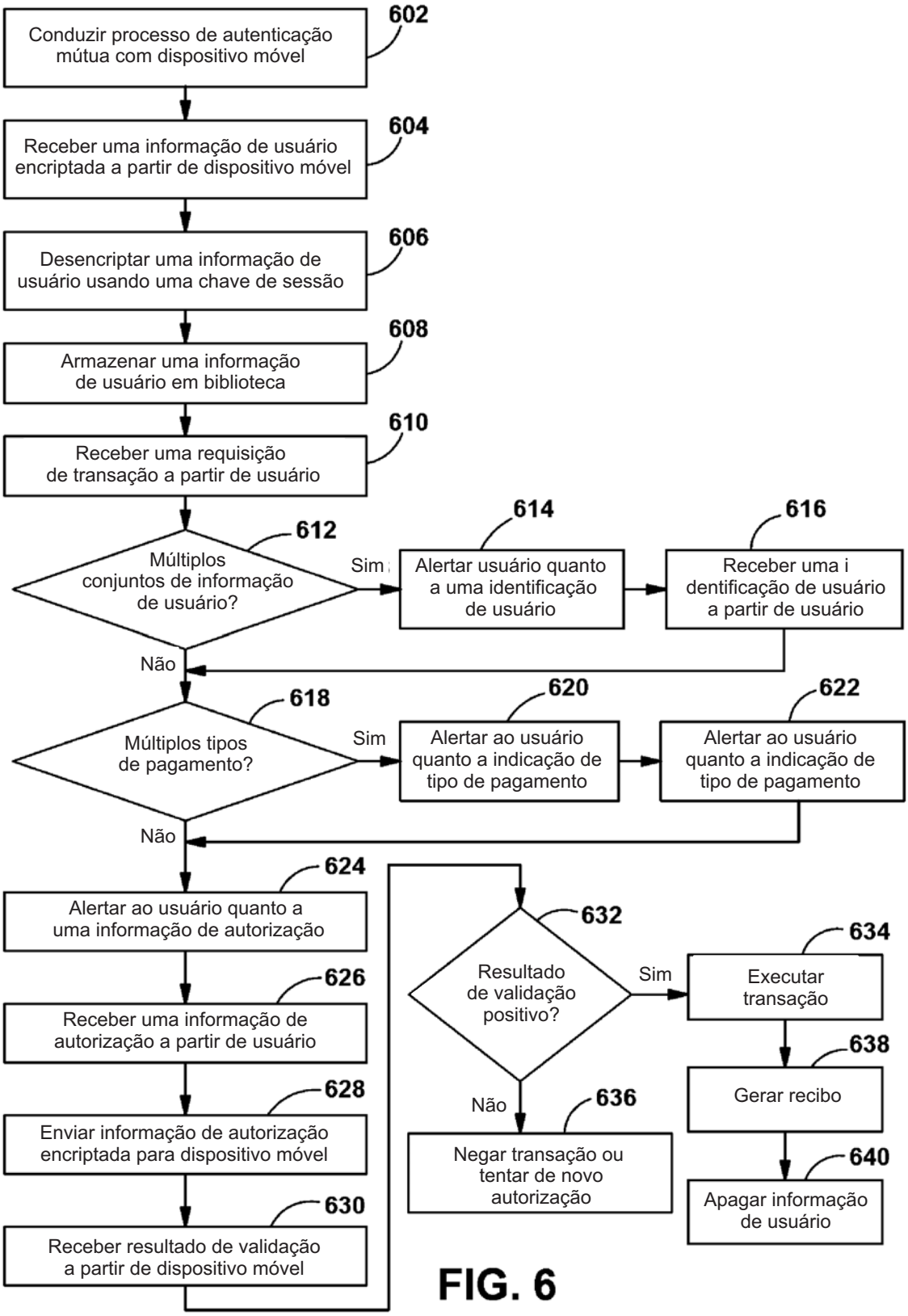
Conduzir processo de autenticação mútua com dispositivo móvel
602
Receber uma informação de usuário encriptada a partir de dispositivo móvel
604
Desencriptar uma informação de usuário usando uma chave de sessão
606
Armazenar uma informação de usuário em biblioteca
608
Receber uma requisição de transação a partir de usuário
610
Múltiplos conjuntos de informação de usuário?
612
Sim
Alertar usuário quanto a uma identificação de usuário
614
Receber uma identificação de usuário a partir de usuário
616
Não
Múltiplos tipos de pagamento?
618
Sim
Alertar ao usuário quanto a indicação de tipo de pagamento
620
Alertar ao usuário quanto a indicação de tipo de pagamento
622
Não
Alertar ao usuário quanto a uma informação de autorização
624
Receber uma informação de autorização a partir de usuário
626
Enviar informação de autorização encriptada para dispositivo móvel
628
Receber resultado de validação a partir de dispositivo móvel
630
Resultado de validação positivo?
632
Sim
Executar transação
634
Gerar recibo
638
Apagar informação de usuário
640
Não
Negar transação ou tentar de novo autorização
636

FIG. 6

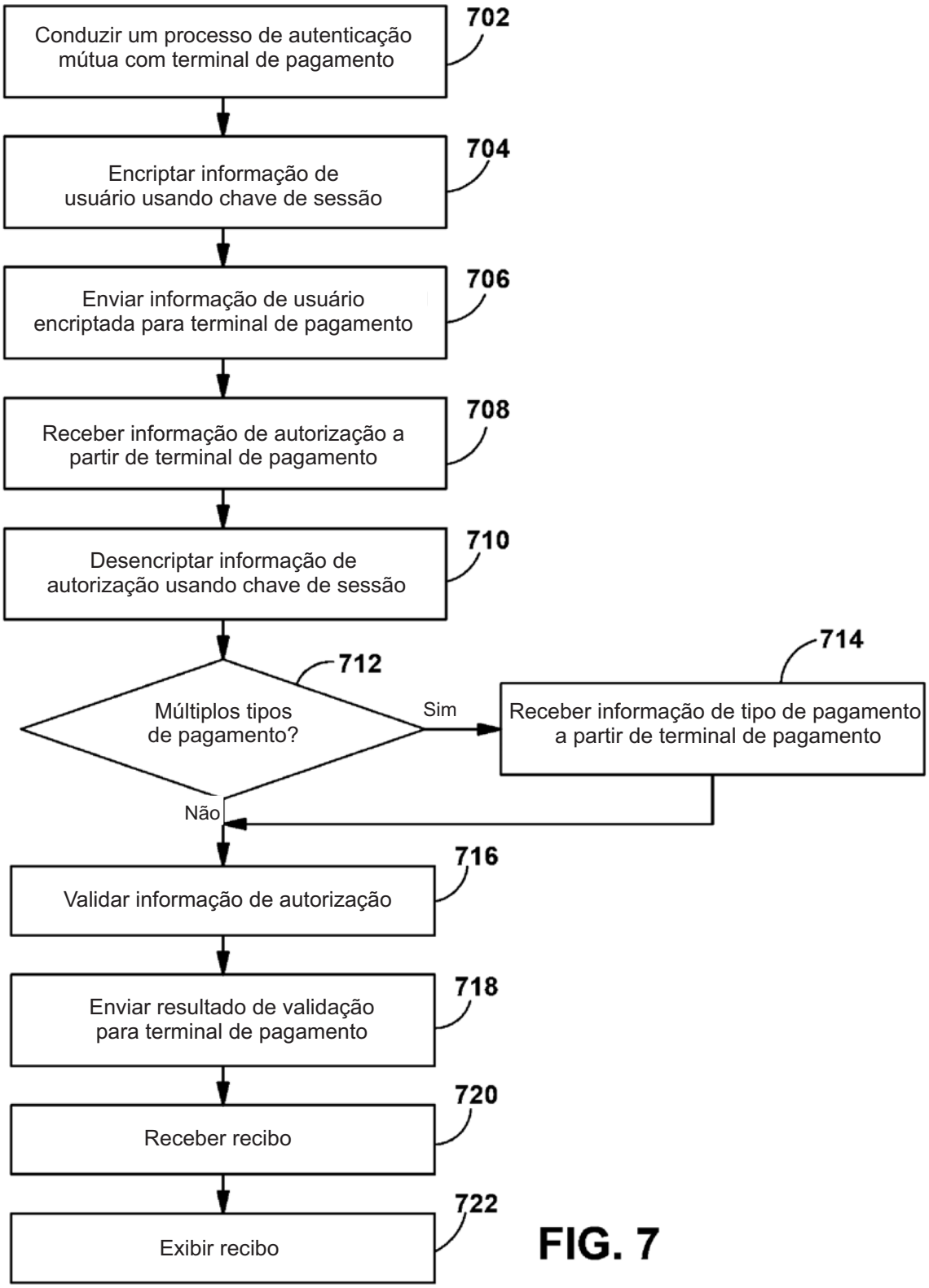
Conduzir um processo de autenticação mútua com terminal de pagamento
702
Encriptar informação de usuário usando chave de sessão
704
Enviar informação de usuário encriptada para terminal de pagamento
706
Receber informação de autorização a partir de terminal de pagamento
708
Desencriptar informação de autorização usando chave de sessão
710
712
Múltiplos tipos de pagamento?
Sim
714
Receber informação de tipo de pagamento a partir de terminal de pagamento
Não
716
Validar informação de autorização
718
Enviar resultado de validação para terminal de pagamento
720
Receber recibo
722
Exibir recibo

FIG. 7

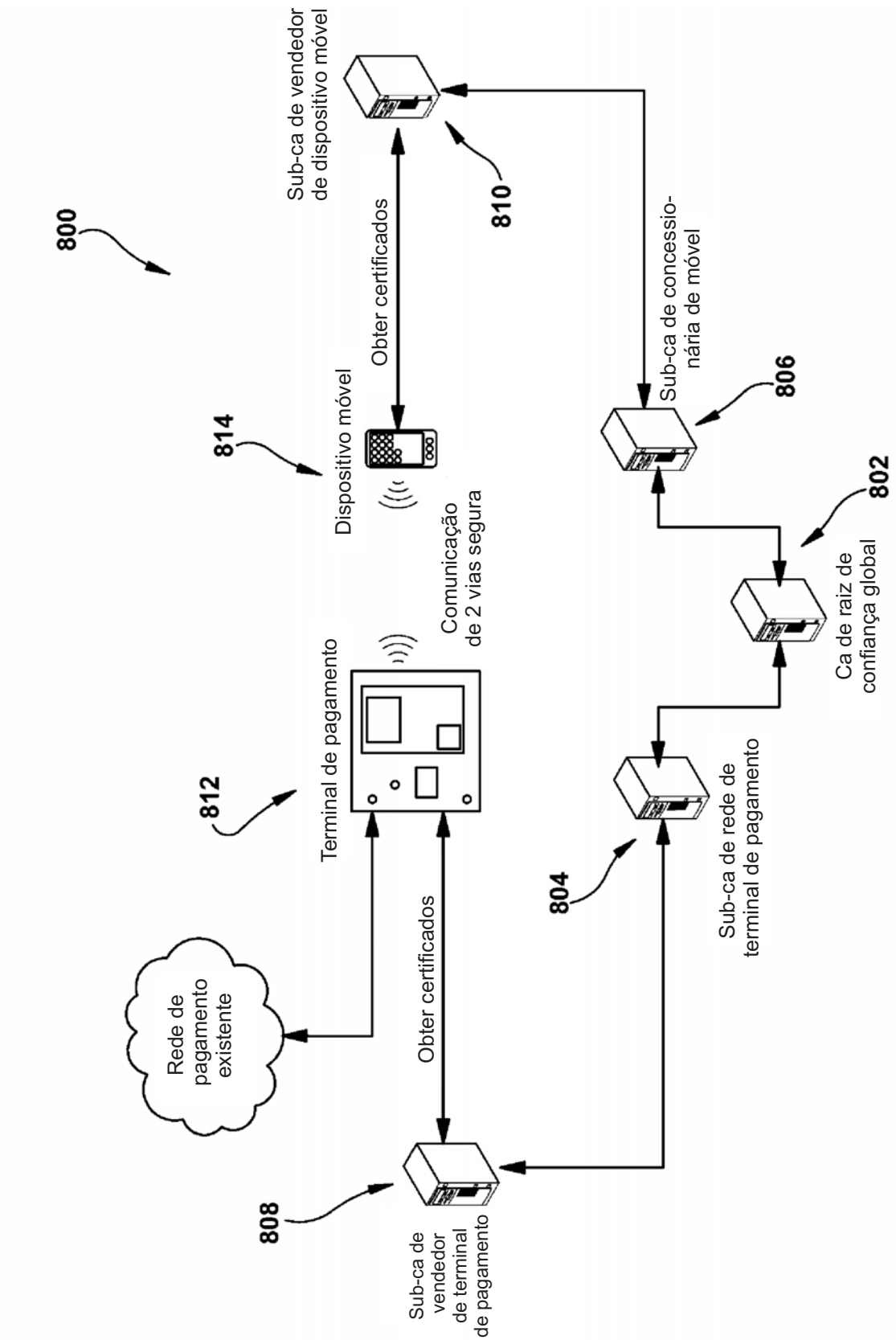
800
Sub-ca de vendedor de dispositivo móvel
810
Obter certificados
814
Dispositivo móvel
Comunicação de 2 vias segura
Sub-ca de concessio-nária de móvel
806
802
Ca de raiz de confiança global
Terminal de pagamento
812
Rede de pagamento existente
Obter certificados
804
Sub-ca de rede de terminal de pagamento
808
Sub-ca de vendedor de terminal de pagamento

FIG. 8

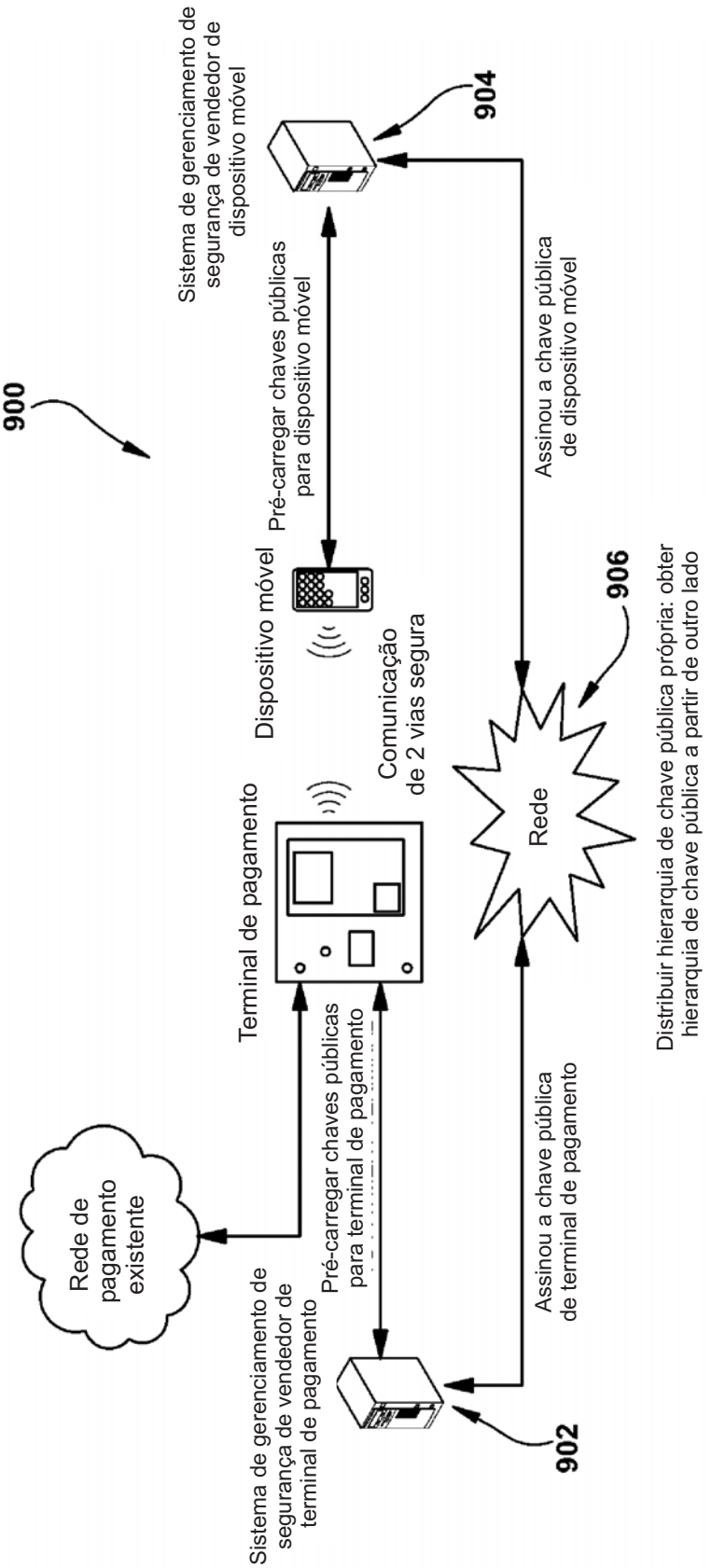
900
Sistema de gerenciamento de segurança de vendedor de dispositivo móvel
904
Pré-carregar chaves públicas para dispositivo móvel
Assinou a chave pública de dispositivo móvel
Dispositivo móvel
Comunicação de 2 vias segura
906
Rede
Terminal de pagamento
Distribuir hierarquia de chave pública própria: obter hierarquia de chave pública a partir de outro lado
Rede de pagamento existente
Sistema de gerenciamento de segurança de vendedor de terminal de pagamento
Pré-carregar chaves públicas para terminal de pagamento
Assinou a chave pública de terminal de pagamento
902

FIG. 9