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

(11) BR 112012007872-0 B1

(22) Data do Depósito: 05/10/2010

(45) Data de Concessão: 22/06/2021

(54) Título: MÉTODO PARA PROPORCIONAR ACESSO A UMA CONTA MANTIDA POR UMA INSTITUIÇÃO, MÉTODO PARA FORNECER CREDENCIAIS DE LOGIN A UM TERMINAL DE TRANSAÇÃO ENVOLVENDO UM DISPOSITIVO MÓVEL E MÉTODO PARA PROPORCIONAR ACESSO A UMA CONTA DE UM USUÁRIO IDENTIFICADO POR IDENTIFICADOR ÚNICO

(51) Int.Cl.: H04L 9/32; H04W 12/06; G06Q 20/10; G06Q 20/12; G06Q 20/38; (...).

(52) CPC: H04L 9/3226; H04W 12/06; G06Q 20/108; G06Q 20/12; G06Q 20/382; (...).

(30) Prioridade Unionista: 05/10/2009 US 61/248,722.

(73) Titular(es): MIRI SYSTEMS, LLC.

(72) Inventor(es): LUDWIK F. ZON; RONALD W. SANDSTROM.

(86) Pedido PCT: PCT US2010051524 de 05/10/2010

(87) Publicação PCT: WO 2011/044161 de 14/04/2011

(85) Data do Início da Fase Nacional: 05/04/2012

(57) Resumo: MÉTODO PARA PROPORCIONAR ACESSO A UMA CONTA MANTIDA POR UMA INSTITUIÇÃO, MÉTODO PARA FORNECER CREDENCIAIS DE LOGIN A UM TERMINAL DE TRANSAÇÃO ENVOLVENDO UM DISPOSITIVO MÓVEL E MÉTODO PARA PROPORCIONAR ACESSO A UMA CONTA DE UM USUÁRIO IDENTIFICADO POR UM IDENTIFICADOR ÚNICO. Um sistema e método para gerar credencial de login de uso limitado associado a uma conta mantida por uma instituição, onde a credencial facilita o acesso seguro à conta.

"MÉTODO PARA PROPORCIONAR ACESSO A UMA CONTA MANTIDA POR UMA INSTITUIÇÃO, MÉTODO PARA FORNECER CREDENCIAIS DE *LOGIN* A UM TERMINAL DE TRANSAÇÃO ENVOLVENDO UM DISPOSITIVO MÓVEL E MÉTODO PARA PROPORCIONAR ACESSO A UMA CONTA DE UM USUÁRIO IDENTIFICADO POR UM IDENTIFICADOR ÚNICO"

REFERÊNCIA RELACIONADA AO PEDIDO

O presente pedido de patente reivindica os benefícios do pedido de patente provisório norte-americano sob o número de série US 61/248,722, intitulado "Electronic Transaction Security System and Method", e depositado em 5 de outubro de 2009, a descrição completa deste é aqui incorporada por referência, como se estabelecido textualmente daqui por diante e confiado para todos os efeitos.

CAMPO DA INVENÇÃO

A presente invenção refere-se genericamente ao processamento das transações com cartão de pagamento. Mais particularmente, a presente invenção refere-se a um sistema e método para aprimorar a segurança das transações com cartão de pagamento.

ANTECEDENTES DA INVENÇÃO

Os cartões de pagamento, tais como, cartões de crédito ou cartões de débito, são comumente utilizados para comprar bens e serviços, pessoalmente ou via telefone ou Internet (*online*). As informações necessárias para iniciar uma transação com cartão de pagamento compreendem tipicamente um número de cartão de pagamento, uma data de expiração do cartão de pagamento e o nome do titular do cartão. Outras informações, como o número de telefone do titular do cartão e endereço podem ser necessárias. Alguns ou todos os dados necessários para efetuar uma transação com cartão de pagamento podem, potencialmente, se tornarem conhecidas a terceiros,

que poderá utilizar as informações sem o conhecimento ou consentimento do titular do cartão.

BREVE DESCRIÇÃO DA INVENÇÃO

A presente invenção reconhece e aborda as considerações precedentes, e outras, das construções e métodos do estado da técnica.

A este respeito, um aspecto da presente invenção refere-se a transações eletrônicas, pagamento de contas, instituições financeiras e sistemas de segurança para os mesmos. Os exemplos de tais assuntos estão contidos nos pedidos de patentes norte-americanos em exame de números US 12/250,416 (intitulado "Electronic Transaction Security System and Method", e depositado em 13 de outubro de 2008) e US 12/713,100 (intitulado "Payment System and Method", e depositado em 25 de fevereiro de 2010), a divulgação completa de cada um desses documentos é aqui incorporada por referência como se estabelecido daqui por diante na íntegra.

Outro aspecto da invenção proporciona um método computadorizado para a geração de um número com tempo limite para o uso em uma transação com cartão de pagamento que envolve um cartão de pagamento emitido para um usuário por uma instituição financeira, em que o cartão de pagamento compreende um número de cartão de pagamento original, o método compreendendo as etapas de fornecer a um processador uma primeira pluralidade de dígitos no número do cartão de pagamento original, onde a primeira pluralidade dos dígitos são dígitos predeterminados associados à instituição financeira, proporcionando ao processador uma data de expiração desejada por meio do qual o número com tempo limite é válido para a aceitação na transação do cartão de pagamento e executando um programa pelo processador para que o programa defina uma primeira pluralidade de dígitos no número com tempo limite para a primeira

pluralidade de dígitos no número do cartão de pagamento original, gerando um primeiro número correspondente a data de expiração desejada, definindo uma segunda pluralidade de dígitos no número com tempo limite para o primeiro número, e liberando o número com tempo limite.

De acordo com outro aspecto, a presente invenção também proporciona um método para aumentar a segurança de uma transação de cartão de pagamento envolvendo um número de cartão de pagamento atribuído a uma conta de usuário por uma instituição financeira, o método compreendendo as etapas de geração de um número com tempo limite compreendendo uma primeira pluralidade de dígitos no número com tempo limite definido para uma primeira pluralidade de dígitos no número do cartão de pagamento associado à instituição financeira e uma segunda pluralidade de dígitos no número com tempo limite definido para um primeiro número correspondente a uma data de expiração desejada, onde o número com tempo limite não é associado com a conta de usuário, transmitindo o número com tempo limite e dados representativos da conta de usuário diferente do número de cartão de pagamento para a instituição financeira, localizando a conta de usuário com base nos dados e validando o número com tempo limite para a transação com base nos dígitos indicando a data de expiração e os dados.

Um aspecto adicional da presente invenção provê um sistema para geração de um número com tempo limite para o uso em uma transação com cartão de pagamento que envolve um cartão de pagamento emitido a um usuário por uma instituição financeira, em que o cartão de pagamento compreende um número de cartão de pagamento original, o sistema compreendendo um dispositivo de processamento e um meio acessível pelo dispositivo de processamento

que compreende instruções quando executadas pelo dispositivo de processamento fazendo com que o dispositivo de processamento realize as etapas de estabelecer uma primeira pluralidade de dígitos no número com tempo limite para uma primeira pluralidade de dígitos no número do cartão de pagamento original, em que a primeira pluralidade de dígitos no número do cartão de pagamento original é dígitos predeterminados associados à instituição financeira, gerando um primeiro número correspondente a uma data de expiração desejada por meio do qual o número com tempo limite é válido para a aceitação na transação do cartão de pagamento, estabelecendo uma segunda pluralidade de dígitos no número com tempo limite para o primeiro número, e liberando o número com tempo limite.

Em outro aspecto, é fornecido um método computadorizado para a identificação de uma conta atribuída a um usuário por uma instituição financeira, em que a conta é atribuída um número de cartão de pagamento, compreendendo as etapas de proporcionar a um dispositivo de processamento informação correspondente a uma transação de cartão de pagamento associada com o usuário, onde uma parte da informação não inclui o número do cartão de pagamento e executando um programa pelo dispositivo de processamento que localiza a conta com base em parte da informação que não inclui o número do cartão de pagamento.

As figuras anexas, que são incorporadas dentro e constituem uma parte desta especificação, ilustram um ou mais realizações da invenção e, juntamente com a descrição, servem para explicar os princípios da invenção.

BREVE DESCRIÇÃO DAS FIGURAS

Uma divulgação completa e permissiva da presente invenção, incluindo o melhor modo do mesmo, dirigida a um técnico no

assunto é estabelecida na especificação, o que faz referência às figuras anexas, nos quais:

A figura 1 é uma ilustração esquemática de um sistema para efetuar uma transação de cartão de pagamento de acordo com uma realização da presente invenção;

A figura 2 é um fluxograma que ilustra um método para codificação e decodificação da informação transmitida a uma instituição financeira, em relação a uma transação de cartão de pagamento de acordo com uma realização da presente invenção;

A figura 3 é um exemplo de interface gráfica de usuário do dispositivo do usuário do sistema mostrado na figura 1, e

As figuras 4, 5, 6, e 7 são fluxogramas que ilustram métodos para codificação e decodificação da informação transmitida a uma instituição financeira, em relação a uma transação de cartão de pagamento de acordo com realizações adicionais da presente invenção.

O uso da repetição dos caracteres de referência na presente especificação e as figuras destinam-se a representar as mesmas ou análogas características ou elementos da invenção.

DESCRIÇÃO DETALHADA DAS REALIZAÇÕES PREFERIDAS

A referência será agora detalhada às realizações preferidas da invenção, um ou mais exemplos dos quais são ilustrados nas figuras anexas. Cada exemplo é fornecido à título de explicação do invento e não limitação da invenção. De fato, será evidente para os técnicos no assunto que modificações e variações podem ser feitas na presente invenção sem se afastar do escopo ou do espírito da mesma. Por exemplo, características ilustradas ou descritas como parte de uma realização podem ser usadas em outra realização para se obter uma realização adicional.

Geralmente, um usuário contata uma instituição financeira,

a fim de solicitar um cartão de pagamento e provê a instituição com as informações correspondentes ao usuário, como nome do usuário, endereço e número de telefone. Neste sentido, um cartão de pagamento pode ser um cartão de crédito, um cartão de débito ou qualquer outro cartão ou dispositivo pelo qual um usuário pode efetuar uma transferência de crédito, dinheiro ou outra moeda corrente para um terceiro. Se a instituição financeira aceita a aplicação do usuário, a instituição emite ao usuário um cartão de pagamento com número de cartão de pagamento, um código de verificação do cartão ("CVC") e uma data de expiração. Os seis primeiros dígitos do número do cartão de pagamento do usuário identificam a instituição financeira que emitiu o cartão de pagamento e é referido como a parte "BIN" do número do cartão de pagamento. O último dígito do número do cartão de pagamento é reservado como uma soma de verificação para garantir que os outros dígitos do número constituam um número válido de cartão de pagamento. Os dígitos restantes entre o BIN e a soma de verificação são referidos como o número da conta pessoal ("PAN"). Normalmente, o PAN é um número de 9 ou 8 dígitos.

Em uma realização preferida, a instituição financeira também fornece um número ("PIN") de identificação privada de 4 dígitos para o usuário. Em uma realização, a instituição financeira seleciona o PIN para o usuário, enquanto que, em outra realização, o usuário é permitido selecionar um PIN desejado ou pode selecionar um PIN desejado depois de ter sido emitido um PIN inicial pela instituição financeira. O usuário pode selecionar um PIN por telefone, através de um site na internet ou outro mecanismo de comunicação com a instituição financeira. A instituição financeira armazena toda a informação correspondente ao usuário e o(s) cartão(ões) de pagamento associado(s) dentro do seu sistema corporativo, como um

Armazenamento Seguro de Dados de Conta de Cartão de Crédito. Uma vez que o cartão de pagamento foi emitido para o usuário, que pode então ser utilizado para iniciar uma transação financeira entre o usuário e um comerciante.

A figura 1 ilustra um sistema 10 para efetuar uma transação eletrônica, tal como uma transação de cartão de pagamento. O sistema 10 compreende um dispositivo do usuário 12, um servidor 14 mantido por uma ou mais instituições financeiras e um ou mais computadores 16 mantidos por pelo menos um comerciante. O dispositivo do usuário 12 pode ser qualquer dispositivo que compreenda um dispositivo de processamento 18, meio 20, um dispositivo de entrada 22 e um visor 24 e pode compreender, por exemplo, um computador pessoal, um computador portátil ou *tablet*, um assistente de dados pessoal, um telefone celular ou um reprodutor multimídia. O meio 20 pode ser qualquer meio capaz de ser acessado pelo dispositivo de processamento 18, tal como memória de acesso aleatório ("RAM"), memória *flash*, um disco rígido, um CD, um DVD ou uma combinação destes. O dispositivo de entrada 22 pode ser qualquer dispositivo, através do qual um usuário pode fornecer informação para o dispositivo 12, tal como um teclado, um *mouse* ou como mostrado na figura 1, um monitor (ecrã) de toque (*touchscreen*). No exemplo mostrado na figura 1, o monitor de toque 22 também funciona como visor 24, mas deve ser entendido que os dois podem ser dispositivos separados. O servidor 14 compreende o seu próprio dispositivo de processamento 26 e meio 28, enquanto o computador 16 compreende um dispositivo de processamento 30 e o meio 32. Os meios 28 e 32 podem ser qualquer meio capaz de ser acessado por dispositivos de processamento 26 e 30, respectivamente, tais como memória RAM, memória *flash*, discos rígidos, CDs, DVDs ou qualquer combinação destes.

O dispositivo do usuário 12, o servidor 14 e o computador 16 são conectados um ao outro por uma rede local ou distribuída 34, tal como a internet ou a uma linha telefônica. Alternativamente, o dispositivo do usuário 12, o servidor 14 e computador 16 podem ser conectados diretamente em uma rede ou qualquer combinação de redes públicas e privadas. Embora as conexões entre o dispositivo do usuário 12, o servidor 14 e o computador 16 para a rede 34 sejam ilustradas como ligações com fios na figura 1, deve ser entendido que cada dispositivo pode ser conectado a rede 34 através de um sistema sem fios, tal como uma rede sem fios ("Wi-Fi") ou rede por celular.

Na presente realização, um usuário direciona um programa de navegador armazenado no meio 20 e executado pelo dispositivo de processamento 18 para um site mantido por um comerciante e armazenado no computador 16. O usuário identifica e seleciona um ou mais bens e/ou serviços oferecidos pelo comerciante através do site (doravante denominada "itens"). Quando o usuário estiver pronto para comprar os itens, ele suprirá o comerciante através do site com as informações necessárias para efetuar uma transação com cartão de pagamento, tal como o nome do usuário, número de telefone, data de expiração do cartão de pagamento e CVC. Em vez de suprir o comerciante com o número real do usuário do cartão de pagamento, no entanto, o usuário gera uma alternativa, o número com tempo limite por um processo de codificação descrito em mais detalhe abaixo. O usuário fornece o número alternativo para o comerciante, que submete todas as informações fornecidas pelo usuário ao servidor 14 da instituição financeira que é capaz de validar a transação. Após a recepção da informação no servidor 14, a instituição financeira descodifica o número alternativo, tal como descrito em mais detalhes abaixo, e, utilizando a informação adicional do usuário, determina se

valida a transação de cartão de pagamento. Se a instituição financeira valida a transação, ela envia uma indicação através do servidor 14 ao computador 16 informando ao comerciante que a transação foi autorizada. O comerciante, em seguida, fornece os itens ao usuário.

Em outra realização, a transação de cartão de pagamento é efetuada pessoalmente ou através do telefone de modo que o usuário e o comerciante negociem os detalhes da operação pessoalmente ou através de uma linha telefônica. Nesta realização, o dispositivo 12 gera o número alternativo, com tempo limite por um processo de codificação descrito abaixo. O usuário fornece o número para o comerciante em qualquer forma aceitável e o processo, normalmente, continua como descrito acima. Deve ser entendido que não é necessário para o dispositivo do usuário 12 ser ligado à rede 34, em tal realização. Uma notificação de autorização por parte da instituição financeira também pode ser transmitida para o comerciante através de uma rede telefônica e pode ser transmitida verbalmente ao contrário de eletronicamente. Deste modo, é também desnecessário para o servidor 14 e o computador 16 ser ligado através da rede 34, em tal realização.

A figura 2 é um fluxograma ilustrando um processo de codificação e decodificação acima referenciado, em conformidade com uma realização da presente invenção. O processo é implementado, preferencialmente, por software, mas também pode ser implementado por hardware, por uma pessoa ou qualquer combinação destes. Na presente realização descrita, o software de implementação do processo de codificação é um programa independente autossuficiente armazenado no meio 20 do dispositivo do usuário 12 e executado por dispositivo de processamento 18. Alternativamente, o software pode ser um módulo embarcado no programa de navegador web do usuário, como um *add-on*, um *plug-in* ou um controle *Active-X*. O software de

implementação do processo de decodificação é um programa independente autossuficiente armazenado no meio 28 do servidor 14 e executado pelo dispositivo de processamento 26. Alternativamente, o software pode ser um módulo instalado dentro do sistema corporativo da instituição financeira.

O software de codificação é instalado no meio 20 do dispositivo do usuário 12, na etapa 100. Em uma realização preferida, o dispositivo do usuário 12 recupera o software a partir do servidor 14. Em outra realização, o usuário recupera o software a partir de outro servidor ou computador conectado operativamente a um dispositivo do usuário 12 ou recebe o software de uma forma, tal como um dispositivo de memória ou CD por correio a partir da instituição financeira ou de outra entidade que tenha sido encarregada para manter o software. Durante a instalação, informações correspondentes à conta do usuário de cartão de pagamento são armazenadas em um meio 20, tais como, nome do usuário, número de telefone, código CVC e data de expiração. Em uma realização, esta informação é recuperada a partir da instituição financeira durante a instalação do software. Alternativamente, outro meio que armazena esta informação é fornecido ao dispositivo do usuário 12, que transfere ou copia a informação para o meio 20. Por exemplo, a memória flash contendo esta informação pode ser inserida no dispositivo do usuário 12 ou outro dispositivo próximo ao dispositivo do usuário pode transmitir a informação sem fio ao dispositivo do usuário 12 através de *Bluetooth*, rede *Wi-Fi*, infravermelho ou por qualquer outra forma adequada. O número do cartão de pagamento, no entanto, não é fornecido ao dispositivo do usuário 12 e não é armazenado no meio 20.

Na etapa 102, o usuário inicia o software, que é recuperado a partir do meio 20 e executado pelo dispositivo de processamento 18. A

maneira pela qual o usuário inicia o software dependerá do dispositivo do usuário 12, mas pode geralmente ser iniciado com inicialização do programa relevante utilizando o sistema de funcionamento do dispositivo do usuário 12. Cada vez que o software for iniciado, o software solicita que o usuário digite o PIN (via dispositivo de entrada 22) fornecido pela instituição financeira ou selecionado pelo usuário, a fim de ter acesso ao software, como representado pelas etapas 104 e 106. Na etapa 108, o usuário é apresentado com um exemplo de interface gráfica do usuário exemplar ("GUI") 50, conforme ilustrado pela figura 3. Referindo-se a figura 3, o GUI 50 compreende um botão de ativação 52 (rotulado "gerar"), nome do titular do cartão em um local 54, a data de expiração do cartão de pagamento real na localização 56, o CVC para o cartão de pagamento no local 58 e uma caixa de *menu* suspensa 60 fornecendo ao usuário vários períodos de tempo opcionais, tais como, uma semana, um mês, um ano, etc. Deve ser entendido que os períodos de tempo apresentados pela caixa de *menu* suspensa 60 pode ser variado, dependendo de quais seleções devem ser disponíveis para o usuário como períodos de tempo aceitáveis, tal como explicado abaixo. Por exemplo, os períodos de tempo selecionáveis podem incluir dias individuais para a semana seguindo o tempo quando o usuário acessa a caixa de *menu* suspensa 60. Um local 62 identifica um número de cartão de pagamento com tempo limite, alternativo gerado pelo processo descrito a seguir, após o usuário ativar o botão 52. Os "Bs" dos números da localização 62 representam o BIN, que é o mesmo para cada número de cartão de pagamento com tempo limite, alternativo, em que o BIN identifica a instituição financeira que emitiu o cartão de pagamento original como descrito acima ou a instituição financeira que validará e/ou processará as transações envolvendo os números com tempo limite gerados. A instituição financeira pode usar o mesmo BIN

para os cartões de pagamento com tempo limite como faz para os cartões de pagamento originais ou pode registrar ou usar um BIN separado para os cartões de pagamento com tempo limite a fim de distribuir transações envolvendo cartões de pagamento com tempo limite para um centro de processamento específico. Os "Xs" representam o PAN e o "L" representa a soma de verificação. O PAN e a soma de verificação são gerados de acordo com o processo descrito abaixo.

Ainda, com referência às figuras 2 e 3, na etapa 110, o usuário seleciona um período de tempo desejado a partir da caixa de *menu* suspensa 60 para o qual o usuário deseja que o número de cartão de pagamento com tempo limite seja válido. Na etapa 112, o usuário ativa o botão 52, assim, instruindo o software a gerar um novo número de cartão de pagamento com tempo limite, desse modo, executando o programa. Neste ponto, o software normaliza a data atual em 00:00:00 Hora Média de Greenwich ("GMT"), independentemente da hora atual. Isto é, o software determina a data atual e define a parte do tempo da data atual para 00:00:00 GMT. Com base no período de tempo selecionado pelo usuário na etapa 110 via caixa de *menu* suspensa 60 e na data atual normalizada, a data de expiração desejada do número do cartão de pagamento com tempo limite é determinado na etapa 114. Deve ser entendido que a data de expiração do número com tempo limite é definida com base no GMT, onde o tempo de expiração é definido como 23:59:59 GMT (aproximadamente meia-noite) na data conforme selecionada pelo usuário na caixa de *menu* suspensa 60. Por exemplo, se o usuário seleciona um período de tempo de "uma semana" em 12 de janeiro a 1 hora pm no leste, esta hora é normalizada para 12 janeiro às 00:00:00 GMT. Assim, a data de expiração é programada para 19 de janeiro às 23:59:59 GMT. Na presente realização descrita, a

data de expiração do cartão de pagamento do usuário é considerada 23:59:59 GMT a partir da data estabelecida no cartão de pagamento original. Deve ser entendido que qualquer zona de hora e/ou hora desejado pode ser selecionada para normalizar a data atual, a data de expiração desejada do número com tempo limite e a data de expiração do cartão de pagamento, enquanto a zona de hora selecionada e a hora desejada são utilizadas de forma consistente com relação a todas as três datas, de modo que as três datas sejam análogas. Isto é, é importante que as três datas sejam convertidas para uma zona de hora comum para comparação.

Na etapa 116, o programa calcula o número de dias entre a data de expiração desejada do número com tempo limite e data de expiração do cartão de pagamento. O número de dias entre os dois é aqui referido como "diferença de dias" para fins de explicação. Uma vez que as instituições financeiras, geralmente, não fazem emissão de cartões de pagamento com uma data de expiração maior do que três anos a partir da data de emissão, o valor da diferença de dias deve ser menor ou igual a 1096 (assumindo um dos três anos é um ano bissexto; isto é, 365 * 3 + 1). Na etapa 118, o software determina o número de dígitos da diferença de dias e zeros são acrescentados à frente da diferença de dias até que o comprimento da diferença de dia seja de cinco dígitos. O resultado é um número de 5 dígitos que representa a data de expiração do número com tempo limite relativo à data de expiração do cartão de pagamento (isto é, o número de dias antes da expiração do cartão de pagamento no momento em que o número com tempo limite expirará).

Na etapa 120, o software anexa o PIN de 3 ou 4 dígitos introduzido pelo usuário na etapa 106 para frente do número de 5 dígitos estabelecido na etapa 118, o que resulta no PAN. Deve ser

entendido que o número de dígitos do PIN ou o número correspondente à data de expiração do número com tempo limite pode ser variado, dependendo do número de dígitos disponível para o processo de codificação e de utilização pretendida do PIN, conforme definido em mais detalhes abaixo. O software acrescenta o PAN ao fim do BIN, resultando em um número de 15 dígitos, na etapa 122. Na etapa 124, um "a verificação Luhn" é realizada com o intuito de gerar o dígito da última soma de verificação do número com tempo limitado alternado. Uma verificação Luhn, como descrito na patente norte-americana US 2.950.048 concedida a H. L. Luhn, que é aqui incorporada por referência, como se estabelecido textualmente, deve ser entendido pelos técnicos no assunto e não é, portanto, aqui descrito em detalhes. Na etapa 126, o software anexa o resultado da verificação Luhn ao final do número de 15 dígitos estabelecido na etapa 122 para criar um número de cartão de pagamento com tempo limite de 16 dígitos, alternativo. Na etapa 128, o GUI 50 exibe o número do cartão de pagamento com tempo limite no local 62.

Tal como acima descrito em relação à figura 1, o usuário provê o comerciante com este número de cartão de pagamento com tempo limite, alternativo, para efetuar uma transação de cartão de pagamento, representado na etapa 130 na figura 2. Deve ser entendido que o usuário pode efetuar a transação fornecendo o número de cartão de pagamento com tempo limite, alternativo, ao comerciante em uma transação presencial ou através de um telefone. Com referência as figuras 1 e 2, o comerciante transmite a informação fornecida pelo usuário durante a transação de cartão de pagamento entre o usuário/comerciante, incluindo o CVC, data de expiração, o nome e o número de telefone associado com o cartão de pagamento do usuário, juntamente com o número do cartão de pagamento alternativo e a data

em que a transação do cartão de pagamento foi efetuada à instituição financeira associada com o BIN na etapa 130. Na realização presentemente descrita, esta informação é transmitida ao servidor 14 através do computador 16, mas pode ser realizada por quaisquer outros meios, tais como, eletronicamente ou verbalmente através de uma linha de telefone.

A instituição financeira recebe a informação relevante para a transação do cartão de pagamento do comerciante na etapa 132. Na realização atual, o software armazenado no meio 32 e executado pelo dispositivo de processamento 30 transmite a informação para a instituição financeira. Alternativamente, o comerciante pode fornecer as informações para a instituição financeira através de uma linha telefônica. Na etapa 134, o dígito de soma de verificação do número do cartão de pagamento, alternativo é extraído e comparado com o resultado da verificação Luhn do BIN e PAN para assegurar que o número alternativo possa ser um número de cartão de pagamento válido. Se não, a transação é rejeitada na etapa 136.

Caso contrário, o software da instituição financeira usa outra informação transmitida pelo comerciante para a instituição financeira para localizar a conta do usuário, na etapa 138. O programa coincide o CVC, nome, número de telefone e data de expiração transmitida pelo comerciante a um CVC, nome, número de telefone e data de expiração associados a uma conta localizada dentro do sistema da instituição financeira. Numa outra realização, um subconjunto destas informações, tal como, o nome e número de telefone ou o número de telefone ou CVC, é usado para localizar a conta correspondente mantida pela instituição financeira. Se cartões de pagamento múltiplos estiverem associados ao usuário ou a conta, o programa usa o CVC e/ou data e expiração para identificar o cartão de

pagamento específico para a qual a transação se refere.

Em outra realização, o dispositivo do usuário 12 (figura 1) transmite a informação capaz de identificar o usuário, com exceção à informação correspondente ao número de cartão de pagamento do usuário, juntamente com o número com tempo limite. A outra informação pode ser uma assinatura de dispositivo, tal como, um serviço de assinante ou de identidade internacional do assinante móvel ("IMSI"). Um IMSI é um número único associado com o dispositivo do usuário 12 e é capaz de identificar o usuário correspondente dentro do sistema da instituição financeira, desde que o IMSI seja armazenado pela instituição na conta do usuário. Alternativamente, o dispositivo do usuário 12 transmite uma sequência de caracteres alfanuméricos exclusivos para a conta do usuário na instituição financeira. A instituição financeira utiliza esta sequência única, que é armazenada na conta do usuário, a fim de localizar a conta do usuário. Deve ser entendido, a partir da descrição acima, que o número real do cartão de pagamento do usuário ou o PAN do número real de pagamento, não são necessários para localizar a conta do usuário.

Na etapa 140, o programa da instituição financeira extrai os outros quatro dígitos do PAN e compara aqueles dígitos ao PIN armazenado pela instituição financeira na conta do usuário identificado na etapa 138. Se os dígitos extraídos e o PIN armazenado não coincidirem, o programa rejeita a operação na etapa 136.

Caso contrário, na etapa 142, o software da instituição financeira normaliza a data em que a transação de cartão de pagamento foi efetuada para 00:00:00 GMT de uma forma idêntica à descrita acima com respeito à etapa 114. Na etapa 144, o software da instituição financeira calcula o número de dias entre a data normalizada da transação efetuada e a data de expiração do cartão de pagamento. Na

etapa 146, o software extrai os últimos cinco dígitos do PAN do número alternativo e, na etapa 148, o software compara os dígitos extraídos ao número de dias determinado na etapa 144. Se o número de dias calculados na etapa 144 for menor do que os cinco dígitos extraídos, isso indica que o número com tempo limite, alternativo expirou. A transação é, portanto, rejeitada na etapa 136. Caso contrário, a transação é autorizada na etapa 150.

Deve ser entendido que o processo acima permite a criação de um número de cartão de pagamento alternativo, que é válido por um período de tempo selecionado pelo usuário. Assim, se o número alternativo for roubado ou tornado público, o número será automaticamente invalidado e inutilizável após o período de tempo selecionado. Além disso, se a informação correspondente à transação do cartão de pagamento, conforme descrito acima for roubada ou comprometida, o possuidor da informação é incapaz de discernir o número real do cartão de pagamento do usuário a partir da informação. O processo acima permite ao usuário gerar um único número de cartão de pagamento com tempo limite para cada dia em que o número alternativo é desejado a expirar.

A figura 4 ilustra um processo de codificação e decodificação, de acordo com outra realização da presente invenção. Nesta realização, o programa do dispositivo do usuário utiliza cinco dígitos do PAN para representar a data em que o número de cartão de pagamento com tempo limite, alternativo expirará, gerado da mesma maneira de como descrito acima em relação à realização da figura 2. Em um determinado ponto de vista, os cinco dígitos do PAN são utilizados para este número de data, 100.000 diferentes números (de 0 a 99.999), podem ser armazenadas nestes dígitos. A maior quantidade de tempo que o usuário pode selecionar para que o número alternativo expire

coincide com a diferença entre a data da emissão do cartão e a sua data de expiração. Uma vez que a data de expiração de qualquer cartão de pagamento, geralmente, é de três anos mais ou menos a partir da data de emissão, o prazo máximo mais provável é de 1.096 dias (permitindo um ano bissexto). Assim, 91 números de cartão de pagamento com tempo limite, alternativo podem ser gerados para cada data de expiração desejada em 3 anos. Isto é, 100.000 números divididos por 1.096 dias resultam em aproximadamente 91 números por dia. Assim, na presente realização descrita, cada dia, em três anos está associado com uma faixa de 91 números dentro dos 100.000 números disponíveis. Por exemplo, a data de expiração do cartão de pagamento é associada com o primeiro conjunto de 91 números, ou seja, de 0 a 90. No dia anterior à data de expiração do cartão de pagamento é associado com o segundo conjunto de 91 números - 91 até 180, e assim por diante.

O processo ilustrado na figura 4 é idêntico ao da figura 2, com relação às etapas 100 até a 116 e o número de dias entre a data de expiração desejada, normalizada do número com tempo limite e a data de expiração do cartão de pagamento são calculados na etapa 116, como descrito acima com relação à figura 2. Na presente realização, com respeito à figura 4, o número de dias determinado na etapa 116 da figura 2 é multiplicado pela faixa de dias (91, neste caso), para desse modo encontrar o menor número no intervalo associado com a data de expiração desejada selecionada na etapa 200. O software adiciona um a menos do que o comprimento da faixa de dias inserida para cada dia (90, neste caso) para o menor número (calculado na etapa 200) para, assim, determinar o maior número dentro da faixa, na etapa 202. Um gerador de números aleatórios executado no software do usuário e limitado pelo menor número (etapa 200) e maior número (etapa 202)

dentro da faixa de dias cria um número aleatório dentro do intervalo na etapa 204. Como descrito acima, os zeros são acrescentados ao número aleatório, conforme necessário, na etapa 206 para gerar um número de 5 dígitos. Este número de 5 dígitos corresponde à data de expiração do número com tempo limite, na medida em que pode ser utilizado juntamente com outra informação associada ao cartão de pagamento real para determinar a data de expiração do número com tempo limite. Este número é anexado ao PIN para formar o PAN. O processo acima substitui o processo descrito anteriormente em relação à etapa 118 da figura 2 e o fluxo do processo prossegue para a etapa 146 e continua de maneira idêntica a do processo descrito acima em relação à figura 2.

Ainda com referência à figura 4, o programa da instituição financeira extrai os cinco dígitos que representam a data de expiração desejada, na etapa 146. O programa da instituição financeira divide o número extraído pela faixa de dias dos números para cada data de expiração (91, neste exemplo descrito) e arredonda para baixo para o número integral mais próximo ou um número inteiro, na etapa 208. O resultado é o número de dias entre a data de expiração desejada do número alternativo e a data de expiração do cartão de pagamento. O fluxo do processo prossegue para a etapa 148 e continua de forma idêntica à descrita acima em relação à figura 2.

O processo descrito acima em relação à figura 4 fornece a capacidade de gerar números de cartões de pagamento com tempo limite, múltiplos para cada data de expiração desejada. Assim, por exemplo, se o usuário gerar números múltiplos para as respectivas transações, o sistema provavelmente gerará números diferentes para a maioria ou todas as transações. Se um dos números for roubado, ele pode, portanto, ser possível de identificar a transação particular envolvida, e, assim, o local de venda particular a partir do qual o

número foi roubado. Também é possível gerar números com tempo limite adicionais para um período de tempo específico, mesmo depois de tal número ter se tornado comprometido.

A figura 5 ilustra um processo de codificação e decodificação de acordo com outra realização da presente invenção. Nesta realização, o fluxo do processo segue para a etapa 206 de uma forma idêntica à descrita acima com relação à figura 4. A etapa 120 (figura 4) é substituída pela etapa 300, onde o programa do usuário no dispositivo 12 cria o PAN intercalando o PIN e o número de 5 dígitos gerado na etapa 206. Por exemplo, cada dígito do PIN é inserido entre dois dígitos adjacentes do número de 5 dígitos. Deve ser entendido que a forma pela qual o PIN e o número de 5 dígitos são intercalados ou rearranjados pode variar desde que a instituição financeira remonte o PIN e o número de 5 dígitos, utilizando um método correspondente, como descrito abaixo. Além disso, o método de intercalação pode variar a partir de um usuário para outro.

O fluxo do processo continua para a etapa 138 de uma forma idêntica à descrita acima em relação à figura 4. Na etapa 302, o programa da instituição financeira remonta o PIN e o número de 5 dígitos do PAN ao contrário da maneira pela qual o PIN e os 5 dígitos foram intercalados na etapa 300. Continuando o exemplo acima, por exemplo, cada dígito do PIN seria extraído a partir de entre os dígitos adjacentes dos números de 5 dígitos onde haviam sido inseridos. O fluxo do processo avança para a etapa 140 e, em seguida, continua de forma idêntica à descrita acima em relação à figura 4. Deve ser entendido que o processo acima intercala o PIN associado com o cartão de pagamento do usuário, a fim de obscurecer a visibilidade do PIN.

A figura 6 ilustra outro processo de codificação e decodificação de acordo com outra realização da presente invenção.

Nesta realização, o fluxo do processo prossegue para a etapa 300 de forma idêntica à descrita acima com relação à figura 5. Pelo fato do programa do usuário ser construído para lembrar o local onde se insere os dígitos do PIN para as posições dentro do PAN, o programa do usuário extrai o último dígito do PIN, independentemente de sua localização dentro do PAN na etapa 400. Na etapa 402, o programa do usuário executa uma verificação Luhn sobre os 15 dígitos restantes do número e coloca o resultado no local onde o último dígito do PIN foi extraído. Na etapa 404, o programa do usuário extrai o terceiro dígito do PIN e executa uma verificação Luhn sobre os 15 dígitos restantes do número. Na etapa 406, o programa do usuário coloca o resultado da verificação Luhn no local onde o terceiro dígito do PIN foi extraído. Na etapa 408, o programa extrai o segundo dígito do PIN e o substitui com o resultado de uma verificação Luhn sobre os 15 dígitos restantes. Na etapa 410, o programa extrai o primeiro dígito do PIN e o substitui com o resultado de uma verificação Luhn sobre os 15 dígitos restantes. O fluxo do processo continua para a etapa 138 em uma maneira idêntica à descrita acima com respeito à figura 5.

O programa da instituição financeira é construído para reconhecer os locais onde o programa do usuário implantou os dígitos do PIN no PAN, e, assim, os locais onde a verificação Luhn substituiu os dígitos do PIN dentro do PAN. Assim, na etapa 412, o programa da instituição financeira extrai o número que substituiu o primeiro dígito do PIN e executa uma verificação Luhn na etapa 414. Se o resultado for qualquer outro diferente do número extraído na etapa 412, a transação é negada na etapa 136. Caso contrário, na etapa 416, o programa da instituição financeira coloca o primeiro dígito do PIN conforme armazenado na conta do usuário mantida pela instituição financeira no local onde o número foi extraído na etapa 412. Na etapa 418, o

programa da instituição financeira extrai o número que substituiu o segundo dígito do PIN e executa uma verificação Luhn na etapa 420. Se o resultado for qualquer um diferente do número extraído na etapa 418, a transação é rejeitada na etapa 136. Caso contrário, na etapa 422, o programa coloca o segundo dígito do PIN, conforme armazenado pela instituição financeira, no local onde o número foi extraído na etapa 418.

O programa da instituição financeira extrai o número que substituiu o terceiro dígito do PIN na etapa 424 e executa uma verificação Luhn na etapa 426. Se o resultado for qualquer um diferente do o número extraído na etapa 424, a transação é negada na etapa 136. Caso contrário, na etapa 428, o programa da instituição financeira inseri o terceiro dígito do PIN como armazenado na conta do usuário mantida pela instituição financeira para o PAN no local onde o número foi extraído, na etapa 424. Na etapa 430, o programa da instituição financeira extrai o número que substituiu o quarto dígito do PIN e executa uma verificação Luhn na etapa 432. Se o resultado for qualquer um diferente do número extraído na etapa 430, a transação é rejeitada na etapa 136. De outra forma, na etapa 434, o programa da instituição financeira coloca o quarto dígito do PIN como armazenado pela instituição financeira no local onde o número foi extraído na etapa 430. O fluxo do processo segue para a etapa 302 e continua de forma idêntica à descrita acima em relação à figura 5.

Deve ser entendido que o processo acima altera cada dígito do PIN, que é armazenado em locais diferentes dentro do PAN do número do cartão de pagamento com tempo limite. Adicionalmente, a alteração de cada dígito é dependente dos outros dígitos e das alterações anteriores. Assim, se uma tentativa de usar o número do cartão de pagamento com tempo limite envolver a alteração de qualquer um dos dígitos, a transação será negada. Além disso, o PIN não é visível

dentro do PAN.

A figura 7 ilustra um processo de codificação e decodificação de acordo com outra realização da presente invenção, onde a informação armazenada no dispositivo do usuário 12 (figura 1) inclui um número de oito dígitos aleatório específico para o usuário (doravante referido como "randomizador" para simplificar). A instituição financeira armazena o randomizador na conta do usuário.

Fazendo referência à figura 7, a instalação na etapa 100 ocorre da mesma maneira como descrito acima em relação à figura 2. O fluxo do processo prossegue a partir da etapa 100 para a etapa 410 de forma idêntica à descrita acima em relação à figura 6. Na etapa 500, o programa do usuário adiciona (soma) o randomizador ao PAN gerado na etapa 410. Na etapa 502, o programa do usuário analisa o comprimento da soma calculada na etapa 500. Se a soma for um número de 10 dígitos, o primeiro "1" é truncado, resultando em um PAN de 9 dígitos. O fluxo do processo segue para a etapa 140, o que também ocorreria se a somatória não fosse um número de 10 dígitos (determinado na etapa 500), e continua de forma idêntica à descrita acima em relação à figura 6.

Na etapa 506, o programa da instituição financeira extrai o PAN do número com tempo limite. Na etapa 508, o programa da instituição financeira compara o randomizador associado com o cartão de pagamento do usuário armazenado pela instituição financeira para o PAN de 9 dígitos. Se o randomizador for maior que o PAN, um primeiro "1" é acrescentado à frente do PAN na etapa 510. O programa da instituição financeira subtrai o randomizador do PAN na etapa 512. O programa reinseri o PAN de 9 dígitos resultante dentro do número do cartão de pagamento com tempo limite no local apropriado - entre o BIN e a verificação da soma. O fluxo do processo segue para a etapa 412 e

continua de maneira idêntica à descrita acima em relação à figura 6.

O processo acima descrito em relação à figura 7 inclui a adição de um número aleatório específico para o usuário. Este número é armazenado no dispositivo do usuário 12 e no servidor 14 da instituição financeira. Qualquer tentativa para decodificar o número de cartão de pagamento com tempo limite gerado pelo processo acima, sem o randomizador não terá êxito.

Com referência à figura 7, em outra realização, a informação armazenada no dispositivo do usuário 12 (figura 1) inclui dois dígitos de um número de validação de 4 dígitos e seis dígitos do randomizador de 8 dígitos. Conforme estabelecido acima, a instituição financeira mantém toda a informação correspondente ao usuário, incluindo todos os quatro dígitos do número de validação e todos os oito dígitos do randomizador.

O PIN introduzido pelo usuário na etapa 106 é composto por outros dois dígitos do número de validação de 4 dígitos e outros dois dígitos do randomizador de 8 dígitos. Deve ser entendido que a localização dos dígitos remanescentes do número de validação e do randomizador dentro do PIN pode variar, desde que o software seja construído de modo a saber a localização de cada dígito. Por exemplo, os dois dígitos do número de validação podem ser os dois primeiros dígitos do PIN ou os dois dígitos do meio, com os dois locais restantes a ser ocupada pelos dois dígitos ausentes da randomizador. Os dígitos também podem ser invertidos em relação à forma de como eles devem aparecer no número de validação e no randomizador. Por exemplo, o último dígito do PIN pode ser o primeiro dígito do número de validação completo e o primeiro dígito do PIN pode ser o terceiro dígito do número de validação completo. Assim, deve ser aparente que a localização de cada dígito dentro do PIN é irrelevante com a condição de que o software

é construído para identificar a localização de cada dígito.

Na presente realização, os dois dígitos do número de validação são extraídos a partir do PIN introduzido pelo usuário e atrelado aos dois dígitos do número de validação dentro do arquivo armazenados no meio 20 para produzir o número de validação completo, na etapa 106. Do mesmo modo, o programa do usuário extrai os dois dígitos do número randomizador a partir do PIN e os junta aos seis dígitos do randomizador dentro do arquivo armazenado no meio 20 para produzir o randomizador completo, na etapa 106. Na realização aqui descrita, o número de validação substitui o número do PIN para o restante do processo, que prossegue para a etapa 108 e continua de uma maneira ou de outra idêntica ao descrito acima. Por exemplo, o número de validação (ao contrário do PIN) e o número de 5 dígitos são intercalados na etapa 300 e reagrupados na etapa 302. O fluxo do processo prossegue de modo similar ao descrito acima.

Na etapa 148, o programa da instituição financeira compara o número de validação reagrupado com o número de validação específico ao usuário mantido pela instituição financeira. Se os números de validação não coincidirem, a transação é negada na etapa 136. Caso contrário, a transação é validada na etapa 150.

O processo acima descrito evita que a informação necessária para gerar um número de cartão de pagamento com tempo limite seja acessível a partir de um único local. Isto é, com exceção da instituição financeira, nenhuma entidade ou dispositivo possui o número de validação inteiro e/ou randomizador, nem mesmo o usuário. Assim, se o dispositivo do usuário 12 for roubado, o criminoso será incapaz de gerar um número válido, sem conhecer o PIN.

Também deve ser entendido que os processos de codificação e decodificação descritos acima são processos exemplificativos e vários

processos podem ser utilizados. Além disso, diferentes processos podem ser utilizados para um ou mais usuários de modo que o processo de codificação e decodificação para um usuário possa ser diferente do processo utilizado para outro usuário. Como resultado, a segurança do sistema descrito acima e do método é aumentada pelo fato de que a descoberta do método associado a um usuário seria ineficaz em comprometer a informação confidencial de outro usuário para o qual um método diferente foi associado.

Com referência às figuras 1 e 7, em outra realização, um arquivo contendo a informação correspondente ao cartão de pagamento do usuário, juntamente com os dois dígitos do número de validação e os seis dígitos do randomizador, é armazenado no meio 20 durante a instalação, na etapa 100. Alternativamente, o arquivo pode ser armazenado no meio 20 antes ou depois da instalação do software, na etapa 100. O arquivo pode ser descarregado a partir do servidor 14 ou a partir de outro computador mantido operativamente por um terceiro conectado ao dispositivo do usuário 12 ou pode até mesmo ser enviado via correio para o usuário pela instituição financeira ou terceiros.

Deve ser entendido que o número de dígitos distribuídos para o número de validação/PIN e para o número de representativo da data de expiração desejada do número de cartão de pagamento com tempo limite pode ser variado, dependendo do número disponível de dígitos e o uso desejado dos dígitos sem se afastar do escopo das realizações presentemente descritas. Por exemplo, cartões de crédito emitidos pela *American Express* são de 15 dígitos de comprimento, em comparação com os números de 16 dígitos acima discutidos. Para acomodar para um dígito menos, um dígito pode ser removido a partir de qualquer dos dígitos atribuídos para o número de validação/PIN ou para a porção representativa da data de expiração desejada. A redução

do número de dígitos atribuídos à data de expiração desejada altera a quantidade de números de cartão de crédito com tempo limite disponíveis por dia de expiração desejado. Por exemplo, a redução do número de dígitos para o número que representa a expiração desejada de 5 a 4 reduz o número de diferentes números com tempo limite que podem ser gerados para cada dia a partir de 91 a 9 (10.000/1.096). Além disso, as instituições financeiras associadas com um BIN específico podem autorizar outras instituições financeiras a usar o mesmo BIN. Neste cenário, os dígitos no PAN seguindo o BIN são usados para identificar quais números de cartões de pagamento foram emitidos pelas instituições autorizadas. As transações envolvendo números de cartões de pagamento que incluem o BIN específico são encaminhadas à instituição autorizadoras. A instituição autorizadora, em seguida, encaminha as transações à instituição autorizada associada com os dígitos do PAN reservado para apenas identificar as instituições autorizadas a qual o número do cartão de pagamento pertinente corresponde. Neste caso, os dígitos disponíveis dentro do PAN para uso nos processos acima descritos são reduzidos. O processo de codificação e decodificação trata com uma quantidade reduzida de dígitos disponíveis dentro do PAN como descrito acima.

Além disso, pode ser desejável colocar mais números de cartões de pagamento com tempo limite disponíveis para uma data de expiração desejada do que para outro. Por exemplo, supondo que cinco dígitos do PAN sejam selecionados para representar a data de expiração desejada do número de cartão de pagamento com tempo limite, como descrito acima, pode ser desejável colocar metade dos números disponíveis ou 50.000 para ser utilizado com números com tempo limite expirando na mesma data como a data de expiração real do cartão de pagamento. Neste caso, apenas os restantes 50.000 números estão

disponíveis para outras datas de expiração, reduzindo assim os números disponíveis por dia de expiração desejada para aproximadamente 45 (50.000/(1.096-1)).

Do mesmo modo, pode ser desejável permitir um conjunto de números com tempo limite com uma utilização específica. Por exemplo, pode ser vantajoso alocar 50.000 dos números disponíveis para serem usados como números de cartão de pagamento de uso único. Isto é, cada número gerado com base em um destes números disponíveis pode ser utilizado apenas uma vez. Em tal realização, o usuário não seleciona um período de tempo ou uma data de expiração. Em vez disso, o programa de codificação gera um número com tempo limite selecionando aleatoriamente um número a partir da faixa disponível de números. O processo, de outra forma, prossegue como descrito acima. Uma vez que o número aleatório é decodificado e extraído a partir do número com tempo limite, o programa de decodificação determina se ele se encaixa dentro da faixa de números aceitáveis e, nesse caso, se o número foi usado anteriormente. Se o número não foi envolvido em uma transação anterior, a instituição financeira autoriza a transação atual e remove o número da lista de números utilizáveis. Caso contrário, a transação será rejeitada. Assim, se outra transação inclui o mesmo número a partir da faixa de números aceitáveis, ele será rejeitado. Isto evita que um número substituto roubado ou comprometido seja usado novamente, uma vez que já foi utilizado em uma transação.

Além disso, o comprimento do PIN emitido pela instituição financeira pode ser variado sem se afastar do escopo da presente invenção. Além disso, a finalidade de cada dígito dentro do PIN pode ser variada dependendo do processo de codificação e decodificação desejado. Por exemplo, a instituição financeira pode emitir um PIN de 5

dígitos, em que um dos dígitos é parte do número de validação e os quatro dígitos restantes são parte do randomizador. Neste exemplo, três dígitos do número de validação são armazenados no meio 20 do dispositivo do usuário 12, e quatro dígitos do randomizador são armazenados no meio.

Também deve ser entendido que a presente invenção não é dirigida apenas às transações que ocorrem através de uma rede, tal como a Internet. Por exemplo, um usuário pode entrar em contato com um comerciante por telefone e fornecer as informações necessárias para efetuar uma transação com cartão de pagamento, incluindo o número do cartão de pagamento com tempo limite, substituto por telefone. Neste exemplo, o dispositivo do usuário 12 gera o número da maneira descrita acima e o usuário fornece verbalmente o número e outras informações necessárias para o comerciante. Além disso, um usuário pode também verbalmente fornecer o número com tempo limite, em uma transação pessoal com um comerciante. Neste momento, o usuário também provê o comerciante com outras informações necessárias para efetuar uma transação com cartão de pagamento, que pode incluir o nome do usuário, CVC e número de telefone. Assim, deve ser entendido que os processos acima descritos podem ser empregados em ambos os modos, conectado e desconectado. Isto é, o dispositivo do usuário 12 (figura 1) pode ser um computador pessoal conectado operativamente a um comerciante e uma instituição financeira através de uma rede física de uma maneira que permita que o dispositivo do usuário interagir com sistemas mantidos pelo comerciante e/ou instituição financeira. Alternativamente, o dispositivo do usuário 12 pode ser um assistente de dados pessoal que não está conectado a um sistema mantido pelo comerciante ou instituição financeira. Em tal realização, as informações armazenadas dentro ou geradas pelo dispositivo do usuário podem ser

fornecidas ao comerciante ou instituição financeira pelo usuário, pelo comerciante ou por qualquer outra forma adequada.

Deve ser entendido que o dispositivo do usuário 12 (figura 1) não precisa ser um dispositivo interativo, mas pode ser um dispositivo não interativo, tal como uma passagem inteligente "*smart pass*", cartão inteligente "*smartcard*" ou chave de segurança "*key fob*". Em tal realização, quando o dispositivo está dentro da faixa de um leitor associado e os detalhes da transação foram estabelecidas, o dispositivo transmite a informação pertinente para o receptor, incluindo um número de cartão de pagamento com tempo limite e uma data de expiração para o número. Nesta realização, a data de expiração está definida para o período de tempo padrão estabelecido pela instituição financeira correspondente. Por exemplo, o dispositivo do usuário 12 seleciona 1 semana como o período de tempo para o número com tempo limite, substituto para expirar por padrão. Deve ser entendido que, pelo fato do número com tempo limite, alternativo ser transmitido pelo dispositivo para o receptor, um visor, tal como visor 24 (figura 1), é desnecessário em tal realização. Deve também ser entendido que o dispositivo do usuário 12 pode ser pré-programado para gerar números com tempo limite, alternativos definidos para expirar em um intervalo fixo. Por conseguinte, um dispositivo de entrada, tal como, o dispositivo de entrada 22 (figura 1), que permite ao usuário selecionar um período de tempo ou data de expiração é desnecessário em tal realização.

Deve também ser entendido que as instituições financeiras podem utilizar métodos de codificação conhecidos e futuramente desenvolvidos e processos em conjunto com as formas de realização acima descritas. Tais técnicas de criptografia podem ser utilizadas em combinação com os processos acima, sem necessidade de alterar materialmente os processos acima descritos. Além disso, técnicas de

criptografia múltiplas podem ser utilizadas para auxiliar os métodos de segurança acima descritos, sem se afastar do escopo da presente invenção.

Também deve ser apreciado que o número gerado pelo processo descrito acima em relação à figura 2, bem como os processos descritos acima em relação às figuras 4 a 7, podem ser utilizados para uma variedade de fins. Em outra realização, por exemplo, o número gerado pode ser utilizado como um nome de usuário ou ambos, a fim de fornecer ao usuário com acesso a um sistema, tal como um sistema *online* ou de software. Novamente referindo à figura 1, por exemplo, o servidor 14, que é mantido por uma instituição financeira pode ser configurado para hospedar um *site*. Isto é, o meio 28 do servidor 14 contém instruções de computador que, quando executado pelo dispositivo de processamento 26, sirva, hospede ou de outro modo forneça um sistema *online* ou *site* que seja acessível a um dispositivo móvel operado pelo usuário, tais como dispositivo do usuário 12, via rede de área ampla ("WAN") 34. O *site* pode ser adaptado para permitir aos usuários exibir, gerenciar e interagir com suas respectivas contas mantidas pela instituição financeira.

Em uma realização, o *site* é configurado como um sistema bancário *online*. Como deve ser entendido, sistemas bancários *online* conhecidos são adaptados para solicitar e validar um nome de usuário e senha fornecidos pelo usuário antes de permitir ao usuário acessar a(s) conta(s) do(s) usuário(s), mantido pela instituição financeira. O sistema bancário *online* pode ainda ser configurado para solicitar informações adicionais do usuário, tal como o PIN associado com a conta do usuário ou a resposta a uma ou mais "perguntas secretas", ao qual apenas o usuário deve saber a resposta. Alternativamente, o sistema pode exigir que o usuário forneça o PIN associado à conta, em vez de uma senha.

Independentemente disso, o usuário fornece as informações solicitadas, a fim de ter acesso à conta do usuário através do sistema bancário *online*. Tipicamente, esta informação é estática e, uma vez comprometida, pode ser utilizado de forma similar por uma parte não autorizada para ganhar acesso a conta do usuário.

Na presente realização descrita, o usuário gera um número através do dispositivo do usuário 12 da forma descrita acima. Quando for solicitado o nome de usuário ou ID do *login*, o usuário fornece o número do sistema *online* hospedado pelo servidor 14. O usuário então fornece a senha, PIN ou qualquer outra informação solicitada pelo sistema. Um ou mais programas executados pelo dispositivo de processamento 26 do servidor 14, então, determinam se o número fornecido é legítimo e identifica o usuário com base no número de um modo semelhante ao descrito acima. O servidor 14, em seguida, determina se o número, juntamente com o resto da informação fornecida pelo usuário, tal como a senha, coincide com a informação armazenada no servidor correspondente à conta do usuário. Se assim for, o *site* oferece ao usuário o acesso às contas do usuário mantidas pela instituição financeira.

Ainda, em outra realização, o usuário fornece o nome de usuário ou *login* associado com a conta do usuário ao sistema e, em seguida, gera um número utilizando um dispositivo 12 por um dos processos descritos acima com relação às figuras 2 e 4 a 7. Quando solicitado a senha ou PIN, o usuário fornece o número gerado pelo dispositivo do usuário 12 para o sistema *online*. O servidor 14 determina se o número é legítimo e se corresponde à mesma conta para que o nome de usuário ou ID do *login* fornecido pelo usuário corresponde. Se assim for, o servidor 14 determina se todas as informações fornecidas pelo usuário coincidem com as informações

armazenadas pelo servidor 14 no meio 28 correspondente à conta. Se assim for, o sistema *online* mantido pelo servidor 14 fornece ao usuário acesso à conta.

Deve ser entendido que, pelo fato do número gerado pelos processos acima ser seguro, isto é, não pode ser usado por uma pessoa não autorizada para determinar o número de conta do usuário, pode ser fornecido por um usuário sem outra informação, a fim de ter acesso à conta do usuário através de um sistema bancário *online*. Isto é, qualquer receptor ou titular do número é capaz de determinar o número da conta a partir do número gerado, tal como explicado acima. Assim, em uma realização preferida, o sistema bancário *online* é configurado para solicitar apenas o número gerado pelo dispositivo do usuário 12. Isto é, o sistema não solicita outras informações diferentes do número, tal como uma senha. Nesta realização, o usuário gera o número e o fornece ao sistema *online* quando solicitado. O servidor 14 identifica o usuário e a conta com base no número e determina se o número é legítimo. Se assim for, o sistema bancário *online* provê ao usuário acesso à conta. Se desejar, o sistema pode fornecer ao usuário acesso a todas as contas associadas com o usuário mantidas pela instituição se o servidor 14 identifica e autentica o usuário, em vez de proporcionar apenas o acesso para a conta associada com o número gerado.

Um sistema bancário *online*, como o fornecido pelo servidor de 14, pode ser configurado para aceitar um número de conta como o nome de usuário ou ID do *login* do usuário associado à conta. Se o número da conta for válido e corresponder a um cliente atual da instituição financeira, o usuário então fornece uma senha. Como conhecido acima, esta informação é tipicamente estática e pode conduzir a um acesso não autorizado à conta do usuário podendo a informação tornar-se comprometida. Portanto, tal sistema bancário

online pode ser configurado em vez de aceitar um número gerado da forma descrita acima, como ambas as identificações de ID do *login* do usuário e uma senha.

Na presente realização descrita, o servidor 14 estabelece um ID único para cada conta mantida pela instituição financeira responsável pelo servidor 14. O ID exclusivo também é armazenado no dispositivo do usuário, tal como o dispositivo do usuário 12. Embora o ID único possa ser qualquer valor alfanumérico de qualquer comprimento, ele é de seis dígitos numéricos no exemplo atual, de modo que ele possa ser substituído pelo BIN associado com a instituição financeira, como explicado em maiores detalhes abaixo. Isso permite que o usuário insira um valor numérico com o mesmo número de dígitos como o número da conta do usuário, mas sem fornecer o número da conta real. Como resultado, um sistema bancário *online* configurado para solicitar um número de conta do usuário como ID do *login* do usuário não precisa ser aperfeiçoado para aceitar um valor não numérico ou um valor com um comprimento para um nome de usuário ou ID diferente do comprimento do número da conta real. Por exemplo, o BIN de um número de conta é usado para identificar a instituição financeira responsável pelo tratamento de uma transação financeira envolvendo a conta, como descrito acima. Como o usuário intencionalmente visita o sistema bancário *online* para uma determinada instituição financeira, a instituição já é conhecida. Assim, a informação utilizada para encaminhar os dados de transações financeiras para a entidade correta, tal como o BIN, torna-se desnecessário. Esses dígitos no número gerado podem ser substituídos com o ID único que identifica a conta do usuário.

Assim, o ID único que corresponde a uma conta de usuário é armazenado no servidor 14 e no dispositivo do usuário 12. O usuário,

em seguida, gera um número de um modo semelhante ao descrito acima, exceto o ID único que é colocado na posição previamente reservada para o BIN. Fazendo referência à figura 2, por exemplo, a porção reservada para o BIN é preenchido com o ID único correspondente à conta, na etapa 122, antes de ser adicionado ao PAN.

Quando o usuário visita o sistema bancário *online* hospedado pelo servidor 14, o usuário é solicitado para fornecer o número da conta. Usando o dispositivo 12, o usuário gera um número utilizando um dos processos descritos acima em relação às figuras 2 e 4 a 7 e o fornece ao sistema. O servidor 14 identifica o usuário baseado nos seis primeiros dígitos (que é o ID único que substituiu o BIN), e em seguida, tenta autenticar o usuário. Isto é, o servidor 14 decodifica o restante do número utilizando os métodos descritos acima. Se o servidor 14 autoriza e aceita o número como legítima, o sistema bancário *online* oferece ao usuário o acesso à conta correspondente.

Desta forma, o número é disposto de modo a identificar e autenticar o usuário, sem modificar substancialmente os requisitos do sistema mantido pelo fornecedor da conta do usuário. Isto é, se o sistema aguarda um número com um arranjo específico, tal como um número de cartão de crédito, um número que é com tempo limite, de uso limitado ou ambos podem ser gerados exibindo o arranjo aguardado. O número, no entanto, fornece a capacidade de identificar e autenticar o usuário ou a conta e pode então ser descartado, a fim de impedir o roubo de impostor. Deve ser entendido, no entanto, que a descrição acima também fornece um modo pelo qual um usuário pode ser unicamente identificado e autenticado por um valor alfanumérico de qualquer comprimento. Isto é, o ID gerado pode compreender qualquer quantidade de dígitos numéricos, alfabéticos ou alfanuméricos. Por exemplo, o dispositivo do usuário 12 pode gerar um ID para um usuário

acessar uma conta mantida em uma entidade que não requer um arranjo específico de números ou caracteres. Em tal realização, o dispositivo do usuário 12 gera um ID para o usuário, que inclui uma porção de dígitos alfanuméricos para identificar o usuário e uma parte de dígitos alfanuméricos de autenticação do usuário. Ambas as partes podem então ser codificadas e transmitidas como descrito acima. A entidade então decodifica, identifica e autentica o usuário se o ID for legítimo. Deve ser entendido que as partes do ID gerado devem ser numéricos, a fim de ser codificado por meio dos processos descritos acima. Entretanto, também deve ser entendido que os valores alfanuméricos podem ser utilizados para estas partes quando um randomizador configurado para randomizar ambos os caracteres e números é usado.

Em uma realização, o servidor 14 impede que cada número gerado a partir da sua reutilização, uma vez que foi utilizado para acessar a conta do usuário, através do sistema bancário *online*, de um modo semelhante ao acima descrito. Por conseguinte, se o número fornecido pelo usuário para ter acesso ao sistema for comprometido ou roubado, após de ter sido usado, uma parte não autorizada impossibilita reutilizar o número de acesso à conta através do sistema. Em tal realização, onde cada número gerado pode ser utilizado apenas uma vez, em vez de gerando parte do número com base no período de tempo, o número é válido, como descrito acima em referência à figura 2, que essa parte do número é, em vez disso, baseada no tempo em que foi gerado. Assim, a parte do número com base no momento em que o número é gerado criou-se da mesma maneira como descrito acima com relação à figura 2, mas se refere ao tempo de geração ao invés do tempo de expiração. Nesta realização, o servidor 14 mantém uma lista dos últimos números fornecidos pelo usuário para acessar o sistema. Em

funcionamento, quando o usuário fornece um número ao servidor 14, o número é adicionado à lista. Se uma tentativa for feita para acessar o sistema utilizando um número já incluído na lista, o pedido é negado. Se essa tentativa for feita, o servidor 14 pode reportar tal acesso não autorizado, tais como, notificar o usuário por e-mail ou alertando as autoridades fisicamente localizadas nos arredores de onde se originou o pedido não autorizado via SMS.

Em outra realização, cada número gerado é associado com um período de tempo durante o qual o número é válido e pode ser utilizado como estabelecido acima. Assim, se um número gerado pelo usuário for comprometido ou roubado, uma pessoa não autorizada recebedora do número não é capaz de usá-lo uma vez que o período de tempo expirou ou extinguiu. A entidade mantenedora das contas correspondentes aos números gerados pelo dispositivo 12 tem a opção de permitir números de uso único, números com tempo limite ou ambos. Por exemplo, um dígito do número gerado pelo dispositivo do usuário 12 pode significar que o algoritmo foi usado para codificar partes do número, se desejado, e, portanto, pode identificar o algoritmo que deve ser utilizado pelo servidor 14 para decodificar o número. Isto inclui a possibilidade de tratar o número como um número de uso único ou com tempo limite.

Deve ser entendido que o dispositivo utilizado para acessar o sistema bancário *online* hospedado pelo servidor 14 através da WAN 34 pode ser diferente do dispositivo usado para gerar o número. Alternativamente, o usuário pode acessar o sistema *online* fornecido pelo servidor 14 usando o mesmo dispositivo como um configurado para gerar o número, como o dispositivo do usuário 12. Em tal realização, o dispositivo do usuário 12 pode ser configurado para fornecer automaticamente o número gerado para o sistema hospedado pelo

servidor 14 quando solicitado. Numa outra realização, o dispositivo do usuário 12 automaticamente tanto gera quanto fornece o número do sistema de hospedado pelo servidor 14, quando solicitado. Por exemplo, se o sistema for acessado através de um *login* de uma página de um *site*, o dispositivo do usuário 12 automaticamente gera e fornece o número para o *login* da página quando o *site* hospedado pelo servidor 14 for acessado pelo dispositivo do usuário.

Ainda, em outra realização, o usuário pode especificar um período de tempo durante o qual o número fornecido automaticamente ao sistema mantido pelo servidor 14 pode ser utilizado. Por exemplo, o usuário pode instruir o dispositivo do usuário 12 para gerar um número que pode ser utilizado durante um mês para fornecer ao usuário acesso ao sistema. O dispositivo do usuário 12, então, fornece automaticamente o número ao servidor 14 quando o usuário tenta acessar o sistema hospedado pelo servidor. Quaisquer tentativas de acessar o sistema utilizando o número após o período de tempo ter expirado são negadas. Adicionalmente, o usuário pode especificar onde o número do dispositivo pode ser utilizado com base em um identificador único associado com o dispositivo, tal como o dispositivo IMSI. Por exemplo, o usuário pode instruir o dispositivo do usuário 12 a gerar um número que é único para o dispositivo do usuário 12 e que apenas o dispositivo do usuário 12 possa usar para se conectar ao sistema hospedado pelo servidor 14. Assim, o sistema pertinente nega qualquer solicitação para acessar o sistema utilizando o número de um dispositivo diferente do dispositivo autorizado.

Em outra realização, o dispositivo do usuário 12 gera números configurados, como *logins*, senhas ou ambos, de um modo semelhante ao descrito acima para utilização com sistemas múltiplos. Por exemplo, quando o usuário deseja acessar um sistema configurado

para solicitar o número, o dispositivo do usuário 12 gera e fornece-o ao sistema. Quando o usuário deseja acessar outro sistema, o usuário gera outro número utilizando o dispositivo 12 e fornece-o ao segundo sistema. Desta forma, o usuário pode gerar um único *login* seguro ou ID para cada sistema que identifica o usuário e permite o acesso aos vários sistemas que exigem autenticação. De preferência, um dispositivo do usuário 12 inclui um módulo separado ou *applet* correspondente para cada instituição financeira ou outra entidade em que o usuário tenha uma conta. Os dados distribuídos acima descritos são fornecidos para o *applet* específico pela entidade a que corresponde o *applet*. Em tal realização, o usuário gera o número usando o *applet* correspondente à entidade mantenedora da conta que o usuário deseja acessar. Deve ser entendido que isto permite que cada entidade especifique adicionalmente o algoritmo de codificação e decodificação ou algoritmos para serem utilizados.

Em uma realização, o usuário informa o dispositivo do usuário 12, qual sistema do usuário deseja acessar. O dispositivo do usuário 12, em seguida, gera um número de um modo similar ao descrito acima, mas único para o sistema que o usuário deseja acessar. Isto é, o número gerado é associado ao sistema identificado e não pode ser usado para acessar sistemas ou outras instituições daquelas identificadas pelo usuário. Assim, caso o número seja comprometido ou roubado, uma pessoa não autorizada é incapaz de usá-lo para acessar os sistemas aos quais o usuário é um membro ou às contas dos usuários localizadas em outras instituições diferentes daquelas para o qual o número foi gerado.

Deve ser entendido que os processos descritos acima, adicionalmente, proporcionam um método para identificar exclusivamente e autenticar um usuário onde tal identificação e

autenticação são necessárias. Além disso, o número fornecido para identificar e autenticar o usuário pode ser configurado para ser utilizável para um período de tempo específico ou apenas para uso único, a fim de evitar fraudes ou roubo de identidade. Por exemplo, a fim de receber serviços de saúde de um prestador de cuidados médicos, um segurado fornece um número para o prestador gerado, de uma maneira semelhante à descrita acima, representativa no lugar do número da conta do seguro do usuário. Na busca de reembolso a partir do provedor do seguro do usuário, o prestador de serviços médicos transmite o número para o provedor de seguros, juntamente com informações sobre os serviços prestados pelo prestador de serviços médicos, tais como o nome e custo do serviço. Se o provedor de seguros identificar e autenticar o segurado utilizando o número, ele reembolsa o prestador de serviços médicos por pelo menos uma parte do(s) serviço(s) com base na apólice de seguro do segurado.

Neste exemplo, o número é então removido da lista de números disponíveis para identificar e autenticar o usuário e a conta de seguro do usuário. Como resultado, uma tentativa de se envolver em fraudes de seguros ou roubo de identidade com o número fornecido pelo segurado é frustrada. Por exemplo, se o prestador de serviços médicos tenta receber um reembolso por serviços que falsamente foram prestados ao segurado, utilizando o número anteriormente fornecido ao provedor de seguros, o número é inutilizável e indica que o prestador de serviços médicos está tentando receber os reembolsos a que não tem direito. O servidor 14 pode alertar o provedor do seguro, que pode fomentar uma investigação sobre as ações do prestador de serviços médicos. Além disso, em uma tentativa não autorizada de uma pessoa de receber serviços de saúde do prestador de serviços médicos, utilizando o número fornecido anteriormente pelo segurado, o número é

inutilizável, e o provedor de seguros alerta o prestador de serviços médicos deste fato e sugere que o provedor de investigue o indivíduo que está tentando utilizá-lo.

Embora uma ou mais realizações preferidas da invenção tenham sido descritos acima, deve ser entendido que qualquer e todas as realizações equivalentes da presente invenção estão incluídas dentro do escopo e do espírito das mesmas. As formas de realização representadas são apresentadas a título de exemplo apenas e não se destinam a limitações sobre o presente invento. Assim, deve ser entendido pelos técnicos no assunto que a presente invenção não se limita a estas formas de realização, uma vez que modificações podem ser realizadas. Portanto, é contemplado que qualquer e todas as realizações estão incluídas na presente invenção como dentro do escopo e do espírito das mesmas.

REIVINDICAÇÕES

1. MÉTODO PARA PROPORCIONAR ACESSO A UMA CONTA MANTIDA POR UMA INSTITUIÇÃO, **caracterizado** pelo fato de compreender as etapas de:

gerar, através de um dispositivo móvel, uma credencial de *login* derivada, porém, diferente, a partir de um número de conta que a instituição associou com a conta e proporcionou a um usuário da conta, de acordo com um algoritmo pré-determinado de conversão de modo que a credencial de *login* tem um mesmo número de dígitos que o número de conta e inclui dados identificando um tempo que é anterior a uma expiração da conta;

transmitir a credencial de *login* a partir do dispositivo móvel para um servidor mantido pela instituição através de uma rede de área ampla, e

em resposta à confirmação pela instituição de que a credencial de *login* recebida pela instituição da etapa de transmissão corresponde à conta, interagir com a conta a partir do dispositivo móvel através da rede de área ampla e do servidor.

2. MÉTODO, de acordo com a reivindicação 1, **caracterizado** pelo fato de que a confirmação compreende confirmar que o tempo não expirou, e, se o tempo estiver expirado, ainda, compreender a rejeição do acesso à conta.

3. MÉTODO PARA FORNECER ACESSO A UMA CONTA MANTIDA POR UMA INSTITUIÇÃO FINANCEIRA, **caracterizado** pelo fato de que a instituição financeira associa a conta com um usuário, um número de conta, um número de validação que a instituição financeira exige que seja fornecido pelo usuário para permitir o usuário acessar a conta, e um identificador que distingue a conta de outras contas mantidas pela instituição financeira, e onde o número de conta compreende, em um formato pré-determinado, um número de identificação de banco

associado à instituição financeira e um número que identifica a conta, o método compreendendo a etapa de:

gerar, através de um dispositivo móvel, uma credencial de *login* tendo um mesmo número de dígitos que o número de conta e sendo diferente do número de conta, onde a credencial de *login* compreende o número de validação;

transmitir a credencial de *login* do dispositivo móvel para um servidor mantido pela instituição financeira através de uma rede de área ampla;

transmitir o identificador do dispositivo móvel para o servidor através da rede de área ampla; e

em resposta à confirmação pela instituição financeira de que o número de validação na credencial de *login* recebido pela instituição financeira da primeira etapa de transmissão está associado com a conta, interagir com a conta do dispositivo móvel através da rede de área ampla e do servidor.

4. MÉTODO, de acordo com a reivindicação 1, **caracterizado** pelo fato de que

a etapa de geração compreende gerar, através do dispositivo móvel, uns sinais de autenticação derivados a partir de dados associados com a conta de acordo com um algoritmo pré-determinado de conversão,

gerar, pelo dispositivo móvel, uma credencial de *login* que compreende os sinais de autenticação e um identificador que identifica exclusivamente a conta, e

a etapa de interação compreende interagir com a conta com base na confirmação de que os sinais de autenticação certifiquem um usuário da conta baseado na identificação do usuário através do identificador único.

5. MÉTODO, de acordo com a reivindicação 3, **caracterizado** pelo fato de que, na etapa de geração, a credencial de *login* compreende o número de identificação de banco, em que a primeira e a

segunda etapas de transmissão são distintas uma da outra e em que o identificador compreende um nome de usuário e uma senha associados pela instituição financeira com o usuário.

6. MÉTODO, de acordo com a reivindicação 3, **caracterizado** pelo fato de que, na etapa de geração, a credencial de *login* compreende o identificador no lugar do número de identificação de banco no formato predeterminado, e em que a primeira e a segunda etapas de transmissão ocorrem simultaneamente ao transmitir a credencial de *login*.

7. MÉTODO, de acordo com a reivindicação 3, **caracterizado** pelo fato de que compreende, antes da etapa de geração, fornecer ao dispositivo móvel uma data de expiração desejada através da qual a credencial de *login* é válida para permitir a interação com a conta.

8. MÉTODO, de acordo com a reivindicação 7, **caracterizado** pelo fato de que a credencial de *login* inclui um número que corresponde à data de expiração.

9. MÉTODO, de acordo com a reivindicação 4, **caracterizado** pelo fato de que

na etapa de geração, os sinais de autenticação têm um mesmo número de dígitos que o número de conta, é diferente do número de conta, e compreende um número de validação que a instituição exige que seja fornecido por um usuário associado à conta para permitir ao usuário acessar a conta, e

a etapa de transmissão compreende ainda transmitir, para o servidor através da rede de área ampla, um identificador que a instituição associa ao usuário da conta.

10. MÉTODO, de acordo com a reivindicação 9, **caracterizado** pelo fato de que, na etapa de transmissão, os sinais de autenticação são submetidos em resposta a uma consulta da instituição para um nome de usuário através do servidor, e o identificador é uma senha

associada pela instituição ao usuário.

11. MÉTODO, de acordo com a reivindicação 1, **caracterizado** pelo fato de que os dados de tempo correspondem a uma data de expiração da credencial de *login*.

12. MÉTODO, de acordo com a reivindicação 1, **caracterizado** pelo fato de que os dados de tempo correspondem a um tempo em que a credencial de *login* é gerada.

FIGURA 1

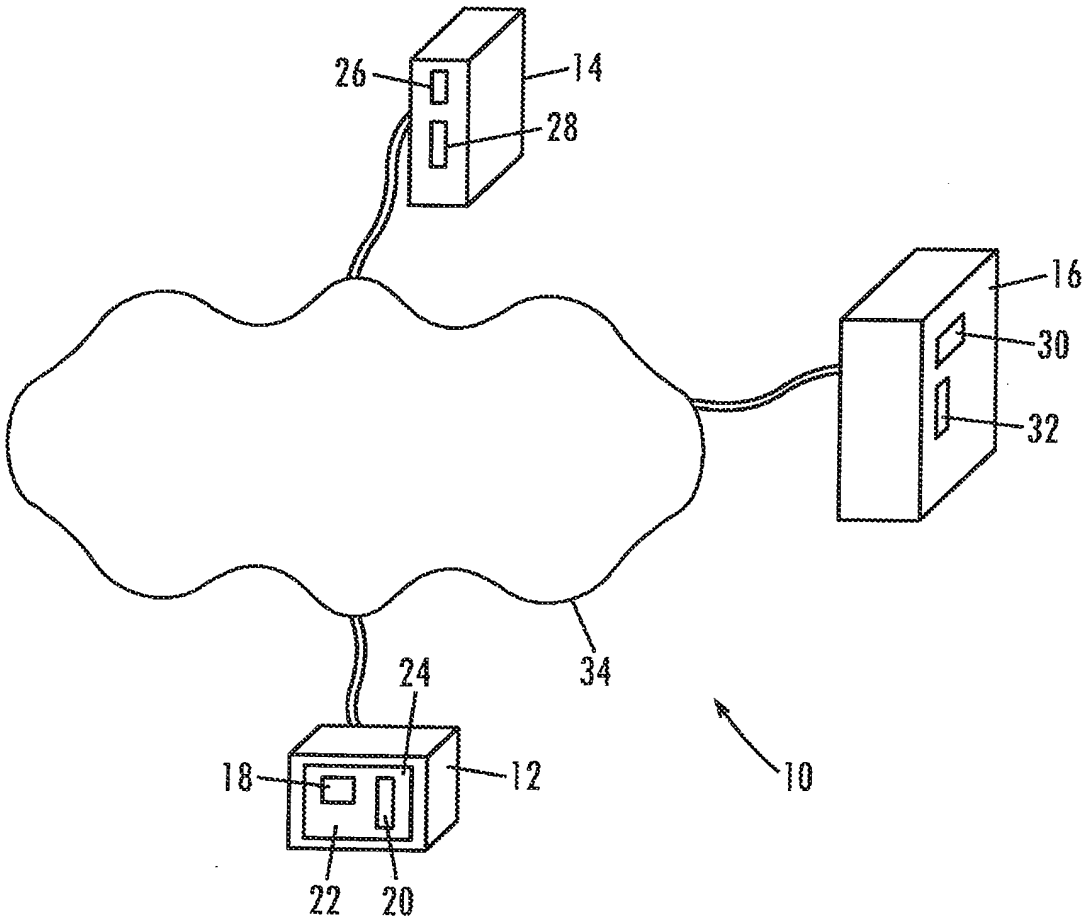


FIGURA 2

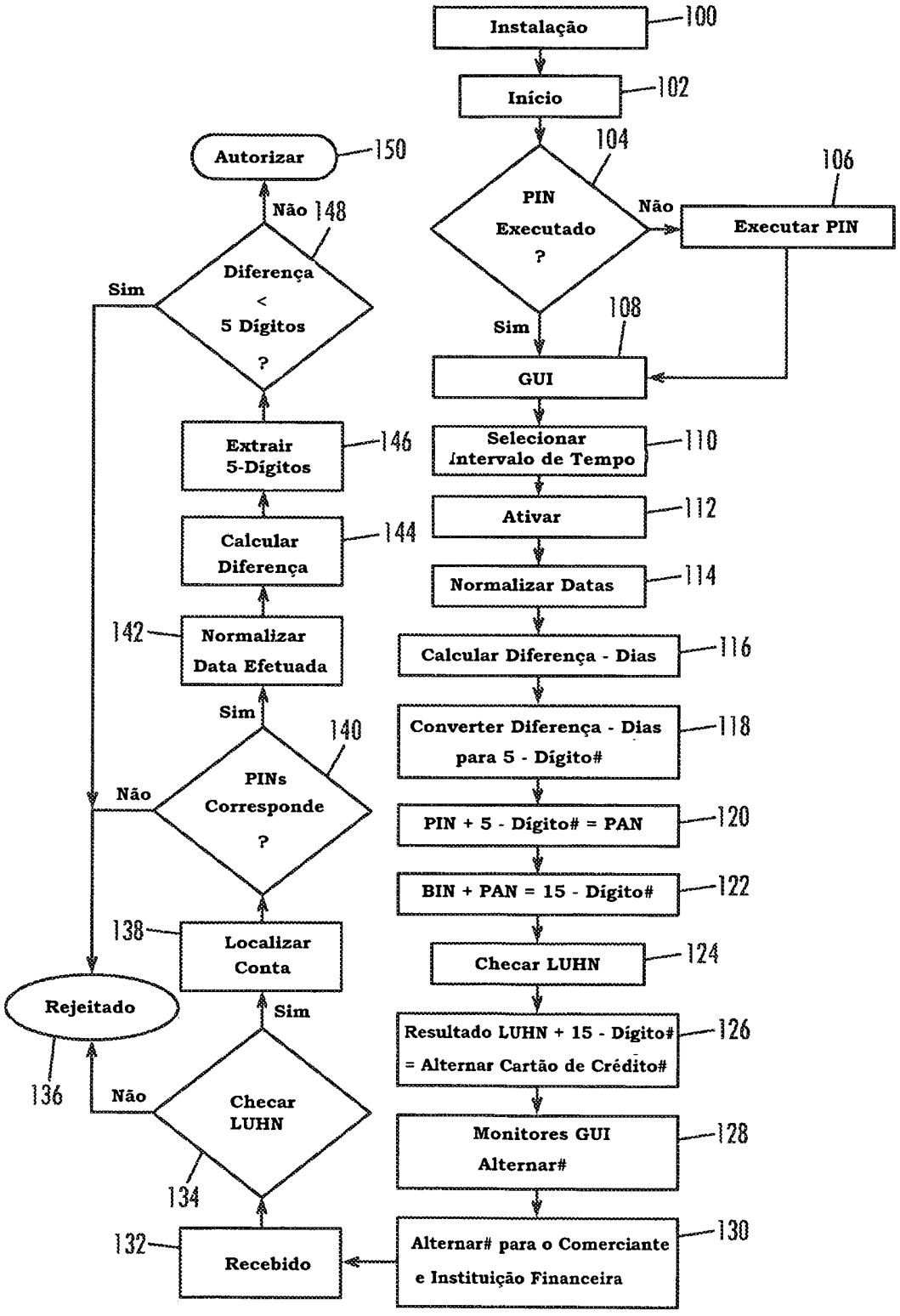

Instalação
100
Início
102
PIN Executado ?
104
Não
106
Executar PIN
Sim
108
GUI
Selecionar Intervalo de Tempo
110
Ativar
112
Normalizar Datas
114
Calcular Diferença - Dias
116
Converter Diferença - Dias para 5 - Dígito#
118
PIN + 5 - Dígito# = PAN
120
BIN + PAN = 15 - Dígito#
122
Checar LUHN
124
Resultado LUHN + 15 - Dígito# = Alternar Cartão de Crédito#
126
Monitores GUI Alternar#
128
Alternar# para o Comerciante e Instituição Financeira
130
Recebido
132
Checar LUHN
134
Não
Sim
Rejeitado
136
Localizar Conta
138
PINs Corresponde ?
140
Não
Sim
Normalizar Data Efetuada
142
Calcular Diferença
144
Extrair 5-Dígitos
146
Diferença < 5 Dígitos ?
148
Não
Sim
Autorizar
150

FIGURA 3

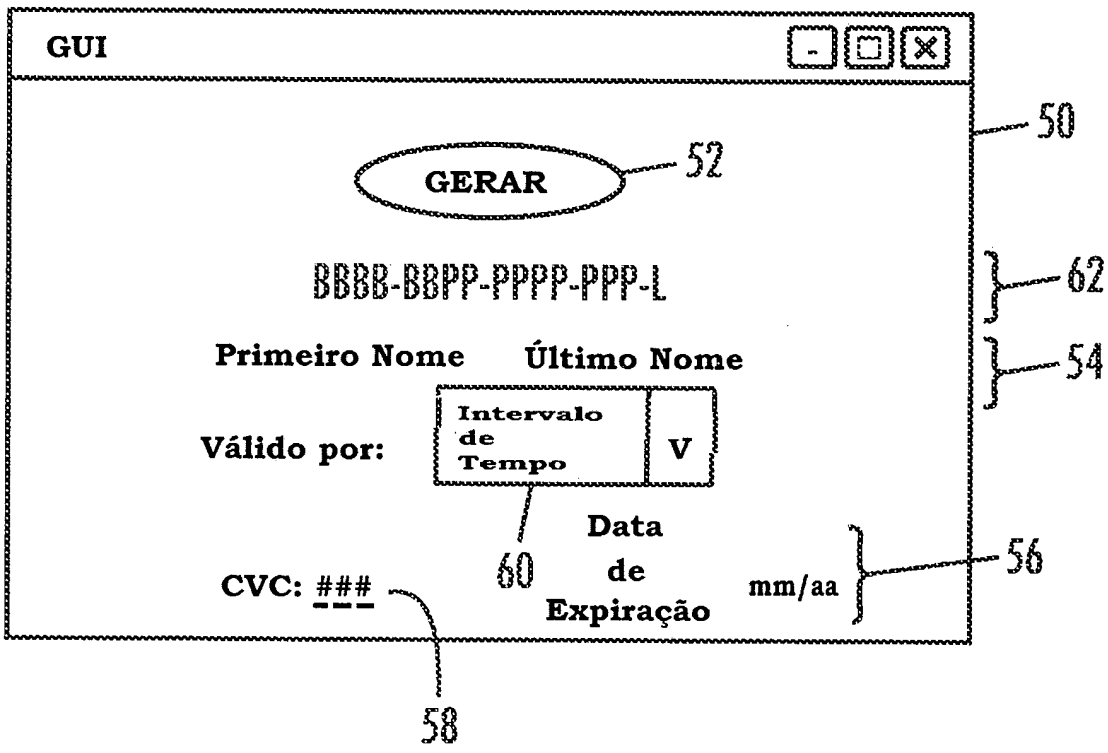

GUI
50
GERAR
52
BBBB-BBPP-PPPP-PPP-L
62
Primeiro Nome
Último Nome
54
Válido por:
Intervalo de Tempo
V
60
Data de Expiração
mm/aa
56
CVC: ###
58

FIGURA 4

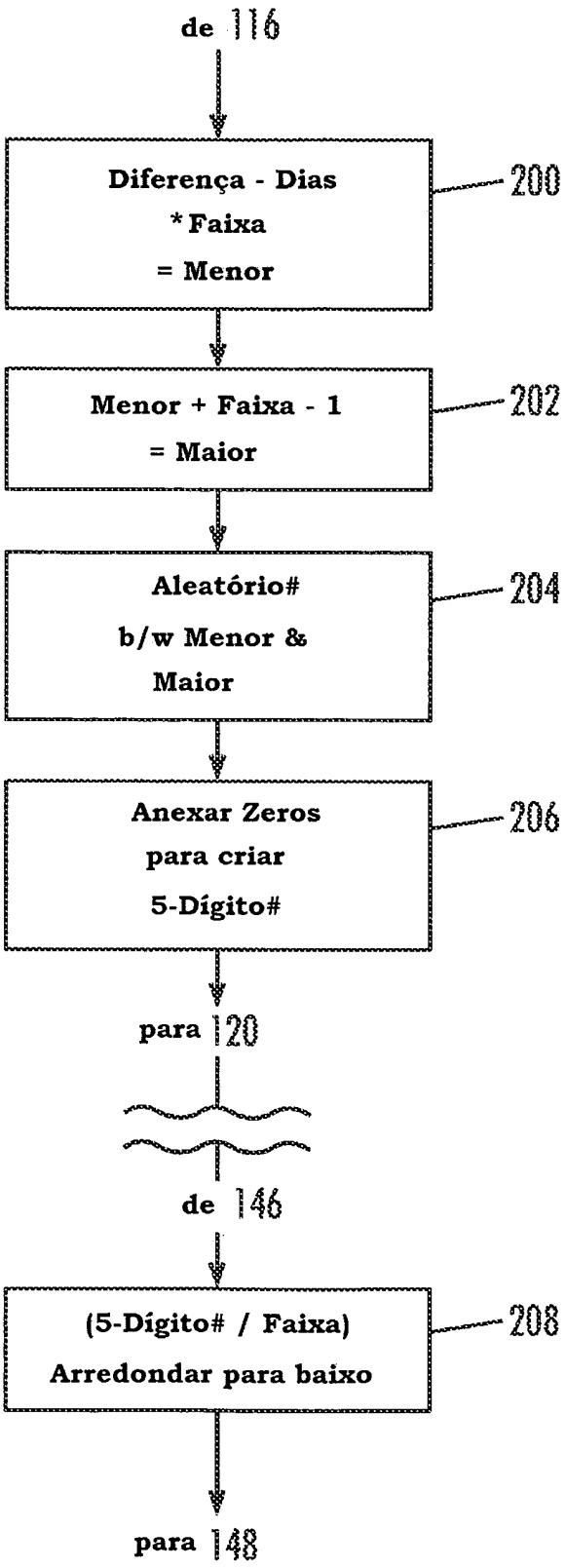

de 116
Diferença - Dias
* Faixa
= Menor
200
Menor + Faixa - 1
= Maior
202
Aleatório#
b/w Menor &
Maior
204
Anexar Zeros
para criar
5-Dígito#
206
para 120
de 146
(5-Dígito# / Faixa)
Arredondar para baixo
208
para 148

FIGURA 5

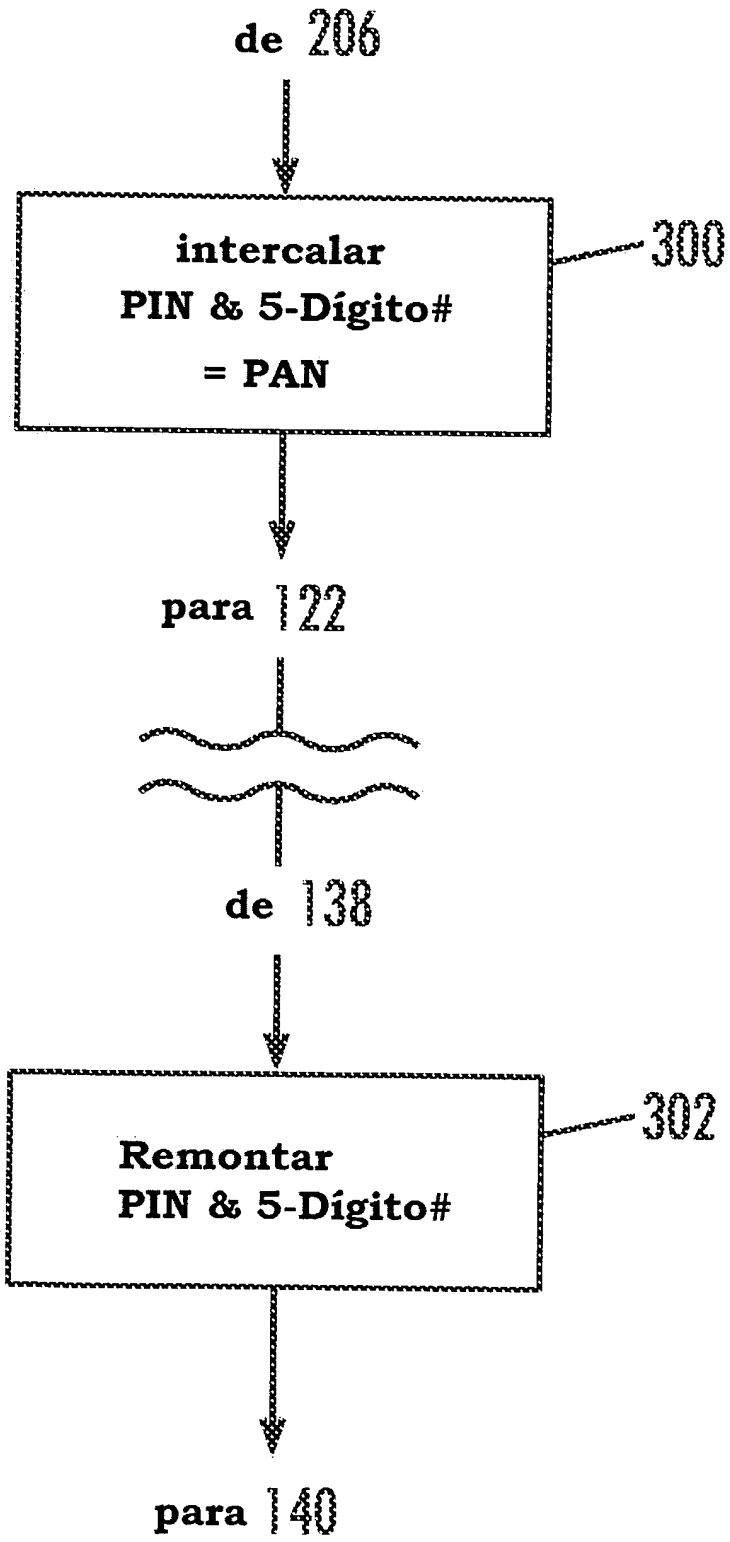

de 206
intercalar
PIN & 5-Dígito#
= PAN
300
para 122
de 138
Remontar
PIN & 5-Dígito#
302
para 140

FIGURA 6

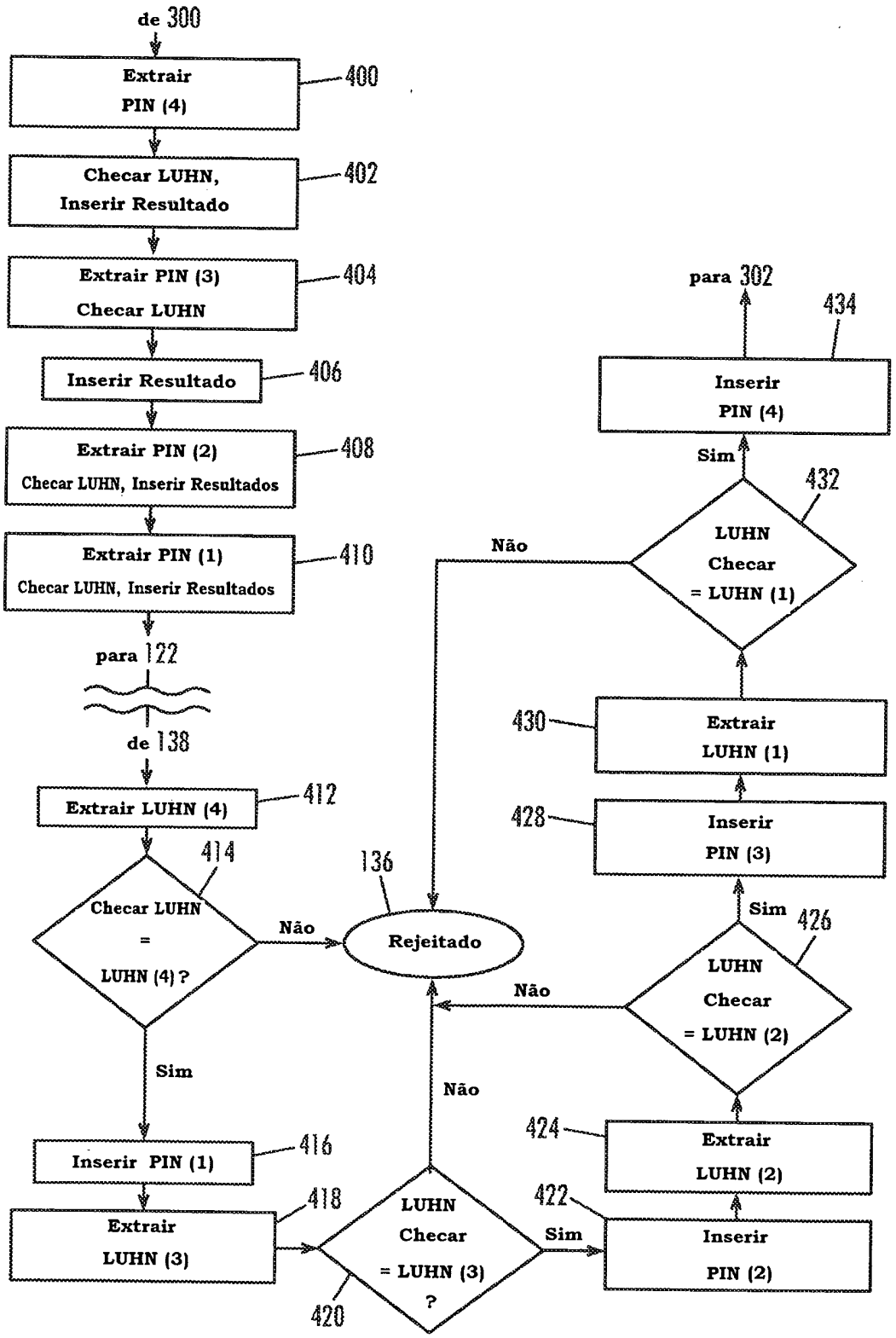
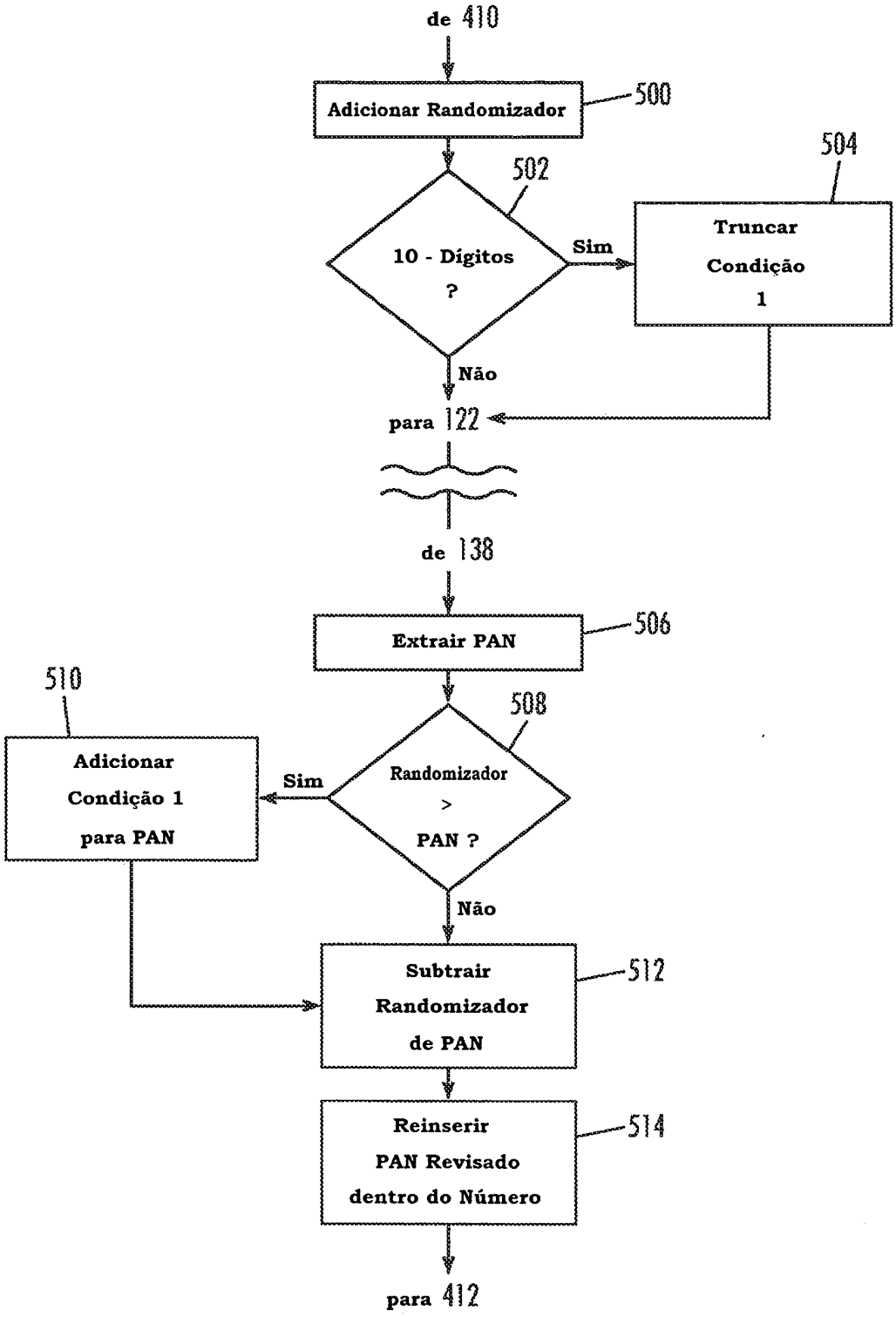

de 300
Extrair PIN (4)
400
Checar LUHN, Inserir Resultado
402
Extrair PIN (3) Checar LUHN
404
Inserir Resultado
406
Extrair PIN (2) Checar LUHN, Inserir Resultados
408
Extrair PIN (1) Checar LUHN, Inserir Resultados
410
para 122
de 138
Extrair LUHN (4)
412
Checar LUHN = LUHN (4)?
414
Não
136
Rejeitado
Sim
Inserir PIN (1)
416
Extrair LUHN (3)
418
LUHN Checar = LUHN (3) ?
420
Não
Sim
Inserir PIN (2)
422
Extrair LUHN (2)
424
LUHN Checar = LUHN (2)
426
Não
Sim
Inserir PIN (3)
428
Extrair LUHN (1)
430
LUHN Checar = LUHN (1)
432
Não
Sim
Inserir PIN (4)
434
para 302

FIGURA 7


de 410
Adicionar Randomizador
500
502
504
10 - Dígitos ?
Sim
Truncar Condição 1
Não
para 122
de 138
Extrair PAN
506
510
508
Adicionar Condição 1 para PAN
Sim
Randomizador > PAN ?
Não
Subtrair Randomizador de PAN
512
Reinserir PAN Revisado dentro do Número
514
para 412