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

(21) PI 0808185-9 A2

(22) Data de Depósito: 30/01/2008
(43) Data da Publicação: 05/08/2014
(RPI 2274)

(51) Int.Cl.:
G06Q 20/00

(54) Título: MÉTODOS E UM SISTEMA PARA PROVER INFORMAÇÕES RELATIVAS A TRANSAÇÕES

(57) Resumo:

(30) Prioridade Unionista: 01/02/2007 GB 07 01940.9

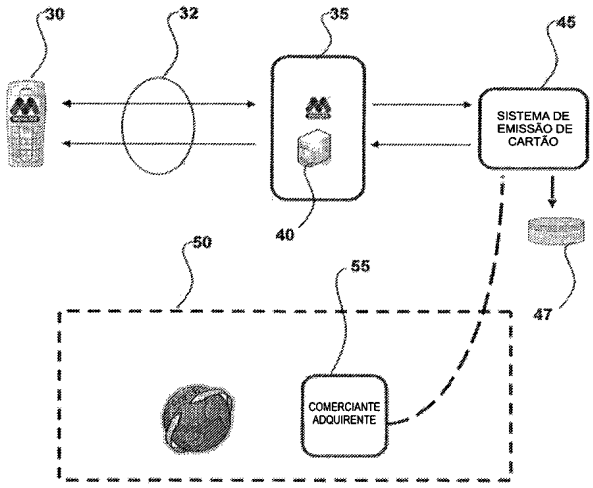
(73) Titular(es): Monitise Group Limited

(72) Inventor(es): Steven Atkinson

(74) Procurador(es): Dannemann ,Siemsen, Bigler & Ipanema Moreira

(86) Pedido Internacional: PCT GB2008050060 de 30/01/2008

(87) Publicação Internacional: WO 2008/093140de 07/08/2008



Relatório Descritivo da Patente de Invenção para **"MÉTODOS E UM SISTEMA PARA PROVER INFORMAÇÕES RELATIVAS A TRANSAÇÕES".**

A presente invenção refere-se a prover dados relativos a transações. Especificamente, a invenção refere-se a um método e sistema que proveem dados que representam os detalhes de um cartão de pagamento para utilização em um processo de transação ou de verificação.

Devido ao risco de fraudes, os consumidores ficam incomodados em suprir os detalhes de um cartão de pagamento (por exemplo, os detalhes de um cartão de crédito, de débito ou pré-pago) para utilização em transações comerciais, especificamente onde o detentor de cartão não está presente no ponto de transação. Enquanto que o nível de comércio eletrônico cresceu, as pesquisas indicam que este crescimento foi desacelerado por consumidores temendo fraudes e sua consequente relutância em prover os detalhes do cartão de pagamento pela Internet.

Mais ainda, os consumidores que não possuem cartões de débito ou de crédito experimentam dificuldades em completar as transações remotas, tais como pela Internet ou por telefone, já que eles são incapazes de suprir os comerciantes com os detalhes de pagamento para liquidar as transações.

É portanto desejável desenvolver um método e/ou sistema pelo qual um consumidor possa completar uma transação, enquanto reduzindo ou minimizando a exposição de detalhes de sua conta ou cartão pessoal ao risco de fraudes. É também desejável permitir aos consumidores que não possuem um cartão de débito ou de crédito utilizar tal método e/ou sistema.

No presente, é conhecido prover os dados que representam os detalhes de um cartão de pagamento os quais podem ser utilizados por consumidores para completar as transações pela Internet ou por telefone. Estes dados são de outro modo conhecidos como detalhes do cartão, e tipicamente compreendem um número de conta de 16 dígitos (Número de Conta Pessoal ou PAN), uma data de expiração, um código de segurança de 3 dígitos (CVV2) e algumas vezes uma data de início.

Os sistemas existentes que proveem tais detalhes do cartão, outros que de um próprio cartão, incluem alguns os quais requerem que um cliente primeiramente registre os seus detalhes pessoais utilizando a Internet antes que eles possam receber um cartão físico através do correio. Utilizando este cartão, o consumidor pode adquirir vouchers de valores predeterminados de um ponto de vendas de varejo os quais são então aceitos em transações de 'detentor de cartão não-presente' ("CNP") (onde quer que o logotipo VISA® seja exibido). Os vouchers são efetivamente cartões de pagamento descartáveis pré-pagos impressos como um recibo de papel ao invés de um cartão de crédito de plástico. Os consumidores podem utilizar um voucher para fazer numerosas comprar de CNP desde que eles não excedam o saldo disponível no voucher. Os fundos não despendidos podem ser resgatados, no entanto existe uma taxa de resgate fixa e os consumidores precisam aguardar por semanas ou mesmo meses para receber o reembolso.

Será apreciado que tais sistemas existentes estão restritos a transações específicas e podem ser inconvenientes, já que estes requerem que o usuário adquira os vouchers com antecedência da transação de um ponto de venda de varejo físico.

SUMÁRIO DA INVENÇÃO

De acordo com a invenção, está provido um sistema eletrônico que provê dados que representam os detalhes de um cartão de pagamento para utilização em uma transação, que compreende um servidor que tem:

uma primeira interface para comunicação com dispositivos de telefonia móvel por uma rede de telefone móvel; e

uma segunda interface para comunicação com um sistema de emissão de cartão para emitir os dados que representam os detalhes de um cartão de pagamento em resposta às informações comunicadas,

em que a primeira interface compreende:

um meio de recepção adaptado para receber uma solicitação para os dados que representam os detalhes de um cartão de pagamento de um usuário que opera um dispositivo de telefonia móvel; e

um meio de transmissão adaptado para prover os dados que representam os detalhes de um cartão de pagamento para um dispositivo de telefonia móvel,

e em que a segunda interface compreende:

um meio de transmissão adaptado para transmitir as informações para o sistema de emissão de cartão com base na solicitação; e

um meio de recepção adaptado para receber os dados que representam os detalhes de um cartão de pagamento do sistema de emissão de cartão.

A invenção também provê um método para solicitar os dados que representam os detalhes de um cartão de pagamento para utilização em uma transação, o método compreendendo as etapas de:

receber uma solicitação para os dados de um usuário que opera um dispositivo de telefonia móvel, o usuário selecionando as opções providas para o usuário pelo dispositivo de telefonia móvel; e

processar a solicitação e comunicar as informações para um sistema de emissão para emitir os dados que representam os detalhes de um cartão de pagamento em resposta à solicitação de dados.

De acordo com outro aspecto da invenção, está provido um método para gerar os dados que representam os detalhes de um cartão de pagamento para utilização em uma transação, o método compreendendo as etapas de:

receber de um intermediário as informações que compreendem os dados do usuário que incluem os dados de identificação de telefonia móvel; e

gerar os dados que representam os detalhes de um cartão de pagamento com base nos dados do usuário.

De acordo com ainda outro aspecto da invenção, está provido um método para suprir os dados que representam os detalhes de um cartão de pagamento para utilização em uma transação, o método compreendendo as etapas de:

comunicar os dados de um sistema de emissão de cartão para

um servidor que tem uma interface para comunicação com um dispositivo de telefonia do usuário por uma rede móvel; e

transmitir os dados pela rede de telefonia móvel para um usuário que opera um dispositivo de telefonia móvel.

A invenção permite que os consumidores comprem remotamente, através da Internet, pedido postal ou por telefone ou em um terminal de Ponto de Venda ("POS") sem precisar divulgar os detalhes de seu cartão de débito ou de crédito reais para o comerciante. Esta portanto minimiza o risco de fraude e pode ajudar os consumidores a superar a sua relutância em comprar de tais modos.

Além de não revelar os detalhes do cartão do consumidor, a invenção pode ainda diminuir o risco de fraude já que os detalhes do cartão que são emitidos podem ser válidos por um período de tempo limitado e por um valor fixo. Estas limitações podem ser selecionadas pelo usuário.

A invenção não requer que o consumidor tenha um cartão de débito ou de crédito, ou de fato qualquer conta de banco baseada em cartão, já que os detalhes do cartão podem ser gerados de, e relacionados com, informações relativas ao usuário, não requerendo um cartão de pagamento normal. A solução também permite que os detentores de cartão de caixa automático (isto é, os cartões que podem ser utilizados em um ATM, para sacar dinheiro, mas não podem ser utilizados como um cartão de débito) para empreender as transações de comércio eletrônico.

A invenção não requer que o comerciante emende as suas políticas, procedimentos ou sistemas, já que os detalhes do cartão providos podem ser processados como uma transação de cartão de débito ou de crédito normal.

BREVE DESCRIÇÃO DOS DESENHOS

Exemplos da invenção serão agora descritos em detalhes com referência aos desenhos acompanhantes, nos quais:

a Figura 1 mostra um procedimento de registro preferido para um sistema da invenção;

a Figura 2 mostra as etapas executadas por um usuário para

fazer uma solicitação de dados que representam os detalhes de um cartão de pagamento;

a Figura 3 mostra esquematicamente um exemplo de um sistema de acordo com uma modalidade da invenção; e

a Figura 4 mostra quatro exemplos de diferentes camadas de segurança presentes na comunicação dentro de um sistema de acordo com a invenção.

DESCRIÇÃO DETALHADA

A invenção provê um método e um sistema para prover um serviço que permite que os usuários solicitem e recebam com segurança os dados que representam os detalhes de um cartão de pagamento utilizando um dispositivo de telefonia móvel. Os dados que representam os detalhes de um cartão de pagamento podem então ser utilizados para participar em uma transação comercial, especificamente onde o usuário não está presente no ponto de transação.

Como o consumidor obtém acesso ao serviço e como um consumidor subsequentemente utiliza o serviço será agora descrito nas seções seguintes. Nas figuras e no texto seguinte, o termo "mobileATM®" pode ser utilizado, e este denota uma implementação de software do serviço/sistema da invenção. É claro, o serviço/sistema da invenção pode ser implementado utilizando produtos de software/hardware alternativos.

REGISTRO DO USUÁRIO

Por razões de segurança pode ser necessário que os usuários registrem-se para o serviço. Isto pode ser conseguido em um de dois modos; registrando através do site da Web de serviço ou registrando para o serviço diretamente de um telefone móvel. Uma vista geral de um processo de registro exemplar é dada na Figura 1, a qual mostra como um usuário registra-se para o serviço.

A Figura 1 mostra os quatro estágios requeridos para utilizar o serviço. No estágio 1, o usuário fica ciente da existência do serviço. No estágio 2, existe um processo de registro, e o estágio subsequente envolve uma senha sendo enviada para o usuário por correio. Isto provê uma cone-

xão entre o endereço de IP ou identidade móvel do usuário e o endereço postal, e por meio disto provê um nível adicional de segurança pela simples utilização anônima de um PC ou telefone móvel. Após o processo de registro, no estágio 4, o usuário é capaz de utilizar o serviço.

Uma vez registrados, os consumidores podem então começar a utilizar o serviço, e fazê-lo navegando para um menu de aplicativos em seu dispositivo de telefone móvel e executando um aplicativo requerido. Em um modo similar ao login em um serviço seguro ou uma Máquina de Caixa Automático (ATM) física, o usuário é requerido inserir um código numérico, ou Senha, a qual forma parte do processo de identificação.

SOLICITAÇÃO DE DETALHES DO CARTÃO DE PAGAMENTO

Uma vista geral de um processo exemplar que mostra como um usuário pode solicitar os detalhes de um cartão de pagamento está mostrada na Figura 2. As cinco imagens na Figura 2 mostram as seguintes operações:

(a) O usuário seleciona uma conta da qual eles desejam que os fundos sejam originados.

(b) O usuário seleciona "PAN de Valor Fixo" do submenu de serviços.

(c) O usuário seleciona o tipo de moeda desejado e então insere o valor requerido (o valor inserido aparece tanto em valores numéricos quanto em palavras para diminuir o risco de erros em teclagem manual). O usuário pode também ser provido com a opção de selecionar uma data de expiração (diminuindo adicionalmente o risco de fraude.

(d) O usuário é solicitado verificar os detalhes providos e confirmar a solicitação para os detalhes do cartão selecionando OK. A solicitação é comunicada para um servidor o qual provê um sistema de emissão de cartão com os detalhes necessários da solicitação que são requeridos para emitir os detalhes do cartão. Puramente como exemplo, os detalhes da solicitação podem compreender: moeda; valor; data de expiração; e detalhes do usuário, por meio disto permitindo que o sistema de emissão de cartão gere os detalhes do cartão únicos especificamente para aquele usuário.

(e) Utilizando os detalhes da solicitação, o sistema de emissão

de cartão gera alguns ou todos os detalhes do cartão (isto é, o número de conta de 16 dígitos, as datas de início e término, e um código de segurança CVV2 de três dígitos) e transmite os detalhes para o servidor. O servidor então criptografa e transmite com segurança os detalhes para o dispositivo de telefone móvel do usuário no qual estes são exibidos.

O usuário pode então utilizar os detalhes para representar um cartão de pagamento e completar o estágio de pagamento de uma transação.

Para evitar qualquer dúvida, deve ser compreendido que a operação acima pode ser completada em uma ordem diferente. Por exemplo, a ordem das etapas (a) e (b) pode ser invertida.

Quando o usuário seleciona "OK" em cada estágio do processo, as informações inseridas no aparelho manual são criptografadas e providas com segurança para o servidor e a próxima tela é exibida, solicitando uma entrada adicional. Deste modo, a quantidade de processamento empreendida pelo dispositivo de telefone móvel pode ser reduzida. Em modalidades alternativas, no entanto, a quantidade de processamento empreendida pelo telefone móvel pode depender do processamento empreendido pelo servidor. Por exemplo, o dispositivo de telefone móvel pode ser disposto para simplesmente transferir as entradas do usuário para o servidor, por meio disto empreendendo uma quantidade mínima de processamento. Ao contrário, o dispositivo de telefone móvel pode completar numerosas etapas de processamento sobre as entradas providas pelo consumidor, com somente um processamento mínimo sendo requerido pelo servidor. Assim, um balanceamento pode ser feito entre o dispositivo de telefone móvel e o servidor em termos das especificações de processamento.

Uma descrição de uma implementação preferida do sistema da invenção segue agora. Uma vista geral de alto nível de tal sistema está mostrada na Figura 3.

1. O usuário seleciona o serviço/aplicativo mobileATM® no telefone móvel 30 e insere um Número de Identificação Pessoal (PIN) para propósitos de segurança. O PIN é criptografado e transmitido com segurança

através de uma rede de telefone móvel 32, para o servidor Monitise 35 para autenticação. O usuário é individualmente identificado e verificado pelo servidor Monitise utilizando um banco de dados 40 o qual armazena as informações relativas aos usuários registrados. Tais informações podem incluir; a identidade de um usuário de um dispositivo de telefonia móvel; outros detalhes do contato do usuário do dispositivo de telefonia móvel; detalhes relativos à identidade do dispositivo de telefonia móvel (por exemplo, a identidade de cartão de módulo de identificação de assinante (SIM) ou Número de Diretório de Assinante Internacional de Estação Móvel (MSISDN)); uma senha provida pelo usuário; detalhes do cartão para o usuário; e um identificador de conta de banco determinado por uma organização bancária.

2. O telefone móvel 30 comunica com o servidor Monitise 35 e o usuário é conduzido através de um número de telas de menu para solicitar os detalhes do cartão (como acima descrito com referência à Figura 2). A solicitação resultante pelos detalhes do cartão providos pelo usuário é transmitida para o servidor 35 utilizando o protocolo de comunicação seguro (além do nível de segurança de rede móvel) e recebido pelo servidor 35.

3. O servidor 35 provê um sistema de emissão de cartão 45 com os detalhes da solicitação de modo que o sistema de emissão de cartão 45 possa gerar os detalhes do cartão que são únicos para a solicitação. Antes de gerar os detalhes do cartão, o sistema de emissão de cartão 45 pode comunicar com uma organização bancária 47 para solicitar os fundos requeridos da organização bancária. Se a organização bancária 47 verificar que a solicitação é válida (isto é, verifica se os fundos solicitados estão disponíveis), o sistema de emissão de cartão 45 continua com a geração dos detalhes do cartão solicitados.

4. Com base nos detalhes providos na solicitação, o sistema de emissão de cartão 45 gera os detalhes do cartão (isto é, o número de conta de 16 dígitos, as datas de início e término, e um código de segurança CVV2 de três dígitos) e transmite os detalhes gerados para o servidor 35. O sistema de emissão de cartão pode também transmitir os detalhes que incluem o valor e a moeda.

5. O servidor 35 então criptografa e transmite com segurança os detalhes do cartão (e possivelmente o valor e a moeda) para o telefone móvel 30 do usuário, através da rede de telefone móvel 32, no qual estes são exibidos.

6. Quando do recebimento dos detalhes do cartão solicitados, o usuário pode confirmar o recebimento seguro e fazer com que o telefone móvel 30 transmita uma mensagem de confirmação para o servidor 35, por meio disto terminando a seção do serviço/aplicativo.

O usuário pode fazer uso dos detalhes do cartão em uma transação de detentor de cartão não-presente. Em tal transação, os detalhes do cartão podem ser processados no mesmo modo que os detalhes de um cartão de débito/crédito real são processados. Por exemplo, em um ambiente de comércio eletrônico (como indicado genericamente por uma caixa tracejada 50), um usuário pode prover os detalhes do cartão para um comerciante 55 para completar o pagamento para um item/serviço. Em um modo similar em que os esquemas de pagamento de cartão existentes são liquidados, o comerciante 55 consulta o sistema de emissão de cartão 45 o qual pode então autorizar e liquidar o pagamento com referência aos detalhes do cartão.

Em modalidades alternativas da invenção, o servidor 35 pode ser disposto para atuar como uma porta para os registros bancários de pelo menos uma organização bancária. Deste modo, o servidor 35 pode ser utilizado para autorizar e liquidar os pagamentos com referência aos detalhes do cartão.

Ainda, como definido por uma data de expiração que pode ser incluída nos detalhes do cartão, os detalhes do cartão podem ser definidos de modo que estes sejam somente válidos por um período de tempo predeterminado. Por exemplo, enquanto que os cartões de débito ou de crédito típicos são tipicamente válidos por um período de tempo de 2 anos, os detalhes do cartão podem ser definidos para serem válidos por menos do que 1 ano, menos do que 6 meses, menos do que 1 mês, etc. Em uma modalidade preferida, os detalhes de cartão podem ser válidos por menos do que 1 dia. Mais de preferência, o usuário pode especificar a data e/ou o tempo de expi-

ração dos detalhes do cartão.

MODELO DE SEGURANÇA DE PONTA A PONTA

Uma consideração de projeto primária para um sistema e/ou serviço de acordo com a invenção é a segurança. Como mostrado na Figura 4, a invenção pode empregar um modelo de segurança de múltiplas camadas.

Na Figura 4, a parte A é uma vista geral de um Modelo de Segurança de Múltiplas Camadas para um Cliente de SIM a qual mostra que a segurança de nível de rede é provida pela criptografia de tráfego pelo ar do cartão SIM 60 e a camada de criptografia de PIN provê uma segurança de nível 3DES de Bloco de PIN para o PIN.

A parte B é uma vista geral do Modelo de Segurança de Múltiplas Camadas para um Cliente de Protocolo de Dispositivo de Informações Móveis (MIDP) 1.0, no qual a segurança foi adicionalmente aperfeiçoada para prover uma segurança de nível de rede mobileATM® além do nível de segurança de rede móvel. Este nível provê uma conexão como Camada de Soquetes Seguros (SSL) entre o aplicativo de telefone móvel e o servidor de mobileATM®.

A parte C é uma vista geral do Modelo de Segurança de Múltiplas Camadas para um Cliente de MIDP 2.0 no qual a segurança de rede foi adicionalmente melhorada pela provisão de um túnel de SSL diretamente do aparelho manual para o servidor de mobileATM®. Este modelo inclui um código de aplicativo assinado para tratar de ataques de homem no meio.

A parte D é um melhoramento adicional para um cliente de MIDP 2.0 com Suporte de Solicitação de Especificação Java (JSR) 177. Neste modelo, as tarefas de criptografia e decifração são executadas dentro do ambiente de SIM.

Como mostrado na Figura 4, os diferentes tipos de clientes permitem diferentes tipos de proteção de segurança. No entanto, em cada caso existe uma Criptografia de OTA, Tunelamento de SSL e criptografia de bloco de PIN, o que provê uma proteção de PIN 3DES.

As características de segurança gerais do serviço podem incluir:

- Nenhum dado de cartão de banco do cliente é armazenado no aplicativo do cliente.

- Nenhum dado de cartão de banco do cliente é armazenado na memória do aparelho manual.

- Informações insuficientes do cartão de banco são mantidas no mobileATM® no lado do servidor para clonar um cartão de banco ou executar uma Transação de Cartão Não-presente.

- O cliente seleciona a sua própria Senha.

- A Senha protege o canal de mobileATM® inteiro.

- O protocolo de mensagem empregado pelo mobileATM® pode ser uma resposta/solicitação de Protocolo de Transferência de Hipertexto (HTTP).

A camada de criptografia de nível de LTS (Segurança de Transporte Leve) pode ter os seguintes atributos:

- O túnel de criptografia de nível de LTS atravessa entre o aplicativo do cliente e o servidor de mobileATM®.

- O túnel de LTS pode impedir uma inserção, remoção, alteração ou reprodução de mensagem durante o transporte entre o cliente e o servidor.

- O cliente e o servidos contêm bibliotecas de criptografia personalizadas para prover o nível de segurança de LTS.

- A chave pública de LTS é armazenada no cliente ofuscado e pode ser de 2048 bits de comprimento.

- A chave de par de LTS tem uma vida máxima de 24 meses.

- Múltiplos pares de chaves de LTS RSA podem estar ativos concorrentemente.

A camada de criptografia de bloco de PIN pode ter os seguintes atributos:

- As Senhas estão associadas com a ID de usuário de mobileATM® às quais estas são relativas.

- O valor de deslocamento de Senha é um valor deslocado do PIN Natural gerado da ID de cliente utilizando a Chave de Criptografia Priva-

da de mobileATM® (PVK).

- O valor de Senha inserido pelo cliente não é mostrado na tela do aparelho manual durante a inserção.

- O valor da Senha mantida pelo mobileATM® é armazenado dentro do banco de dados de mobileATM® como um valor deslocado de PIN protegido pela PVK do mobileATM®.

- A PVK do mobileATM® é uma chave DES de comprimento duplo.

- Ao usuário serão concedidas cinco tentativas sucessivas para inserir corretamente a sua Senha no cliente.

- Cada Senha inserida pelo usuário será formada em um bloco de PIN ISO Formato-1 e criptografada com a Chave de Trabalho (WK) de mobileATM® antes do transporte para o servidor de mobileATM®.

-Após cinco tentativas consecutivas incorretas de inserção de Senha, a conta de mobileATM® para este cliente será bloqueada. Para obter acesso ao serviço, o cliente deve solicitar uma nova chave randômica a qual é postada para o seu endereço residencial.

- O servidor de mobileATM® utiliza um HSM (Módulo de Alta Segurança) Thales RG8000 (o qual é um componente de segurança bancária padrão) para verificar a Senha inserida pelo cliente criptografada em relação ao valor deslocado armazenado no banco de dados de mobileATM®.

VANTAGENS PROVIDAS PELA INVENÇÃO

Os detalhes do cartão podem ser utilizados para representar os detalhes de um cartão de pagamento para fazer compras pela Internet, pelo telefone, por pedido postal ou no ponto de venda, por exemplo. Assim, a invenção permite que os clientes façam compras tanto em um ambiente de detentor de cartão não-presente quanto de detentor de cartão presente, sem precisar divulgar os seus detalhes do cartão de débito ou de crédito e portanto ajuda a minimizar o risco de fraude. A utilização do serviço/sistema pode ser promovida por bancos e comerciantes para minimizar o risco de fraude e superar a relutância dos clientes em comprar on-line.

Além de não revelar os detalhes do cartão do cliente, a invenção

pode diminuir adicionalmente o risco de fraude já que os detalhes do cartão que são emitidos podem ser válidos por um período de tempo limitado e por um valor fixo.

A invenção pode também permitir aos clientes que não possuem cartões de débito ou de crédito comprar em um ambiente de detentor de cartão não-presente. Isto também beneficia os consumidores que tem "cartões de caixa automático" os quais podem ser utilizados para retirar dinheiro de ATMs mas não oferecem uma funcionalidade de cartão de débito.

Os usuários da invenção podem ser capazes de solicitar os detalhes do cartão e prover estes para a família ou amigos permitindo-os fazer uma compra. Os detalhes do cartão podem ser providos ou como um presente ou puramente para facilitar uma transação onde o recebedor não tem acesso a um cartão de débito ou de crédito.

CARACTERÍSTICAS DO SISTEMA

As características notáveis que podem ser providas por um sistema de acordo com a invenção incluem as seguintes: [Dan, algumas destas são características opcionais]

- Um PIN ou Senha é requerido para entrar e utilizar o sistema/serviço.

- Uma solicitação de detalhes do cartão pode ser provida para o servidor de um telefone móvel através de um método de entrega seguro e criptografado.

- Os detalhes do cartão podem ser providos para o usuário de um telefone móvel através de um método de entrega seguro e criptografado.

- O usuário pode selecionar um valor para coincidir exatamente com o pagamento requerido, ao invés de um valor fixo incremental.

- O usuário pode selecionar de uma variedade de moedas.

- Uma data de expiração pode ser selecionada pelo usuário.

- A transação pode ser autorizada e liquidada da conta de banco do usuário ou do cartão de débito/crédito ao invés de pré-pagar um valor.

- O usuário pode selecionar, em tempo real, uma conta a ser utilizada como uma fonte de liquidação, e esta pode ser escolhida depen-

dendo da disponibilidade de fundos.

- os detalhes do Cartão podem ser gerados do ou estar relacionados com o código de classificação e número de conta de uma conta sem cartão (isto é, o sistema/serviço não requer que o usuário tenha um cartão de débito/crédito ou qualquer conta bancária baseada em cartão).

- O sistema/serviço pode não basear-se em pré-pagamento de um valor antes de utilizar os detalhes do cartão.

- O sistema/serviço permite uma geração e entrega em tempo real de detalhes do cartão em qualquer lugar e a qualquer tempo, os quais podem então ser utilizados para pagamento dentro de segundos.

- O risco de fraude pode ser adicionalmente reduzido permitindo ao usuário minimizar o tempo dentro do qual os detalhes do cartão podem ser utilizados e nominando um valor fixo ou limite de valor.

- Lidando com os medos dos consumidores referentes à fraude, a invenção pode ajudar reduzir a relutância do usuário em comprar on-line, por meio disto levando a um aumento no nível do e-comércio.

- A invenção não requer que o comerciante emende os seus procedimentos ou sistemas de política já que os pagamentos que utilizam os detalhes do cartão podem ser processados como transações de cartão de débito ou de crédito normais.

- O sistema/serviço é altamente seguro já que o procedimento de registro pode levar em conta a identidade do dispositivo de telefone móvel, uma senha provida pelo usuário e o endereço do usuário.

- Uma criptografia de Bloco de PIN 3DES é utilizada para a comunicação com o usuário.

- Um sistema de criptografia LTS é utilizado para a comunicação com o usuário.

Várias outras implementações serão, é claro, possíveis, e estas e outras modificações serão aparentes para aqueles versados na técnica.

REIVINDICAÇÕES

1. Sistema eletrônico que provê dados que representam os detalhes de um cartão de pagamento para utilização em uma transação, que compreende um servidor que tem:

uma primeira interface para comunicação com dispositivos de telefonia móvel por uma rede de telefone móvel; e

uma segunda interface para comunicação com um sistema de emissão de cartão para emitir os dados que representam os detalhes de um cartão de pagamento em resposta às informações comunicadas,

em que a primeira interface compreende:

um meio de recepção adaptado para receber uma solicitação para os dados que representam os detalhes de um cartão de pagamento de um usuário que opera um dispositivo de telefonia móvel; e

um meio de transmissão adaptado para prover os dados que representam os detalhes de um cartão de pagamento para um dispositivo de telefonia móvel,

e em que a segunda interface compreende:

um meio de transmissão adaptado para transmitir as informações para o sistema de emissão de cartão com base na solicitação; e

um meio de recepção adaptado para receber os dados que representam os detalhes de um cartão de pagamento do sistema de emissão de cartão.

2. Sistema de acordo com a reivindicação 1, em que a primeira interface é para comunicação com um cartão SIM e uma aplicação de software móvel de um dispositivo de telefonia móvel.

3. Sistema de acordo com qualquer reivindicação precedente, em que a primeira interface inclui um número de identificação pessoal ou um sistema de segurança de senha.

4. Sistema de acordo com a reivindicação 3, em que a primeira interface inclui uma criptografia de 3DES de Bloco PIN.

5. Sistema de acordo com qualquer reivindicação precedente, em que a primeira interface ainda inclui um sistema de criptografia de segu-

rança de transporte leve.

6. Sistema de acordo com qualquer reivindicação precedente, ainda compreendendo um banco de dados que armazena as informações relativas aos usuários do sistema.

7. Sistema de acordo com qualquer reivindicação precedente, em que o sistema implementa um processo de verificação de segurança verificando pelo menos um de: a identidade de um usuário de um dispositivo de telefonia móvel; a identidade do dispositivo de telefonia móvel [SIM/MSISDN]; uma chave ou senha provida pelo usuário; e um identificador de conta de banco determinado por uma organização bancária.

8. Sistema de acordo com a reivindicação 7, em que o sistema está adicionalmente adaptado para verificar um número de identificação pessoal de conta de banco acordado com a organização bancária.

9. Sistema de acordo com qualquer reivindicação precedente, em que as informações transmitidas para o sistema de emissão de cartão compreendem as informações relativas a pelo menos um de: a identidade de um usuário de um dispositivo de telefonia móvel; detalhes relativos à identidade do dispositivo de telefonia móvel; e uma chave provida pelo usuário; um saldo solicitado; um tipo de moeda; e uma data de expiração solicitada.

10. Rede de telefone móvel, que compreende:

um sistema de acordo com qualquer reivindicação precedente; e

uma pluralidade de dispositivos de telefonia móvel,

em que o sistema está disposto para comunicar com pelo menos uma organização bancária.

11. Rede de telefone móvel de acordo com a reivindicação 10, em que o servidor está disposto para atuar como uma porta para os registros bancários de pelo menos uma organização bancária.

12. Rede de telefone móvel de acordo com a reivindicação 10 ou 11, em que o sistema de emissão de cartão está disposto para atuar como uma porta para os registros bancários de pelo menos uma organização bancária.

13. Rede de telefone móvel de acordo com qualquer uma das

reivindicações 1 a 12, em que os dispositivos de telefonia móvel do usuário são operáveis para solicitar os dados que representam os detalhes de um cartão de pagamento para utilização em uma transação.

14. Método para solicitar os dados que representam os detalhes de um cartão de pagamento para utilização em uma transação, o método compreendendo as etapas de:

receber uma solicitação para os dados de um usuário que opera um dispositivo de telefonia móvel, o usuário selecionando as opções providas para o usuário pelo dispositivo de telefonia móvel; e

processar a solicitação e as informações de comunicação para um sistema de emissão para emitir os dados que representam os detalhes de um cartão de pagamento em resposta à solicitação de dados.

15. Método de acordo com a reivindicação 14, em que as informações comunicadas para o sistema de emissão de cartão compreendem as informações relativas a pelo menos um de: a identidade de um usuário de um dispositivo de telefonia móvel; detalhes relativos à identidade do dispositivo de telefonia móvel; e uma chave provida pelo usuário; um saldo solicitado; um tipo de moeda; e uma data de expiração solicitada.

16. Método de acordo com a reivindicação 15, em que a etapa de processar a solicitação compreende verificar pelo menos um de: a identidade de um usuário de um dispositivo de telefonia móvel; detalhes relativos à identidade do dispositivo de telefonia móvel; e uma chave provida pelo usuário.

17. Método de acordo com a reivindicação 15 ou 16, em que a etapa de processar a solicitação compreende verificar um número de identificação pessoal de conta de banco acordado com uma organização bancária.

18. Método de acordo com qualquer uma das reivindicações 14 a 17, em que a criptografia de 3DES de Bloco PIN é utilizada para a comunicação com o usuário.

19. Método de acordo com qualquer uma das reivindicações 14 a 18, em que um sistema de criptografia de LTS é utilizado para a comuni-

cação com o usuário.

20. Método para gerar os dados que representam os detalhes de um cartão de pagamento para utilização em uma transação, o método compreendendo as etapas de:

receber de um intermediário as informações que compreendem os dados do usuário que incluem os dados de identificação de telefonia móvel; e

gerar os dados que representam os detalhes de um cartão de pagamento com base nos dados do usuário.

21. Método de acordo com a reivindicação 20, em que os dados que representam os detalhes de um cartão de pagamento compreendem os dados de identificação do usuário.

22. Método para suprir os dados que representam os detalhes de um cartão de pagamento para utilização em uma transação, o método compreendendo as etapas de:

comunicar os dados de um sistema de emissão de cartão para um servidor que tem uma interface para comunicação com um dispositivo de telefonia do usuário por uma rede móvel; e

transmitir os dados pela rede de telefonia móvel para um usuário que opera um dispositivo de telefonia móvel.

23. Método de acordo com a reivindicação 22, em que a criptografia de 3DES de Bloco PIN é utilizada para a transmissão de dados entre o servidor e o usuário

24. Método de acordo com a reivindicação 22 ou 23, em que um sistema de criptografia de LTS é utilizado para a transmissão de dados entre o servidor e o usuário.

25. Método para prover os dados que representam os detalhes de um cartão de pagamento para utilização em uma transação, o método compreendendo as etapas de:

solicitar os dados de acordo com o método de qualquer uma das reivindicações 14 a 19;

gerar os dados de acordo com o método da reivindicação 20 ou

21; e

suprir os dados de acordo com o método de qualquer uma das reivindicações 22 a 24.

26. Sistema eletrônico que provê dados que representam os detalhes de um cartão de pagamento para utilização em uma transação, que compreende um servidor que tem:

uma primeira interface para comunicação com dispositivos de telefonia móvel do usuário por uma rede de telefone móvel; e

uma segunda interface para comunicação com um sistema de emissão de cartão para emitir os dados que representam os detalhes de um cartão de pagamento em resposta às informações comunicadas,

em que a primeira interface está adaptada para permitir que solicitações de dados que representam os detalhes de um cartão de pagamento sejam submetidas para o sistema de emissão de cartão e prover os dados que representam os detalhes de um cartão de pagamento para um usuário de um dispositivo de telefonia móvel.

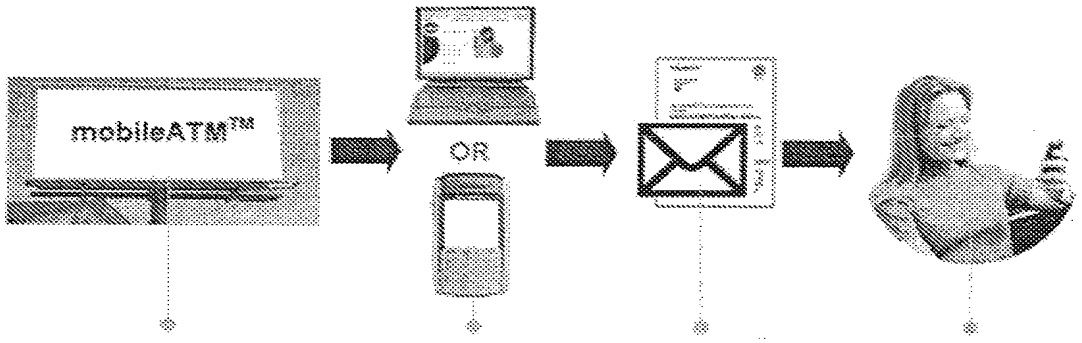
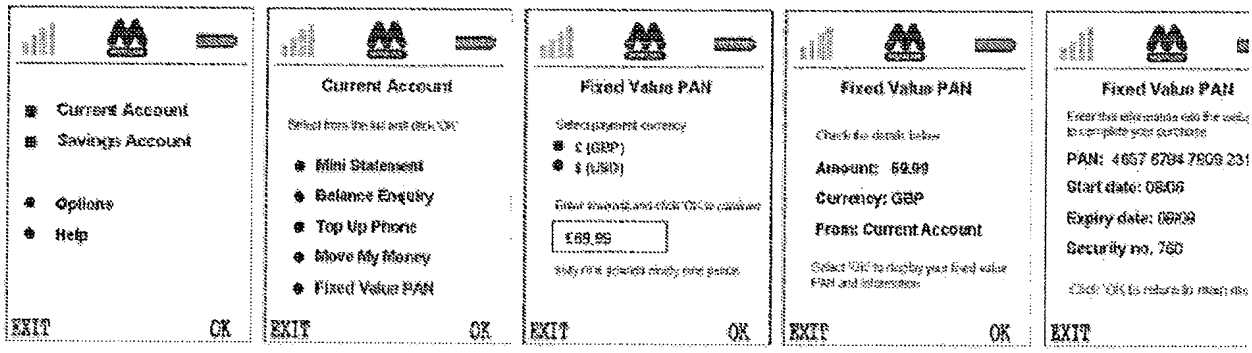

mobileATM™
OR
1 - CLIENTE FICA SABENDO SOBRE O mobileATM™ ATRAVÉS DE CAMPANHAS DE MARKETING
2 - O CLIENTE SE REGISTRA PARA O mobileATM™ ATRAVÉS DE PC OU TELEFONE MÓVEL
3 - UMA SENHA É ENVIADA PARA O CLIENTE POR CORREIO
4 - O CLIENTE UTILIZA O mobileATM™

FIG. 1


Current Account
Savings Account
Options
Help
EXIT
OK
Current Account
Mini Statement
Balance Enquiry
Top Up Phone
Move My Money
Fixed Value PAN
EXIT
OK
Fixed Value PAN
£ (GBP)
$ (USD)
£69.99
EXIT
OK
Fixed Value PAN
Amount: 69.99
Currency: GBP
From: Current Account
EXIT
OK
Fixed Value PAN
Start date: 0806
Security no. 760
EXIT

(a) (b) (c) (d) (e)

FIG. 2

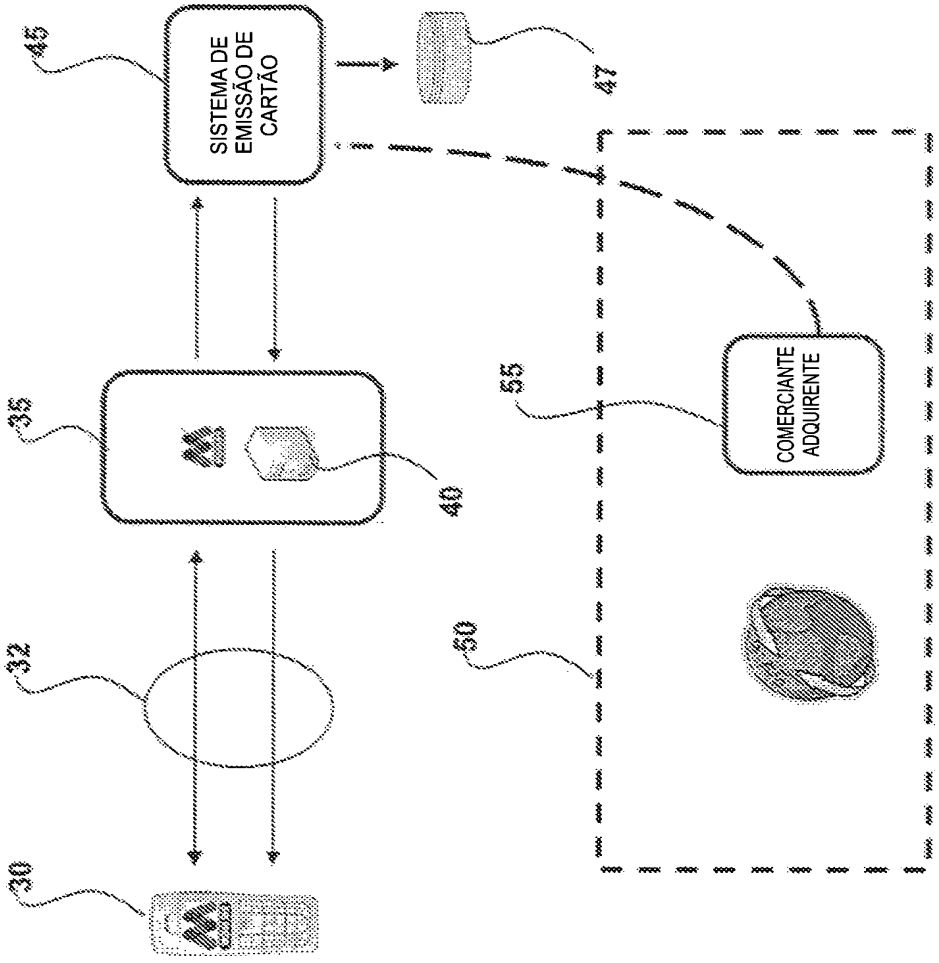

45
SISTEMA DE EMISSÃO DE CARTÃO
47
35
40
55
COMERCIANTE ADQUIRENTE
32
50
30

FIG. 3

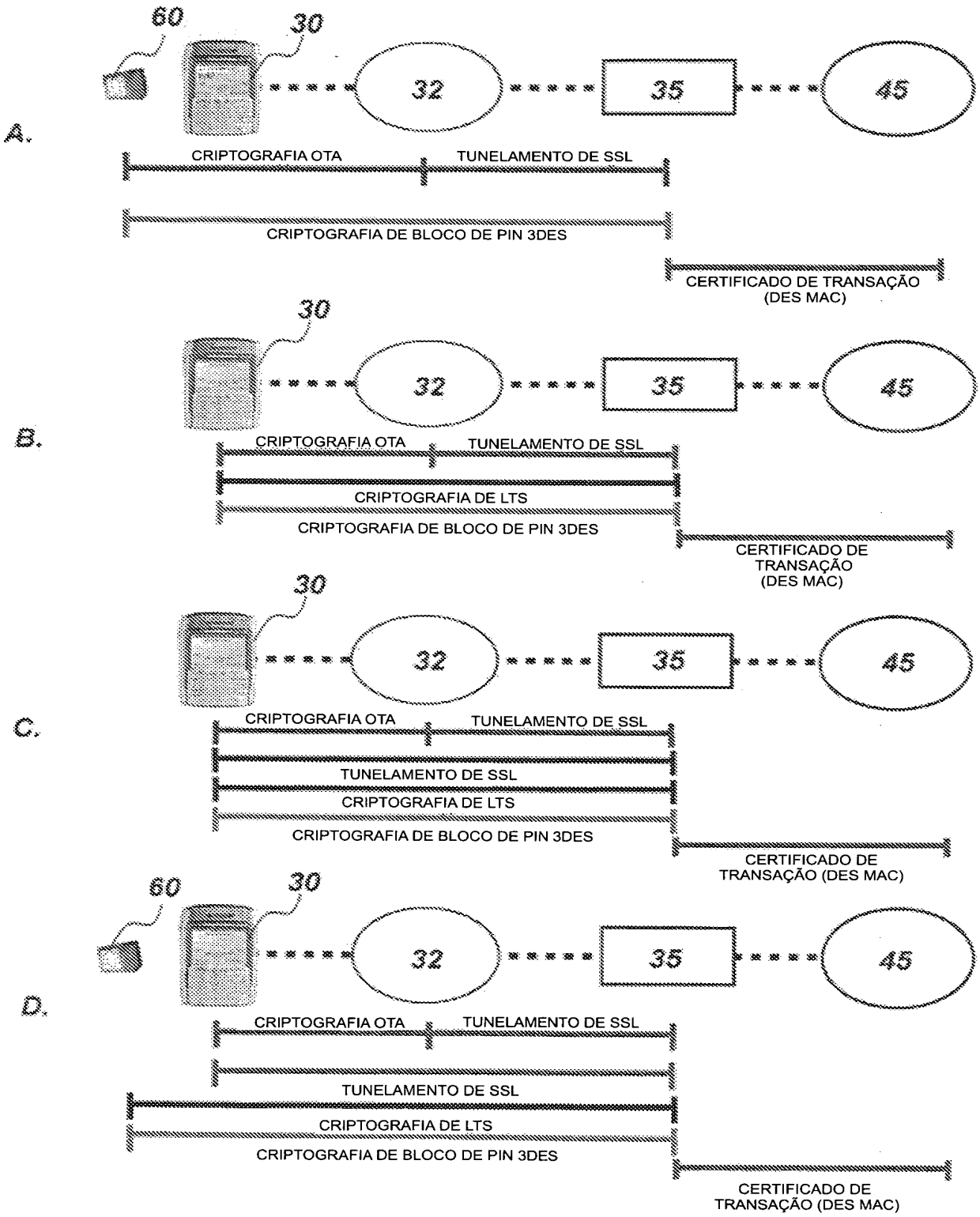

A.
60
30
32
35
45
CRIPTOGRAFIA OTA
TUNELAMENTO DE SSL
CRIPTOGRAFIA DE BLOCO DE PIN 3DES
CERTIFICADO DE TRANSAÇÃO (DES MAC)
B.
30
32
35
45
CRIPTOGRAFIA OTA
TUNELAMENTO DE SSL
CRIPTOGRAFIA DE LTS
CRIPTOGRAFIA DE BLOCO DE PIN 3DES
CERTIFICADO DE TRANSAÇÃO (DES MAC)
C.
30
32
35
45
CRIPTOGRAFIA OTA
TUNELAMENTO DE SSL
TUNELAMENTO DE SSL
CRIPTOGRAFIA DE LTS
CRIPTOGRAFIA DE BLOCO DE PIN 3DES
CERTIFICADO DE TRANSAÇÃO (DES MAC)
D.
60
30
32
35
45
CRIPTOGRAFIA OTA
TUNELAMENTO DE SSL
TUNELAMENTO DE SSL
CRIPTOGRAFIA DE LTS
CRIPTOGRAFIA DE BLOCO DE PIN 3DES
CERTIFICADO DE TRANSAÇÃO (DES MAC)

FIG. 4

RESUMO

Patente de Invenção: **"MÉTODOS E UM SISTEMA PARA PROVER INFORMAÇÕES RELATIVAS A TRANSAÇÕES".**

A presente invenção refere-se a métodos e um sistema para prover um serviço que permite aos usuários solicitar e receber com segurança os dados que representam os detalhes de um cartão de pagamento utilizando um dispositivo de telefonia móvel. Os dados que representam os detalhes de um cartão de pagamento podem então ser utilizados para participar em uma transação comercial na qual o usuário não está presente no, ou remotamente localizado do, ponto de transação.