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

(21) PI 1005627-0 A2

* B R P I 1 0 0 5 6 2 7 A 2 *

(22) Data de Depósito: 20/12/2010
(43) Data da Publicação: 11/02/2014
(RPI 2249)

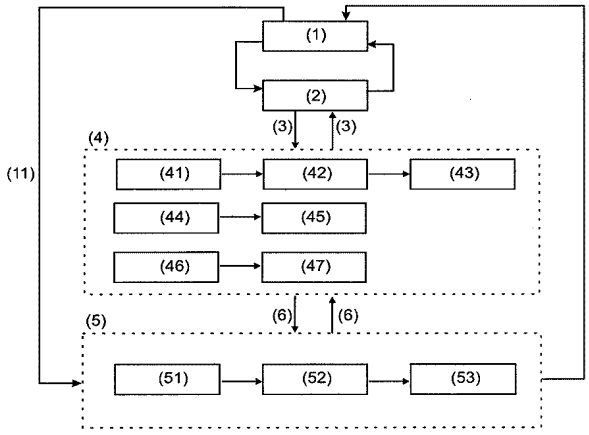
(51) Int.Cl.:
G06Q 20/08
G06F 21/44

(54) Título: SISTEMA EMBARCADO EM HARDWARE PARA CERTIFICAÇÃO DE IDENTIFICAÇÃO E MÉTODO DE CERTIFICAÇÃO DE IDENTIFICAÇÃO MÓVEL UTILIZANDO O DITO SISTEMA

(73) Titular(es): Arthur Philip Sander Junior

(72) Inventor(es): Arthur Philip Sander Junior

(57) Resumo: SISTEMA EMBARCADO EM HARDWARE PARA CERTIFICAÇÃO DE IDENTIFICAÇÃO E MÉTODO DE CERTIFICAÇÃO DE IDENTIFICAÇÃO MÓVEL UTILIZANDO O DITO SISTEMA, descreve um sistema de certificação de identificação móvel, denominado de "Sistema CIM", para autenticação de senhas junto a serviços fornecidos por meios eletrônicos e equipamentos específicos, compreendido por um software de identificação, denominado de "programa único", embarcado em aparelho celular ou outro dispositivo de comunicação remota, juntamente com um software de autenticação embarcado em outro dispositivo/sistema que necessite segurança, como por exemplo, um banco, um cofre ou um veículo, e o "sistema CIM" vai identificar e autenticar o usuário de um serviço/equipamento através da comunicação entre o "programa único" com o software de autenticação embarcado no dispositivo/sistema que necessite segurança; e a comunicação é através da confirmação da identificação por meio da comunicação do "programa único" com o software de autenticação, por um meio de comunicação alternativo àquele utilizado pelo dispositivo/sistema para requisição do acesso/emissão da ordem/autenticação ou autorização da transação.



SISTEMA EMBARCADO EM HARDWARE PARA CERTIFICAÇÃO DE IDENTIFICAÇÃO E MÉTODO DE CERTIFICAÇÃO DE IDENTIFICAÇÃO MÓVEL UTILIZANDO O DITO SISTEMA

O presente relatório de pedido de patente descreve um sistema de certificação de identificação móvel, doravante denominado de "Sistema CIM", que consiste numa forma alternativa para autenticação junto a serviços fornecidos por meios eletrônicos e junto a equipamentos específicos, se posicionando como um modelo intermediário entre o tradicional 'login e senha' passível de captura e utilização indevida, e a Certificação Digital, que ainda não é acessível à grande parte da população. Trata-se de um sistema de autenticação pessoal, pela utilização de um programa único instalado num celular, ou outro equipamento específico, do usuário, como portador de todas suas 'chaves' de convênios, tornando-o um aglutinador de autenticações em serviços, destinado a todos os usuários de tecnologias e empresas prestadoras de serviços que necessitem de segurança em suas relações, e aplicável desde um serviço de e-mail na internet, uma compra via internet, caixas automáticos ATM a internet banking.

Existem inúmeros sistemas e métodos de certificação e autenticação digital, cada qual apresentando seu diferencial técnico, construtivo e de funcionamento conferindo, para cada um, vantagens para aplicações específicas e desvantagens para outras aplicações. Cabe citar uma variedade de sistemas e métodos encontrados em banco de patentes, a fim de entendermos de forma mais clara o sistema e o método objeto do presente relatório.

O documento de patente PI0305273-7 descreve um sistema e método para transmitir informação reduzida de um certificado para executar operações de criptografia, que basicamente se baseia em um certificado digital dividido em

duas partes, onde uma fica junto ao cliente e outra junto ao provedor do serviço, e é destinado à criptografar mensagens trocadas entre dois ou mais pontos. O documento de patente PI051 7168-7 descreve um método para transmissão de mensagens entre um emissor e ao menos um receptor, e sistema para implementação de tal método, que pode ser entendido como um processo criptográfico, onde existe um dado que é criptografado de um lado e decriptografado do outro, somado à forma que se dá a conversão dos dados. O documento de patente PI0802118-0 descreve um sistema de segurança de negócios na internet que envolve a utilização de certificados digitais e cartões inteligentes. O documento de patente PI9508716-8 descreve um método de controle de acesso e método de imposição de uma política de segurança em um sistema criptográfico, que se baseia em certificados digitais, onde "Uma transação de usuário no sistema só e considerada válida após o usuário receber a informação contida nos referidos certificados digitais". O documento de patente PI0305072-6 descreve um método para controlar a autenticação de um primeiro dispositivo para um segundo dispositivo, baseado um método de determinação ponto a ponto. O documento de pedido de patente JP2001022698 descreve um sistema e método para autenticação por telefone celular, sendo que o celular é ligado num PC com o autenticador local para utilização do equipamento. O documento de patente KR20020088155 descreve um método para certificação de um usuário de internet por meio de um telefone com sistema acoplado no dito celular; este modelo proposto consiste na utilização do aparelho celular como instrumento de identificação conjunta na Internet por uma senha também enviada via o aparelho celular. O documento de patente WO0195310 descreve um dispositivo de controle e de armazenamento de dados e método de utilização e

certificação dos dados, que consiste num modelo destinado a modelos de negócios em lojas virtuais, utilizando o telefone celular como recebedor de um código de autenticação do pedido. O documento de patente JP2005192110 descreve um método de distribuição de autenticações e chaves dinâmicas em dispositivo móvel. O documento de patente CN101414909 descreve um sistema um método e um terminal móvel de comunicação para identificação e autenticação de usuários em rede. O documento de patente KR20090033594 descreve um método e um aparelho específico para apresentação de senha exclusiva de números, mas que valida senhas localmente por interpretação do cliente final. O documento de patente US2004/0268142 descreve um método de implementação de acesso seguro, que se baseia em Certificação Digital, com geração de chaves públicas e privadas no aparelho cliente para sincronismo deste para autenticação do usuário. O documento de patente CN1949709 descreve um método de identificação e autorização para acesso de uma rede e método de atualização da chave de autorização. O documento de patente CN101330420 descreve um dispositivo e método de autenticação para terminais novéis, cujo método se baseia numa certificação digital para verificação da autenticidade de uma mensagem. O documento de patente CN101163011 descreve um método seguro de autenticação para sistema de "internet bank", destinado para banco online e se baseia via certificação digital em aparelhos celulares. O documento de patente JP2003258794 descreve um sistema de segurança para celular cujo objetivo é evitar o roubo ou utilização ilegal de um celular. O documento de patente CN101350720 descreve um sistema e método de autenticação dinâmica, pela geração de senhas dinâmicas, sistema parecido ao sistema e método a ser descrito no presente relatório, porém atua com a

identificação do usuário, necessitando possuir todo o cadastro deste para seu funcionamento.

O objetivo, do objeto do presente pedido de patente, é proporcionar segurança em transações e comandos executados pela identificação inequívoca do usuário, ou permissão de funcionamento exclusivo em sua presença, garantindo a irrefutabilidade das ações realizadas em seu nome ou sob suas ordens, se posicionando como um modelo intermediário entre o praticado hoje, de username e senha passíveis de extravio ou captura, e a certificação digital, a partir da utilização do aparelho celular pessoal ou aparelho similar; instrumento de larga aceitabilidade e acesso na atualidade.

Dito sistema apresentado no presente relatório difere-se dos disponíveis no estado da técnica devido seu método de funcionamento e utilização.

O "Sistema Embarcado em Hardware para Certificação de Identificação" consiste num sistema de certificação de identificação móvel, aqui denominado de "Sistema CIM", compreendido por um software de identificação, doravante denominado de programa único, embarcado em aparelho celular ou outro dispositivo de comunicação remota de interação com o usuário, juntamente com um software de autenticação embarcado em outro dispositivo ou local que necessite de segurança, como por exemplo, o sistema de um banco, um cofre, um veículo, etc. O sistema de identificação está caracterizado pelo fato de identificar e autenticar um usuário de um serviço ou equipamento através da comunicação entre o programa único, embarcado no aparelho celular ou outro dispositivo de comunicação remota de interação com o usuário, com o software de autenticação embarcado no dispositivo ou local que necessite de segurança. Dita comunicação está caracterizada por ser através de um meio alternativo em

relação à comunicação que está sendo utilizada para interação do usuário com o dito dispositivo em questão, ou seja, a identificação será confirmada por meio da comunicação do programa único com o software de autenticação, parte do dito sistema, por um meio de comunicação alternativa àquela utilizada pelo dispositivo ou sistema que necessita de segurança.

O sistema funciona através da disponibilização de um software de autenticação de usuários para todas as empresas/entidades/dispositivos que necessitem de segurança em suas operações on-line, ou acesso a localidades, conteúdos e equipamentos, juntamente com o programa único instalado num celular ou outro dispositivo similar para interação com o usuário; passível de ser afiliado a várias redes de serviços, distribuído via liberação identificada do usuário, baseando-se na capilaridade da rede cartorial brasileira.

Dito sistema é compreendido por um grupo de programas, onde uma parte é executada no celular do usuário, por meio do "programa único", a qual é acessível apenas por meio de apresentação de senha, e outra parte é executada pelo "software de autenticação" instalado nos equipamentos ou sistemas que necessitam de segurança. Estes equipamentos podem ser os mais variados como trancas, fechaduras, veículos, sistemas bancários, etc.

O "software de autenticação" pode funcionar de diversas formas, como por exemplo, via acesso em serviço 'Single SignOn' – fornecido pelo provedor do "Sistema CIM" – ou em servidor 'Appliance' instalado no próprio parque do provedor do serviço ao qual o usuário deseja acesso, bem como junto a micro servidores disponibilizados em equipamentos ou limitadores de acesso a localidades.

O "Sistema CIM" pode possuir uma segunda senha de acesso, para os

casos de COAÇÃO, que ativa normalmente o sistema de autenticação, porém envia uma mensagem ao prestador do serviço, ou equipamento ou regulador da localidade que se deseja acessar, informando que o usuário está acessando sob pressão, permitindo assim o conhecimento da ocorrência pelos responsáveis do sistema, possibilitando que estes tomem atitudes para proteção das informações, patrimônios, segurança e integridade física do cliente portador do "Sistema CIM".

O método de funcionamento e interação do sistema confere ao dito sistema vantagens técnicas e funcionais e comodidade ao usuário de certificar sua identificação para acessar seus serviços conveniados, por meio do seu celular de maneira simples e segura.

A vantagem do "Sistema CIM", objeto do presente relatório, em todas as suas modalidade de autenticação do usuário em um sistema ou serviço eletrônico pelos dois meios de comunicação distintos, está no fato do "Sistema CIM" dispor uma confirmação final de qualquer tipo de transação ou ordem efetuada, como por exemplo, bancária, que seja feita através do "Sistema CIM" instalado no celular do usuário, apresentando os dados da transação solicitada pelo meio de comunicação tradicional para execução de transações; Internet, caixa de auto-atendimento ou mesmo o caixa do banco. A apresentação das informações, pelo dispositivo alternativo portador do "Sistema CIM", em um segundo canal de comunicação, evita assim a prática conhecida como 'Homem do Meio': Modalidade onde um usuário se insere no meio das comunicações tradicionais, simulando para o cliente a tela e informações da instituição financeira que está sendo acessada, e ao mesmo tempo simulando para o banco a conexão do cliente, transitando entre os dois apenas as informações pertinentes à fraude que está sendo praticada neste simulacro. Com a introdução do "Sistema CIM" como

o autenticador da ação requisitada pelo usuário, ou mesmo ordem emitida indevidamente pelo 'Homem do Meio', a transação só passa a ser aceita a partir de validação efetuada após comunicação e aprovação executada pelo "Sistema CIM" instalado no dispositivo disponibilizado ao cliente verdadeiro, proprietário da conta, inviabilizando a ação do 'Homem do meio', onde o mesmo modelo vale para a clonagem de cartões de contas bancárias.

A descrição detalhada da invenção juntamente com as figuras associadas, dados a título de exemplo e ilustração, farão compreender melhor o objeto do presente pedido de patente e o seu método de funcionamento.

A figura 1 mostra um representação em fluxograma do método de funcionamento do "Sistema CIM" num de seus modos de funcionamento, que é o modo de autenticação por requisição de contra-senha.

A figura 2 mostra um representação em fluxograma do método de funcionamento do "Sistema CIM" num outro modo de funcionamento, que é o modo de autenticação direta.

A figura 3 mostra uma representação ilustrativa do funcionamento do "Sistema CIM", num serviço de "internet banking" de um banco, no seu modo funcionamento de autenticação por requisição de contra-senha.

A figura 4 mostra uma representação ilustrativa do funcionamento do "Sistema CIM", num serviço de "Caixa Eletrônico" de um banco, no seu modo funcionamento por autenticação direta, ou autenticação por requisição de contra-senha.

O "Sistema Embarcado em Hardware para Certificação de Identificação e Método de Certificação de Identificação Móvel Utilizando o Dito Sistema", aqui denominado de "Sistema CIM", é compreendido por um "software de

autenticação"(4) que é instalado num sistema de serviço ou equipamento que se necessita de uma maior segurança para sua utilização, juntamente com um "programa único"(5) de interação com o usuário(1) que é instalado num dispositivo de comunicação, mais especificamente num celular, ou meio similar a este, que promova algum tipo de comunicação entre o mesmo e o equipamento onde se encontra instalado o "software de autenticação"(4). Conforme figuras 1 e 2, o "Sistema CIM" funciona por meio da interação do usuário(1) com um dispositivo(2), por exemplo um PC ou caixa eletrônico, ou outro dispositivo, que por algum meio(3) de comunicação ou conexão, por exemplo a internet, acessa um serviço ou equipamento que necessita uma condição de segurança mais elevada. O sistema deste serviço ou equipamento é portanto um portador do "software de autenticação"(4) do "Sistema CIM". Dito "software de autenticação"(4) pode ser disponibilizado no sistema do serviço/equipamento em forma de appliance, software servidor, embarcado, ou ainda serviço centralizado de single sign-on, todos operacionalizado no modelo OTP (One Time PassWord); e o serviço/equipamento pode ser um sistema bancário, um cofre, etc. Dito "software de autenticação"(4) se comunica com o "programa único"(5), parte do dito "Sistema CIM" que é instalado no celular ou dispositivo similar do usuário(1). A comunicação entre o "servidor de autenticação"(4) e o "programa único"(5) se dá por outro meio(6) de comunicação, como por exemplo o GPRS, porém diferente do meio(3) de comunicação entre o dispositivo(2) com o "servidor de autenticação"(4). O Usuário(1) utiliza seu aparelho celular – ou outro dispositivo – que contém o "programa único"(5), e este fará a interação com o "Servidor de autenticação"(4), verificando se há contra-senha disponível para ser enviada ao "programa único"(5), para que o usuário(1) utilize no meio tradicional de acesso,

que consiste no dispositivo(2), para validação junto ao "Servidor de autenticação"(4), ou ainda, para o usuário(1) efetuar a autenticação direta junto ao "Servidor de autenticação"(4) por meio do uso do "programa único"(5); opção de modelo de autenticação definida pelo fornecedor do serviço ao qual o usuário(1) deseja acessar. O "Sistema CIM" pode trabalhar com diversos "softwares de autenticação"(4). O "programa único"(5) instalado no celular se comunicará, via meio(6) de comunicação, com cada um dos "softwares de autenticação"(4) de cada um dos locais ou dispositivos que o usuário(1) estiver cadastrado como conveniado. Toda a comunicação se dará de forma criptografada, via conexão SSL ou outros modelos definidos.

O "Sistema CIM" apresenta dois modos de funcionamento, que consiste no "modo de autenticação" e no "modo de coação". No "modo de autenticação", o sistema poderá ser configurado em dois modos de autenticação: o "modo de autenticação por requisição de contra-senha", conforme ilustrado no diagrama da figura 1, ou no "modo de autenticação direta por certificação do usuário", conforme ilustrado no diagrama da figura 2.

No "modo de autenticação", o Prestador / Provedor do serviço ou equipamento protegido, possui um "software de autenticação"(4) instalado no local ou dispositivo que se necessita de segurança, ou, caso este dispositivo possua conexão com a Internet, também poderá ser utilizado o "Software de autenticação"(4) disponibilizado no servidor central pelo fornecedor do "Sistema CIM" no modelo 'Single sing-on'. Ao ter sua rede convencional acessada por um usuário(1), por intermédio de um dispositivo(2), como um PC, ou caixa eletrônico, ou um painel de acesso, e que seja afiliado ao sistema, este "software de autenticação"(4) instalado em sua infra-estrutura ou à rede Single Sign-On

disponibilizada no Provedor do serviço, passa a necessitar da certificação de identificação deste usuário(1). O "servidor de autenticação"(4) disponibilizado no sistema do serviço ou equipamento efetua uma sequência de operação que, dependendo da sua configuração pode ser a geração de uma contra-senha criptografada para aquele usuário(1), no caso do sistema estar configurado no "modo de autenticação por requisição de contra-senha", a qual fica armazenada para utilização pelo período determinado pelo Prestador do Serviço; ou aguarda a "autenticação de acesso", no caso do sistema estar configurado no "modo de autenticação direta por certificação do usuário". Tanto para localizar a contra-senha, quanto para autenticação do acesso, o usuário deverá fazer por meio do "programa único"(5) instalado em seu celular, que usará um meio(6) de comunicação alternativo, para se comunicar com o "servidor de autenticação"(4) e certificar a correta identificação do usuário(1).

A figura 1 mostra um fluxograma do funcionamento do "Sistema CIM" no seu "modo de autenticação por requisição de contra-senha". O usuário(1) conveniado num determinado serviço que usa o dito sistema de certificação, como por exemplo, o serviço de banco em "internet banking". Neste caso o banco possui um "software de autenticação"(4) instalado em seu sistema e o usuário(1) faz uso do "Sistema CIM" e possui o convênio para o uso do sistema com o banco e possui então instalado em seu celular o "programa único"(5) que se comunica com o "software de autenticação"(4) instalado no sistema do banco. No caso de uma transação via "internet banking", o usuário(1) acessa um dispositivo(2), no caso um PC, ou notebook e por um meio(3) de comunicação, neste caso a internet, e terá acesso à sua conta bancária. No momento do acesso do usuário(1) à sua conta bancária via internet, o "servidor de

autenticação"(4) instalado no sistema do banco, irá gerar(41) uma contra-senha, criptografar(42) a contra-senha e armazenar(43) a contra-senha, por um determinado período de tempo. No momento de efetivação da transação, a página da "internet banking" do usuário(1) irá solicitar a autenticação do usuário(1), que neste caso a autenticação é a apresentação da contra-senha gerada e armazenada no "servidor de autenticação"(4) no sistema do banco. O usuário(1) então deverá acessar(11) o "programa único"(5) instalado em seu celular; o "programa único"(5) é acessado mediante senha, o usuário(1) então digita(51) a senha, escolhe(52), na sua lista de convênios, o banco que estará ali listado e acessa(53) o "software de autenticação"(4) do banco, via um meio(6) de comunicação alternativo, por exemplo GPRS. Ao acessar o "software de autenticação"(4) do banco, o dito "software de autenticação"(4) certifica(44) a autenticação do usuário(1) e envia(45) a contra-senha gerada para a transação para o celular do usuário(1); o usuário(1) visualiza a contra-senha na tela do celular e digita a contra-senha no local específico da sua página do "internet banking" por meio do dispositivo(2) que está sendo usado para interação do usuário(1) com a sua conta. O "software de autenticação"(4) do sistema do banco, confere(46) a contra-senha digitada pelo usuário(1) e autoriza(47) o acesso do usuário(1).

Para impedir a ação e atuação de um usuário clandestino, ou hacker, ou sistema computacional mal intencionado, como um vírus por exemplo, aqui denominado de 'Homem do Meio', que pode a vir se instalar entre o "dispositivo"(2) e os serviços eletrônicos, como um 'Internet Banking' por exemplo, criando uma interface paralela, neste caso para o banco e para o usuário(1), o "sistema CIM" segue o mesmo modelo de autenticação descrito

acima, porém mantém o canal de comunicação aberto entre o "programa único"(5) e o meio(6) de comunicação alternativo, permitindo assim que o "software de autenticação"(4), além de autorizar o acesso do "usuário"(1) aos seus sistemas, também efetue a confirmação das transações requisitadas através do "dispositivo"(2), para que estas sejam validadas exclusivamente através do meio(6) de comunicação alternativo acessado pelo "programa único"(5), apresentando na tela do celular, por exemplo, os valores e destinos (contas de crédito) a serem executados, e aguardando a confirmação do "usuário"(1), via o "programa único"(5) pelo meio(6) comunicação alternativo, evitando assim a intromissão de qualquer outro usuário no meio(3) de comunicação tradicional, que poderia alterar os dados das transações ou ordens emitidas pelo "usuário"(1).

No modo de autenticação, denominado de "modo de autenticação direta por certificação do usuário", representado na figura 2, o modo de funcionamento do dito sistema é similar, porém o "software de autenticação"(4) não gera nenhuma contra-senha. O usuário(1) deve apenas acessar o programa único(5) instalado em seu celular e se autenticar. Neste caso, usando o mesmo exemplo de uma transação via "internet banking", o usuário(1) acessa sua conta via "internet banking" para realizar a sua transação de interesse; no instante em que o usuário(1) acessa a sua conta por um dispositivo(2), por exemplo um PC, por um meio(3) de comunicação, neste caso a internet, o "software de autenticação"(4) instalado no sistema do banco, irá gerar(41') uma solicitação de autenticação e aguardar(42') a certificação desta autenticação. No momento de efetivação da transação, a página da "internet banking" do usuário(1) irá solicitar a certificação de autenticação do usuário(1), que neste caso é apenas o acesso

do usuário(1) no "software de autenticação"(4) do banco, por meio do programa único(5) instalado em seu celular ou dispositivo similar. Para isso o usuário(1) acessa(11) o "programa único"(5) instalado em seu celular, então digita(51) a senha, escolhe(52), na sua lista de convênios, o banco que estará ali listado e acessa(53) ao "software de autenticação"(4) do banco via um meio(6) de comunicação alternativo, por exemplo GPRS. O "servidor de autenticação"(4) do banco então confere(43') o certificado de autenticação do usuário(1) com aquele gerado no dito "software de autenticação"(4) e autoriza(44') a transação do usuário(1).

As figuras 3 e 4 mostram uma representação ilustrativa da interação do usuário(1) com o dispositivo(2), que no caso pode ser um PC, um notebook, no caso da figura 3, ou um caixa ATM, como representado na ilustração da figura 4, ou outro dispositivo, como um painel de algum equipamento, como um cofre, uma porta, ou acesso a um controle remoto, etc. O interação do usuário(1) com este dispositivo(2) que desencadeará a comunicação, por algum meio(3), com o equipamento ou serviço que faz uso do "Sistema CIM" e que possui o "software de autenticação"(4) embarcado em seu sistema ou no próprio equipamento. Mostra também a interação do usuário(1) com o "programa único"(5) que é instalado num dispositivo de interação com o usuário(1), mais especificamente um celular, ou dispositivo similar, que acessará o "software de autenticação"(4) por um meio(6) de comunicação alternativo diferente do meio(3) convencional de acesso ao serviço ou equipamento desejado. Desta forma o usuário(1) acessa o serviço/equipamento via um meio(3) de comunicação ou de acesso e faz com que o "servidor de autenticação"(4), que é parte do "Sistema CIM" crie uma sequência de operações para certificação do usuário(1); deste modo o usuário

para se autenticar com o dito "servidor de autenticação"(4) deve acessar o "programa único"(5) instalado em seu celular, por exemplo, e que é parte do "Sistema CIM" que irá se comunicar via um meio(6) de comunicação alternativo diferente do meio(3) – rede GPRS de operadora, bluetooth, wifi ou outro – de comunicação e irá realizar a autenticação do dito usuário(1), seja para receber uma contra-senha para digitar no dispositivo(2), seja apenas para se autenticar diretamente.

No "modo de coação", que compreende o segundo modo de funcionamento do sistema, consiste no mesmo método de funcionamento do "Sistema CIM", porém o usuário(1) configura uma senha de coação para o dito sistema. Esta senha é configurada no "programa único"(5) que é instalada no dispositivo de interação com o usuário, no caso um celular ou dispositivo similar e deve ser utilizada em momentos de coação do usuário(1), como por exemplo, um assalto. O dito sistema de autenticação, ao ser acessado pelo canal correto, pela rede alternativa de comunicação, GPRS, ou outra, ou conjunto de redes, e tendo recebido a correta identificação do usuário, porém apresentado o alerta de coação, realiza as mesmas sequências de operações em resposta à requisição efetuada, porem envia também ao Prestador do Serviço a mensagem de que seu cliente se encontra sob coação. No caso do "Sistema CIM" estar configurado no "modo de autenticação direta" o "servidor de autenticação"(4) instalado no Prestador do Serviço envia a mensagem de autenticação da identidade do usuário(1) usando a mesma metodologia já descrita, porém enviando também ao Prestador do Serviço a mensagem de que seu cliente se encontra sob coação. No caso do "Sistema CIM" estar configurado no "modo de autenticação por requisição de contra-senha" o "servidor de autenticação"(4) instalado no

Prestador do Serviço envia a contra-senha, conforme metodologia já descrita, porém envia também ao Prestador do Serviço a mensagem de que seu cliente se encontra sob coação. Fica a cargo do Prestador do Serviço ou da configuração do equipamento que está embarcando o "Sistema CIM", a definição das medidas a serem tomadas para preservação da integridade física, patrimonial e sigilo das informações do usuário(1) final, tais como acionar as autoridades, ou mascarar as informações, acionar algum outro tipo de segurança, entre outros.

REIVINDICAÇÕES

1. "SISTEMA EMBARCADO EM HARDWARE PARA CERTIFICAÇÃO DE IDENTIFICAÇÃO", dito sistema, aqui denominado de "Sistema CIM" consiste numa forma alternativa para autenticação junto a serviços fornecidos por meios eletrônicos e junto a equipamentos específicos, caracterizado por compreender um software de identificação, aqui denominado de "programa único"(5), embarcado num aparelho celular ou outro dispositivo de comunicação remota de interação com o usuário(1), juntamente com um "software de autenticação"(4) embarcado em outro dispositivo, sistema ou local que necessite de segurança; e o "Sistema CIM" identificar e autenticar um usuário(1) ou uma transação, de um serviço, ou um equipamento, por meio da comunicação entre o "programa único"(5), com o "software de autenticação"(4) por um meio(6) de comunicação alternativo ao meio(3) de comunicação tradicionalmente utilizado pelo dispositivo ou sistema que necessita de segurança.

2. "SISTEMA EMBARCADO EM HARDWARE PARA CERTIFICAÇÃO DE IDENTIFICAÇÃO", de acordo com reivindicação 1, caracterizado pelo fato do "software de autenticação"(4), parte do dito "Sistema CIM" ser disponibilizado no sistema do serviço/equipamento em forma de "appliance";

3. "SISTEMA EMBARCADO EM HARDWARE PARA CERTIFICAÇÃO DE IDENTIFICAÇÃO", de acordo com reivindicação 1, caracterizado pelo fato "software de autenticação"(4), parte do dito "Sistema CIM" ser disponibilizado no sistema do serviço/equipamento em forma de software servidor, operacionalizado no modelo OTP (One Time PassWord);

4. "SISTEMA EMBARCADO EM HARDWARE PARA CERTIFICAÇÃO DE IDENTIFICAÇÃO", de acordo com reivindicação 1, caracterizado pelo fato do

"software de autenticação"(4), parte do dito "Sistema CIM" ser disponibilizado no sistema do serviço/equipamento em forma de serviço centralizado de single sign-on, operacionalizado no modelo OTP (One Time PassWord);

5. "SISTEMA EMBARCADO EM HARDWARE PARA CERTIFICAÇÃO DE IDENTIFICAÇÃO", de acordo com reivindicação 1, caracterizado pelo fato do dito "Sistema CIM" apresentar o modo de funcionamento compreendido pelo "modo de autenticação";

6. "SISTEMA EMBARCADO EM HARDWARE PARA CERTIFICAÇÃO DE IDENTIFICAÇÃO", de acordo com reivindicação 5, caracterizado pelo fato do "modo de autenticação" poder ser configurado no "modo de autenticação por requisição de contra-senha";

7. "SISTEMA EMBARCADO EM HARDWARE PARA CERTIFICAÇÃO DE IDENTIFICAÇÃO", de acordo com reivindicação 5, caracterizado pelo fato do "modo de autenticação" poder ser configurado no "modo de autenticação direta por certificação do usuário";

8. "SISTEMA EMBARCADO EM HARDWARE PARA CERTIFICAÇÃO DE IDENTIFICAÇÃO", de acordo com reivindicação 1, caracterizado pelo fato do dito "Sistema CIM" apresentar o modo de funcionamento compreendido pelo "modo de coação".

9. "MÉTODO DE CERTIFICAÇÃO DE IDENTIFICAÇÃO MÓVEL UTILIZANDO O DITO SISTEMA" descreve o método de funcionamento do "Sistema CIM" funcionando no "modo de autenticação por requisição de contra-senha" conforme reivindicações 1, 5 e 6, caracterizado pelo fato de que o usuário(1) ao acessar um dispositivo(2), por um meio(3) de comunicação que acessa um determinado equipamento/dispositivo/serviço, o "servidor de autenticação"(4), disposto no

determinado equipamento ou dispositivo a ser acessado, irá gerar(41) uma contra-senha; Criptografar(42) a contra-senha e Armazenar(43) a contra-senha, por um determinado período de tempo; e o usuário(1) acessar(11) o "programa único"(5) instalado em seu celular, mediante senha, digitar(51) a senha, escolher(52), o serviço desejado e acessar(53) o "software de autenticação"(4) do equipamento/dispositivo/ serviço; e ao acessar o "software de autenticação"(4), o dito "software de autenticação"(4) vai certificar(44) a autenticação do usuário(1) e enviar(45) a contra-senha gerada que deve ser fornecida ao dispositivo(2), e para o celular do usuário(1); e ao ser fornecida a contra-senha ao dispositivo(2), o "software de autenticação"(4), vai conferir(46) a contra-senha digitada pelo usuário(1) e autorizar(47) a solicitação do usuário(1).

10. "MÉTODO DE CERTIFICAÇÃO DE IDENTIFICAÇÃO MÓVEL UTILIZANDO O DITO SISTEMA" de acordo com reivindicação 9, caracterizado pelo fato do "Sistema CIM" manter o canal de comunicação aberto entre o "programa único"(5) pelo meio(6) de comunicação alternativo, e permitir que o "software de autenticação"(4), autorize o acesso do "usuário"(1) aos seus sistemas e efetue a confirmação das transações requisitadas através do "dispositivo"(2), de modo que estas transações sejam validadas e confirmadas exclusivamente através do meio(6) de comunicação alternativo acessado pelo "programa único"(5);

11. "MÉTODO DE CERTIFICAÇÃO DE IDENTIFICAÇÃO MÓVEL UTILIZANDO O DITO SISTEMA" descreve o método de funcionamento do "Sistema CIM" funcionando no "modo de autenticação direta por certificação do usuário", conforme reivindicações 1, 5 e 7, caracterizado pelo fato de que o usuário(1) ao acessar um dispositivo(2), por um meio(3) de comunicação que acessa um determinado equipamento/dispositivo/serviço, o "servidor de autenticação"(4)

disposto no determinado equipamento/dispositivo a ser acessado, irá gerar(41') uma solicitação de autenticação e aguardar(42') a certificação desta autenticação pelo usuário(1); e pelo usuário(1) acessar(11) o "programa único"(5) instalado em seu celular, digitar(51) a senha, escolher(52), o serviço desejado e acessar(53) o "software de autenticação"(4) do equipamento/dispositivo/serviço; e ao acessar o "software de autenticação"(4), o dito "software de autenticação"(4) conferir(43') o certificado de autenticação do usuário(1) com aquele gerado no dito "software de autenticação"(4) e então autorizar(44') a solicitação do usuário(1);

12. "MÉTODO DE CERTIFICAÇÃO DE IDENTIFICAÇÃO MÓVEL UTILIZANDO O DITO SISTEMA", de acordo com reivindicação 9 ou 11, caracterizado pelo fato da senha digitada(51) pelo usuário(1) ser uma senha configurada como senha de coação, configurada no "programa único"(5);

13. "MÉTODO DE CERTIFICAÇÃO DE IDENTIFICAÇÃO MÓVEL UTILIZANDO O DITO SISTEMA", de acordo com reivindicação 12, caracterizado pelo fato de que o programa único(5) ao ser acessado por meio da senha de coação enviar, ao Prestador do Serviço, a mensagem de que seu cliente se encontra sob coação;

14. "MÉTODO DE CERTIFICAÇÃO DE IDENTIFICAÇÃO MÓVEL UTILIZANDO O DITO SISTEMA", de acordo com reivindicação 12, caracterizado pelo fato de que o programa único(5) ao ser acessado por meio da senha de coação, enviar um aviso ao "software de autenticação"(4) para mascarar as informações solicitadas pelo usuário(1);

15. "MÉTODO DE CERTIFICAÇÃO DE IDENTIFICAÇÃO MÓVEL UTILIZANDO O DITO SISTEMA", de acordo com reivindicação 12, caracterizado pelo fato de que o programa único(5) ao ser acessado por meio da senha de coação, enviar

um aviso ao software de autenticação(4) para acionar as autoridades competentes;

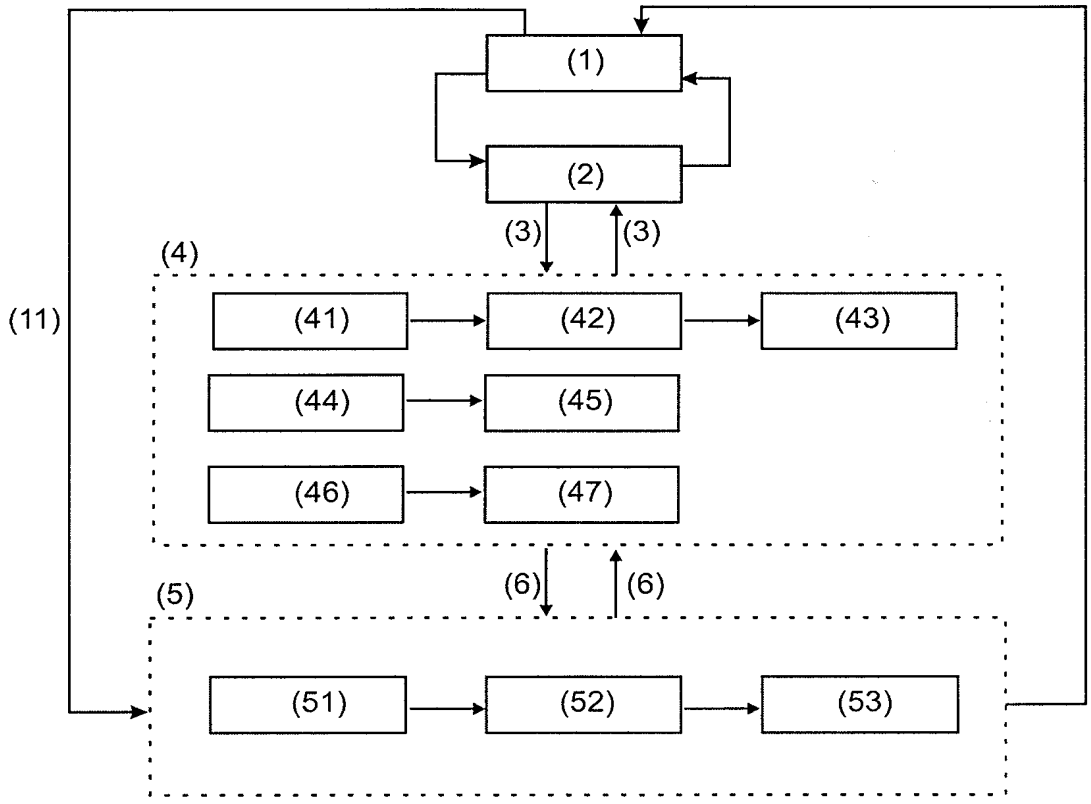

(1)
(2)
(3)
(3)
(4)
(11)
(41)
(42)
(43)
(44)
(45)
(46)
(47)
(6)
(6)
(5)
(51)
(52)
(53)

Fig. 1

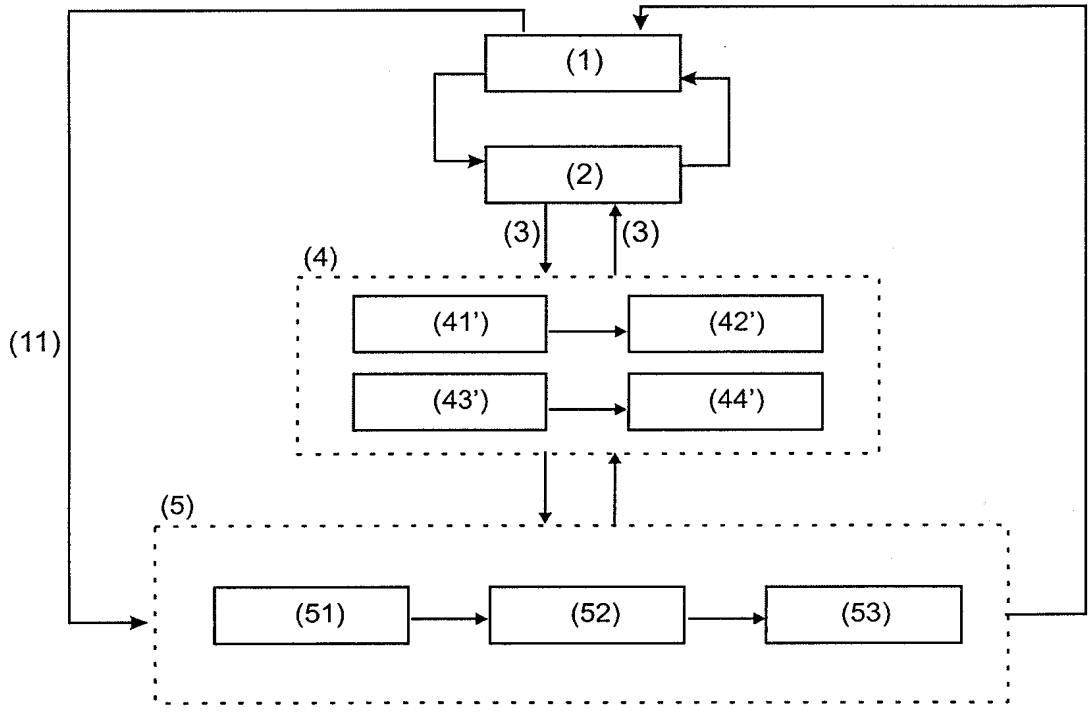

(1)
(2)
(3)
(3)
(4)
(11)
(41')
(42')
(43')
(44')
(5)
(51)
(52)
(53)

Fig.2

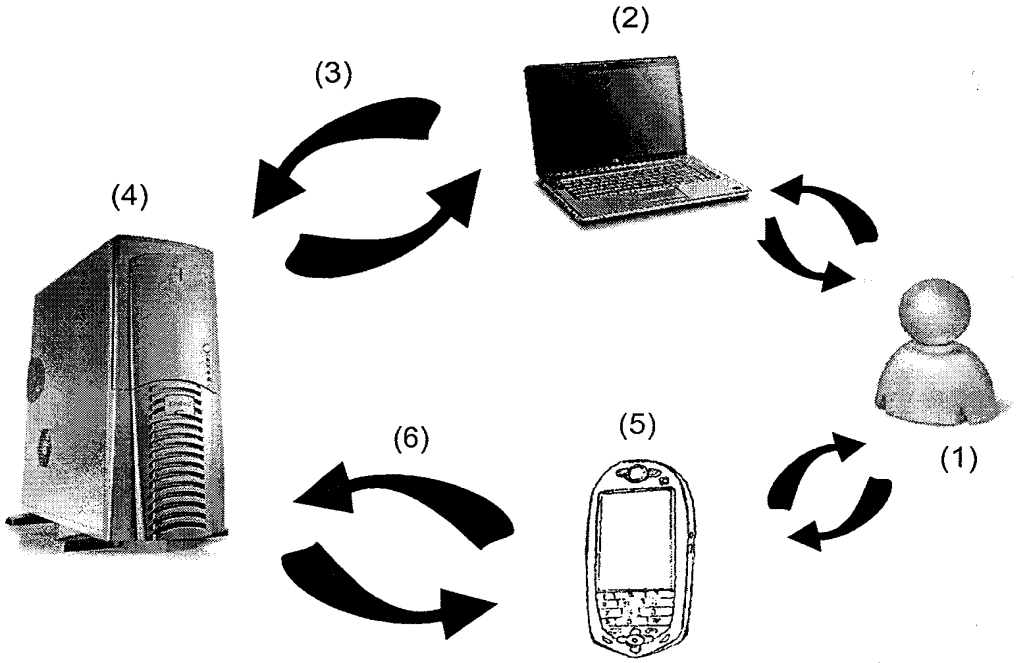


Fig. 3

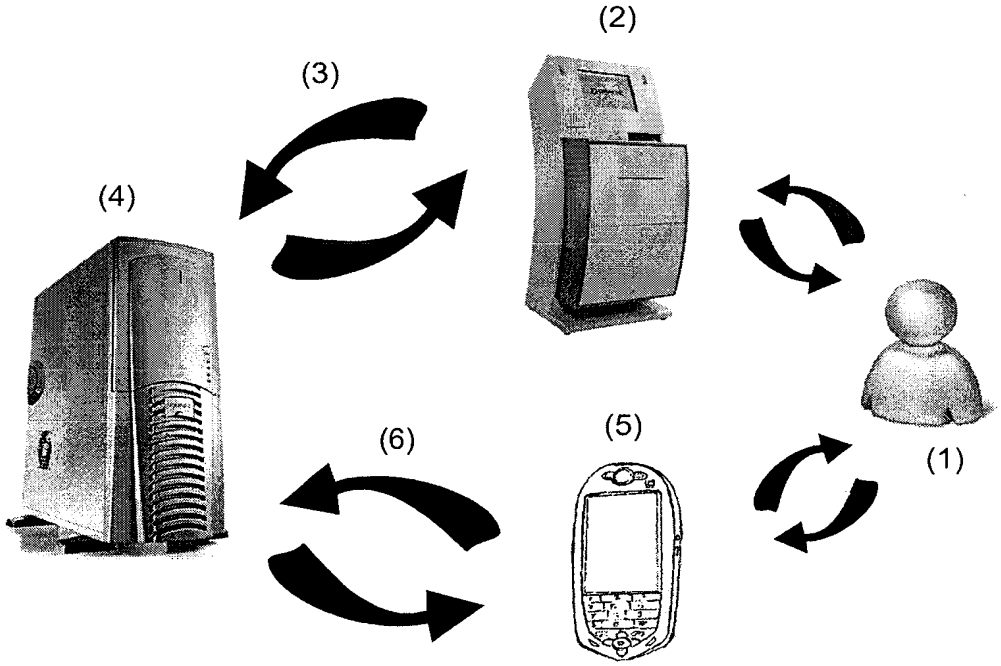


Fig. 4

RESUMO

"SISTEMA EMBARCADO EM HARDWARE PARA CERTIFICAÇÃO DE IDENTIFICAÇÃO E MÉTODO DE CERTIFICAÇÃO DE IDENTIFICAÇÃO MÓVEL UTILIZANDO O DITO SISTEMA", descreve um sistema de certificação de identificação móvel, denominado de "Sistema CIM", para autenticação de senhas junto a serviços fornecidos por meios eletrônicos e equipamentos específicos, compreendido por um software de identificação, denominado de "programa único", embarcado em aparelho celular ou outro dispositivo de comunicação remota, juntamente com um software de autenticação embarcado em outro dispositivo/sistema que necessite segurança, como por exemplo, um banco, um cofre ou um veículo, e o "sistema CIM" vai identificar e autenticar o usuário de um serviço/equipamento através da comunicação entre o "programa único" com o software de autenticação embarcado no dispositivo/sistema que necessite segurança; e a comunicação é através da confirmação da identificação por meio da comunicação do "programa único" com o software de autenticação, por um meio de comunicação alternativo àquele utilizado pelo dispositivo/sistema para requisição do acesso/emissão da ordem/autenticação ou autorização da transação.