(12) PEDIDO INTERNACIONAL PUBLICADO SOB O TRATADO DE COOPERAÇÃO EM MATÉRIA DE PATENTES (PCT)

(19) Organização Mundial da Propriedade Intelectual
Secretaria Internacional

(43) Data de Publicação Internacional
25 de Janeiro de 2018 (25.01.2018)

WIPO | PCT

(10) Número de Publicação Internacional
WO 2018/014103 A1

(51) Classificação Internacional de Patentes:
G06F 21/33 (2013.01) *G06K 19/067* (2006.01)
G06F 21/34 (2013.01) *H04L 9/32* (2006.01)
G06F 21/64 (2013.01)

(21) Número do Pedido Internacional:
PCT/BR2017/050204

(22) Data do Depósito Internacional:
21 de Julho de 2017 (21.07.2017)

(25) Língua de Depósito Internacional: Português

(26) Língua de Publicação: Português

(30) Dados Relativos à Prioridade:
102016017113-0
22 de Julho de 2016 (22.07.2016) BR

(71) Requerente: **VALID SOLUÇÕES E SERVIÇOS DE SEGURANÇA EM MEIOS DE PAGAMENTO E IDENTIFICAÇÃO S.A.** [BR/BR]; Rua Peter Lund, Nº 146/202, CAJU, Rio De Janeiro, 20930390 Rio de Janeiro (BR).

(72) Inventores: **LIMA, Marcio Campos De**; Rua Pio Correia, 80 - apto. 402b - Jardim Botanico, Rio de Janeiro, Rio de Janeiro (BR). **LOPES, Rogerio Ferreira**; Rua Fábio Luz, 135/504 Bl.2, Méier, Rio de Janeiro, Rio de Janeiro (BR).

(74) Mandatário: **REMER VILLAÇA & NOGUEIRA ASSESSORIA E CONSULTORIA DE PROP. INTELECTUAL S/S LTDA.**; Rua Padre João Manuel, 755, 3º andar, São Paulo, 01411-001 São Paulo (BR).

(81) Estados Designados *(sem indicação contrária, para todos os tipos de proteção nacional existentes)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(54) Title: SYSTEM FOR PROVISIONING, SIGNING AND VERIFYING ELECTRONIC DOCUMENTS, METHOD FOR PROVISIONING AND SIGNING ELECTRONIC DOCUMENTS AND METHOD FOR VERIFYING THE AUTHENTICITY OF ELECTRONIC DOCUMENTS

(54) Título: SISTEMA DE PROVISIONAMENTO, ASSINATURA E VERIFICAÇÃO DE DOCUMENTO ELETRÔNICO, MÉTODO DE PROVISIONAMENTO E ASSINATURA DE DOCUMENTO ELETRÔNICO E MÉTODO DE VERIFICAÇÃO DE AUTENTICIDADE DE DOCUMENTO ELETRÔNICO

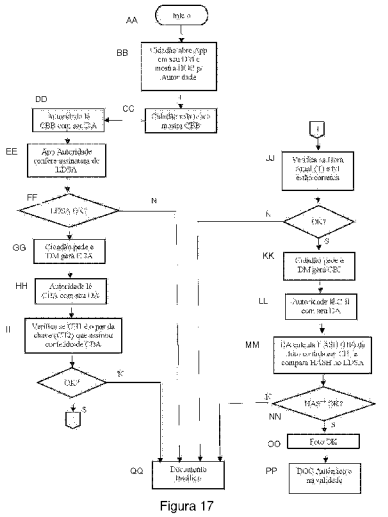

Figura 17

AA Début
BB Individu ouvre App dans son DM et montre DOC à instance
CC Individu fait défiler écran et montre CBB
DD Instance lit CBB avec son DA
EE App instance confère signature à LDSA
FF LDSA OK?
GG Individu demande DM et génère CBA
HH Instance lit CBA avec son DA
II Vérification pour déterminer si CH1 est paire de la clé (CH2) ayant signé contenu de CBA
JJ Vérification pour déterminer si heure actuelle (T) et NI sont corrects
KK Individu demande et DM génère CBI
LL Instance calcule HASH (HF) de photo contenue dans CBI et compara HASH dans LDSA
NN HASH OK?
OO Photo OK
PP DOC authentique et dans validité
QQ Non
RR Oui

(57) **Abstract:** The present invention describes systems and methods for provisioning and verifying electronic documents including the generation of machine-readable codes. Specifically, the present invention includes a system and methods for signing and verifying authenticity in electronic documents including searching for data to be used in the electronic documents, the digital signature of the data and the generation of machine-readable codes to verify authenticity. In one embodiment, authenticity is checked using the identification number (NI) of the device (DM), the image HASH of the user, using the signature of the data structure (LDS) and using the code generation time. The present invention relates to the fields of information technology, and more specifically to the area of information security.

(57) **Resumo:** A presente invenção descreve sistemas e métodos para provisionamento e verificação de documento eletrônico compreendendo a geração de códigos legíveis por máquina. Especificamente, a presente invenção compreende um sistema e métodos para assinatura e verificação de autenticidade em documento eletrônico compreendendo a busca por dados a serem utilizados no documento eletrônico, a assinatura digital dos dados e a geração de códigos legíveis por máquina para verificação de autenticidade. Em uma concretização, a autenticidade é checada por meio do número de identificação (NI) do dispositivo (DM), o HASH de imagem do usuário, pela assinatura da estrutura de dados (LDS) e pelo horário de geração de código. A presente invenção se situa nos campos de Tecnologia da Informação, mais especificamente na área de Segurança da Informação.

WO 2018/014103 A1

(Continua na página seguinte)

(84) Estados Designados *(sem indicação contrária, para todos os tipos de proteção regional existentes)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasiático (AM, AZ, BY, KG, KZ, RU, TJ, TM), Europeu (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Publicado:

— *com relatório de pesquisa internacional (Art. 21(3))*

— *antes da expiração do prazo para modificar as reivindicações e a republicar na eventualidade de receção de tais modificações (Regra 48.2(h))*

Relatório Descritivo de Patente de Invenção

SISTEMA DE PROVISIONAMENTO, ASSINATURA E VERIFICAÇÃO DE DOCUMENTO ELETRÔNICO, MÉTODO DE PROVISIONAMENTO E ASSINATURA DE DOCUMENTO ELETRÔNICO E MÉTODO DE VERIFICAÇÃO DE AUTENTICIDADE DE DOCUMENTO ELETRÔNICO

Campo da Invenção

[0001] A presente invenção descreve um sistema de provisionamento, autenticação e verificação de documento eletrônico, um método de provisionamento e autenticação de documento eletrônico e método de verificação de autenticidade de documento eletrônico. A presente invenção se situa nos campos de Tecnologia da Informação, mais especificamente na área de Segurança da Informação.

Antecedentes da Invenção

[0002] Os aparelhos de comunicação móveis modernos, tais como o telefone celular ou o chamado telefone celular inteligente (smartphone) tornaram-se quase onipresentes na sociedade. A maioria dos adultos e adolescentes rotineiramente transportam estes aparelhos, bem como um número cada vez maior de crianças. Nos dias de hoje é mais fácil o cidadão esquecer a carteira em casa do que o celular. O aparelho de comunicação móvel incorpora um poder de processamento considerável e comunicações sofisticadas, com um sistema de visualização poderoso e sensores embutidos.

[0003] Por outro lado, carregamos cada vez mais cartões em nossas carteiras com nossas diversas identificações, como identidades, carteira de estudante, carteira de motorista, carteira do plano de saúde e etc.

[0004] Dessa forma, o uso de uma carteira virtual se torna atraente, uma vez que podemos ter tudo que precisamos em nossos aparelhos de comunicação móvel, ao invés de precisarmos carregar os diversos cartões, carteiras e bolsas.

[0005] As aplicações para um sistema de identificação móvel seguro são infinitas, pois passamos a ter uma carteira virtual com nossas diversas identificações. Um sistema de identificação móvel seguro requer muito mais do que simplesmente colocar a imagem de uma identificação no aparelho de comunicação móvel, é importante que esta identificação não possa ser burlada de modo que a autoridade, para quem ela está sendo apresentada, possa confiar que ela é verdadeira.

[0006] Para que a identificação móvel emitida em um estado seja aceita em outro é necessária à imposição de um padrão, e uma vasta infraestrutura para a verificação da identificação em um aparelho de comunicação móvel. Outro desafio é desenvolver um sistema para operar em um país extenso como o Brasil, onde nem sempre teremos disponibilidade de um sinal de comunicação para validar a identificação móvel.

[0007] Portanto, é importante que o sistema funcione de forma segura independente do sinal de comunicação, isto é, funcione "off-line". No estado da técnica atual, não é detectada nenhuma solução consolidada e em pleno uso que permita, de forma segura, a utilização do documento de identificação do cidadão em seu aparelho de comunicação móvel. Existem alguns sistemas pilotos de identificação móvel sendo estudados e testados em algumas regiões dos Estados Unidos, entre eles, destacam-se projetos estudados nos estados de Delaware e Iowa.

[0008] Alguns destes sistemas estão utilizando o mesmo nível de segurança que a identificação física, isto é, reproduzem na tela do aparelho de comunicação móvel os mesmos itens de segurança do documento impresso. Como esta reprodução acaba sendo falha, acréscimos de segurança, como PIN (“Personal Identification Number”), impressão digital e reconhecimento facial, estão sendo estudados e experimentados. Contudo, os projetos estudados ainda apresentam susceptibilidade a falsificações e adversidades em suas aplicações.

[0009] Encontra-se em estudo, também, formas de transmitir informação

do aparelho de comunicação móvel do cidadão para o da autoridade. Existem projetos que estudam a utilização de Bluetooth ou NFC (Near Field Communication) para fazer a dita transferência dos dados. Contudo, alguns desses projetos requerem que o cidadão entregue seu dispositivo móvel para a autoridade, o que pode causar algumas adversidades.

[0010] Assim, nesses casos, a autoridade, portando o dispositivo do cidadão com intuito de verificação da validade, pode danificar o mesmo, sofrendo consequências devido a tal adversidade e, ainda, poderá ter acesso a informações confidenciais contidas no dispositivo, podendo até mesmo ser acusada de invasão de privacidade em alguns casos.

[0011] Na busca pelo estado da técnica em literaturas científica e patentária, foram encontrados os seguintes documentos que tratam sobre o tema:

[0012] O documento WO 2015/117212 A1 refere-se à geração e emissão de código de segurança emitido por meio da combinação de dados enviados pelo cliente, e opcionalmente com a geolocalização do órgão emissor e no qual o conjunto de dados é assinado digitalmente no Padrão de Infraestrutura de Chave Públicas (PKI) e cifrados com um par de chaves criptográficas para este propósito. Apesar de executar a geração de um código bidimensional lido por decifragem, o mesmo pode ser replicado, uma vez que não apresenta meios de comprovação de autenticidade da geração do código no dispositivo eletrônico.

[0013] O documento WO 2010/028903A1 A1 refere-se a um método de provisionamento e fiscalização de documento de identificação com dados identificáveis opticamente e representação óptica de uma assinatura digital do documento. Contudo, o documento não menciona a participação no provisionamento do documento de um dispositivo eletrônico, e dessa forma, não garante a autenticidade do dispositivo eletrônico no qual poderia ser exibido o documento.

[0014] O documento "US 2016/0162898 A1" revela um código bidimensional gerado a partir de dados autenticados que podem ser exibidos

em um dispositivo de autenticação. O dito código gerado em um primeiro dispositivo é lido e decodificado por uma aplicação de autenticação de um dispositivo de autenticação. Então, é gerado um segundo código bidimensional, a partir das informações do primeiro código no dispositivo de autenticação. Contudo, o sistema requer que o segundo código seja gerado por um dispositivo de autenticação. Ainda, o método é vulnerável a replicações, uma vez que com a obtenção do primeiro código é possível replicar o método uma vez que o segundo código é gerado no dispositivo de autenticação e não garante que a geração do código é feita no dispositivo móvel de um usuário.

[0015] O documento "US 2014/0013106 A1" revela métodos e sistemas para autenticação de documentos de identidade eletrônica que promovem o envio de documentos eletrônicos codificados e decodificados de uma autoridade de certificação para um dispositivo móvel. Contudo, a solução referente ao documento é vulnerável a replicações, uma vez que não promove meios de comprovação autenticidade do dispositivo móvel no qual o documento será exibido.

[0016] Assim, do que se depreende da literatura pesquisada, não foram encontrados conteúdos antecipando ou sugerindo os ensinamentos da presente invenção, de forma que a solução aqui proposta possui novidade e atividade inventiva frente ao estado da técnica.

[0017] Dessa forma, as soluções propostas para identificação de indivíduos apresentam adversidades relacionadas à vulnerabilidade a réplicas e fraudes nos documentos de identificação e a sistemas falhos de verificação da autenticidade de documentos. Ainda, as soluções existentes não garantem de forma mútua, a autenticidade do documento referente ao órgão emissor e ao dispositivo eletrônico no qual o documento eletrônico é exibido.

Sumário da Invenção

[0018] Dessa forma, a presente invenção tem por objetivo resolver os problemas constantes no estado da técnica a partir da provisão e verificação de

documentos eletrônicos compreendendo a assinatura digital de dados, garantindo a autenticidade da emissão do documento eletrônico executando a formação de estrutura de dados no servidor do órgão emissor, a autenticidade do dispositivo móvel solicitante e a autenticidade da relação entre o órgão emissor e o dispositivo móvel por meio da geração de códigos legíveis por máquina (Machine Readable Codes).

[0019] Em um primeiro objeto, a presente invenção apresenta um sistema de provisionamento, assinatura e verificação de documento eletrônico compreendendo ao menos:

a. um primeiro dispositivo (DM);
b. um banco de dados (BD);
c. um servidor (S);
d. um processador de criptografia (P);

em que;

- o servidor (S) está associado ao primeiro dispositivo (DM) e ao banco de dados (BD) por meio de canais seguros de comunicação;
- o processador de criptografia (P) é comunicante ao servidor (S) e compreende gerador de chaves criptográficas de autenticação; e
- o dispositivo (DM) compreende armazenamento oculto de chave criptográfica, algoritmo gerador de senhas descartáveis e de códigos legíveis por máquina.

[0020] Em um segundo objeto, a presente invenção apresenta um método de provisionamento e assinatura de documento eletrônico implementado no sistema de acordo com o primeiro objeto, compreendendo as etapas de:

a. solicitação de documento eletrônico por primeiro dispositivo (DM) a um servidor (S);
b. busca por dados (D) em banco de dados (BD) por servidor (S);
c. envio de dados (D) provenientes do banco de dados (BD) para o servidor (S);

d. formação de estrutura (LDS) no servidor (S) compreendendo os dados (D);
e. assinatura digital da estrutura (LDS) no processador de criptografia (P), gerando uma estrutura assinada (LDSA);
f. geração de um código base legível por máquina (CBB);

em que,

- o código base legível por máquina (CBB) compreende a estrutura assinada (LDSA); e
- ao menos um entre o servidor (S) ou o primeiro dispositivo (DM) é configurado para geração de código base legível por máquina (CBB).

[0021] Em um terceiro objeto, a presente invenção apresenta um método de verificação de autenticidade de documento eletrônico compreendendo ao menos as etapas de:

a. recepção de chave de autenticação de emissor (CH3), provinda de um servidor (S), por um segundo dispositivo (DA); e
b. leitura de um código base legível por máquina (CBB) utilizando o referido segundo dispositivo (DA);

em que, o referido método de verificação de autenticidade de documento eletrônico compreende adicionalmente ao menos uma das etapas de:

- leitura de código de autenticação legível por máquina (CBA) pelo segundo dispositivo (DA); e
- leitura de código de imagem legível por máquina (CBI) por segundo dispositivo (DA).

[0022] Ainda, o conceito inventivo comum a todos os contextos de proteção reivindicados tem como base o provisionamento de um documento eletrônico compreendendo a geração de códigos para verificação de autenticidade do documento em relação ao usuário e ao emissor do documento.

[0023] Estes e outros objetos da invenção serão imediatamente valorizados pelos versados na arte e pelas empresas com interesses no

segmento, e serão descritos em detalhes suficientes para sua reprodução na descrição a seguir.

Breve Descrição das Figuras

[0024] Com intuito de melhor definir o conteúdo da presente invenção, são apresentadas as seguintes figuras:

[0025] A figura 1 representa a infraestrutura de uma unidade do órgão emissor do documento eletrônico, composta por rede de comunicação segura, servidor (S), banco de dados (BD) e um processador criptográfico (P).

[0026] A figura 2 representa o dispositivo móvel (DM) comunicante ao servidor (S) da infraestrutura do órgão emissor através da rede segura.

[0027] A figura 3 mostra um esquema da etapa de solicitação de documento eletrônico por um usuário no dispositivo (DM) compreendendo o envio de número de matrícula (NM) e de número de documento (ND).

[0028] A figura 4 representa o fluxo dos dados enviados pelo dispositivo móvel (DM) ao servidor (S) do órgão emissor na etapa de solicitação: número de matrícula (NM), número de identificação (NI) e número de documento (ND).

[0029] A figura 5 representa o fluxo de dados entre o servidor (S) do órgão emissor, o banco de dados (BD) e o processador criptográfico (P). Nesta concretização são buscados no banco de dados (BD) a imagem e os dados (D) do documento eletrônico. Ainda, um par de chaves de criptografia (CH1 e CH2) é enviado ao servidor (S).

[0030] A figura 6 representa o fluxo de dados entre o servidor (S) do órgão emissor e o processador criptográfico (P), em que a estrutura de dados (LDS) é enviada ao processador de criptografia (P) para assinatura, formando a estrutura assinada (LDSA).

[0031] A figura 7a representa uma concretização em que o conteúdo código base legível por máquina (CBB) é gerado pelo servidor (S) do órgão emissor ou pelo dispositivo (DM). Onde, nesta concretização, dito código base (CBB) compreende a estrutura (LDS) do tipo 1, composta por dados (D),

número de identificação (NI), chave pública (CH1) e HASH (HF).

[0032] A figura 7b representa uma concretização o conteúdo código base legível por máquina (CBB) é gerado pelo servidor (S) do órgão emissor ou pelo dispositivo (DM). Onde, nesta concretização, dito código base (CBB) compreende a estrutura (LDS) do tipo 2, composta por dados (D), número de identificação (NI), chave pública (CH1) e imagem.

[0033] A figura 8 representa, em uma concretização, o envio pelo servidor (S) do órgão emissor do código base (CBB), dos dados (D), da imagem e da chave criptográfica privada (CH2) para o dispositivo móvel (DM).

[0034] A figura 9 representa a remontagem pelo dispositivo móvel do cidadão (DM) da imagem do documento de identificação idêntica ao documento impresso.

[0035] A figura 10 representa o primeiro código base legível por máquina (CBB), gerado pelo servidor (S) do órgão emissor do documento de identificação ou pelo dispositivo (DM), sendo apresentado na tela do dispositivo (DM).

[0036] A figura 11 revela um fluxograma de uma concretização da presente invenção compreendendo a solicitação de documento eletrônico por um primeiro elemento, busca por dados (D) em banco de dados (BD), envio de dados (D), da foto, de par de chaves de criptografia, provindo de um processador dedicado de criptografia (P), e do número de identificação (NI) do dispositivo (DM) para um servidor (S), formação de uma estrutura (LDS) no servidor (S), autenticação digital da estrutura LDS (LDSA) em um processador dedicado de criptografia (P) e geração de um código base legível por máquina (CBB).

[0037] A figura 12 revela fluxograma de uma concretização compreendendo a solicitação e provisionamento de documento eletrônico por um usuário de um dispositivo (DM), em que, o processador de criptografia (P) está compreendido no dispositivo (DM) e envia a chave pública de criptografia (CH1) para formação da estrutura (LDS) no servidor (S) e assinatura pelo

órgão emissor (OE), o dispositivo (DM) remonta o documento (DM) e gera o código base legível por máquina (CBB).

[0038] A figura 13 representa o código de autenticação legível por máquina (CBA), que é gerado pelo dispositivo móvel do cidadão (DM), sendo apresentado em sua tela.

[0039] A figura 14 representa o código de imagem legível por máquina (CBI), que é gerado pelo dispositivo móvel do cidadão (DM), sendo apresentado em sua tela.

[0040] A figura 15 representa o conteúdo do código de autenticação legível por máquina (CBA), gerado pelo dispositivo móvel do cidadão (DM), que compreende a hora de sua geração (T) e o número de identificação único (NI) do dispositivo móvel do cidadão (DM).

[0041] A figura 16 representa o conteúdo do código de imagem legível por máquina (CBI), gerado pelo dispositivo móvel do cidadão (DM), que compreende a foto do cidadão.

[0042] A figura 17 revela um fluxograma de uma concretização da verificação de autenticidade do documento de identificação.

Descrição Detalhada da Invenção

[0043] As descrições que se seguem são apresentadas a título de exemplo e não limitativas ao escopo da invenção e farão compreender de forma mais clara o objeto do presente pedido de patente.

[0044] Em um primeiro objeto, a presente invenção apresenta um sistema de provisionamento, autenticação e verificação de documento eletrônico compreendendo ao menos: um primeiro dispositivo (DM), um banco de dados (BD), um servidor (S) e um processador de criptografia (P).

[0045] O servidor (S) está associado ao dispositivo (DM) e ao banco de dados (BD) por meio de canais seguros de comunicação. Em uma concretização, o servidor (S) compreende gerador de códigos legíveis por máquina. Por códigos legíveis por máquina (Machine Readable Code) entende-

se códigos gerados pela codificação de dados cuja leitura é factível por um dispositivo compreendo meios de leitura e/ou escaneamento de códigos, tais como códigos QR (Quick Response), código de barras, motion QR-Codes, ou qualquer outro código legível por máquina.

[0046] Em uma concretização, o servidor (S) é um sistema de computação que compreende processamento de dados. Em uma concretização, o servidor (S) compreende gerador de Machine Readable Codes.

[0047] Em uma concretização, o dispositivo (DM) é um dispositivo eletrônico capaz de conectar-se a redes de comunicação wireless ou com fio, com acesso à internet ou não, por exemplo, um smartphone, Tablet, notebook ou computador. O primeiro dispositivo (DM) compreende meios de geração de códigos legíveis para verificação de autenticidade do documento eletrônico.

[0048] Em uma concretização, o dispositivo (DM) compreende interface de exibição do documento eletrônico provisionado. O dispositivo (DM) compreende armazenamento oculto de chave criptográfica, ou seja, as chaves criptográficas armazenadas no dito dispositivo não ficam disponíveis e/ou acessíveis a um usuário, de modo a evitar que uma pessoa mal intencionada possa modificar alguma chave ou colher informações indevidamente na tentativa de desvio ou roubo de dados. Ainda, o dispositivo (DM) compreende um algoritmo gerador de senhas descartáveis, ou seja, o dispositivo é capaz de gerar uma senha que é descartada após sua utilização. Em uma concretização, o dito algoritmo gerador de senhas descartáveis é um algoritmo gerador de OTP (One Time Password).

[0049] O processador de criptografia (P) é comunicante ao servidor (S) e compreende gerador de chaves criptográficas de autenticação. Em uma concretização, o processador criptografia (P) é um processador dedicado para esta função e capaz de gerenciar e proteger chaves digitais para autenticação e execução do processamento de criptografia, como por exemplo, um HSM (Hardware Security Module).

[0050] Em uma concretização, o processador de criptografia (P) está compreendido no primeiro dispositivo (DM) e é comunicante ao servidor (S) por meio de canais de comunicação seguros. Nesta concretização, o processador de criptografia (P) pode estar implementado no processador principal do dispositivo (DM) ou ser um processador dedicado à geração de códigos criptográficos, sendo integrado na arquitetura do dispositivo (DM) e capaz de se comunicar com o processador principal do dispositivo (DM) por meio de, por exemplo, um barramento de dados convencional.

[0051] O processador de criptografia (P) compreende gerador de chaves criptográficas de autenticação. O dito gerador de chaves criptográficas, em uma concretização, é um algoritmo de geração de chaves por Curvas Elípticas, de criptografia quântica, ou qualquer outro algoritmo gerador de chaves assimétricas.

[0052] Em uma concretização, o banco de dados (BD) é um sistema que compreende um conjunto de arquivos que se referem a registros relacionados a documentos de identificação de cidadãos. Por exemplo: dados biográficos e fotos referentes a carteiras de identidade, carteiras de trabalho, carteiras nacionais de habilitação, cadastros de pessoas físicas, passaportes, títulos eleitorais e/ou registros de identidade civil.

[0053] Os ditos canais seguros de comunicação compreendem infraestrutura que promove a troca de dados entre o servidor (S), o dispositivo (DM) e o banco de dados (BD), tal como redes seguras de comunicação ethernet ou wireless, e.g., Wi-Fi.

[0054] Em uma concretização, o sistema opera no ambiente seguro de um órgão emissor de documentos, onde um cidadão solicita o provisionamento e personalização digital de seu documento de identificação e na qual os funcionários inserem seus números de registros (Figura 3).

[0055] Em uma concretização, o sistema opera em um ambiente seguro, tal como em um órgão emissor de documentos compreendendo redes de comunicações protegidas (Figuras 1 e 2).

[0056] Em uma concretização, o sistema compreende um segundo dispositivo (DA) compreendendo meios de leitura de código legível por máquina e chave de criptografia do órgão emissor (CH3). Dessa forma, o segundo dispositivo (DA) é capaz de verificar a autenticidade de um código gerado pelo primeiro dispositivo (DM).

[0057] Em uma concretização, o meio de leitura de códigos legíveis por máquina é um leitor CCD, um scanner de imagem bidimensional, um leitor do tipo caneta ou qualquer dispositivo compreendendo meios de processamento de imagem.

[0058] Em uma concretização, a chave de criptografia do órgão emissor (CH3) corresponde com uma assinatura digital para verificação da autenticidade da assinatura realizada em um órgão emissor ou qualquer outro local compreendendo meios de assinatura digital de uma estrutura de dados.

[0059] Ainda, o sistema compreende o cálculo de HASH (HF) de imagem para aumentar a segurança na autenticidade do documento eletrônico. Dessa forma um algoritmo calculador de HASH (HF) é implementado no servidor (S) e/ou no primeiro dispositivo (DM) e/ou no segundo dispositivo (DA).

[0060] Em uma concretização, o documento eletrônico é um documento eletrônico de identificação (EID), tal como uma carteira de habilitação, registro geral (RG), cadastro de pessoa física (CPF), passaporte, carteira de identificação de funcionário. Ainda, o dito documento pode ser um certificado de registro de veículo (CRV), ingresso de evento ou qualquer outro documento eletrônico.

[0061] Em um segundo objeto, a presente invenção apresenta um método de provisionamento e assinatura de documento eletrônico implementado no sistema do primeiro objeto e compreendendo as etapas de: solicitação de documento eletrônico por primeiro dispositivo (DM) a um servidor (S); busca por dados (D) em banco de dados (BD) por servidor (S); envio de dados (D) provenientes do banco de dados (BD) para o servidor (S); formação de estrutura (LDS) no servidor (S) com base nos dados (D) da etapa anterior;

assinatura digital da estrutura (LDS) no processador de criptografia (P); e geração de um código base legível por máquina (CBB).

[0062] Etapa de solicitação de documento eletrônico por primeiro dispositivo (DM) a um servidor (S)

[0063] A etapa de solicitação de documento eletrônico compreende o inicio do provisionamento do documento. Preferencialmente, a solicitação é executada por meio de canais de comunicação seguros.

[0064] Em uma concretização, um usuário insere dados de identificação, tal como o número de registro de funcionário e a informação referente ao documento de um cidadão que solicitou o provisionamento do documento.

[0065] Em uma concretização, os dados de identificação incluem o número de registro de funcionário (NM), o número de registro do documento solicitado (ND), e o número de identificação (NI) do dispositivo (DM) (Figura 4).

[0066] O número de identificação (NI) do dispositivo (DM) é um código único disponibilizado para cada dispositivo (DM) fabricado por uma empresa especializada na área, sendo, por exemplo, o código IMEI (International Mobile Equipment Identity) do dispositivo.

[0067] Etapa de busca por dados (D) em banco de dados (BD) por servidor (S);

[0068] Com a solicitação de documento, é executada a etapa de busca de dados (D) em banco de dados (BD). O banco de dados (BD) compreende os dados (D) referentes ao documento a ser emitido, tais como dados biográficos ou dados de registro e imagens.

[0069] Em uma concretização, o banco de dados (BD), está compreendido na infraestrutura do órgão emissor (OE). Ainda, o banco de dados (BD) pode estar compreendido em uma nuvem, onde esta é acessada com o recebimento da solicitação.

[0070] Em uma concretização, a busca por dados é efetuada de acordo com o número de registro de documento solicitado (ND). Dessa forma, o banco de dados (BD) é acessado com o dito número de registro (ND) inserido.

[0071] Etapas de envio de dados (D) e de formação de estrutura (LDS) no servidor (S) com base nos dados (D) da etapa anterior

[0072] Após a busca por dados, uma estrutura (LDS) no servidor (S) compreendendo os dados (D) é formada para assinatura.

[0073] Adicionalmente, é enviada pelo processador de criptografia (P) para o servidor (S) uma chave criptográfica ou, em uma concretização, um par de chaves criptográficas, sendo uma chave pública (CH1) e uma chave privada (CH2). Em uma concretização, o par de chaves é gerado no processador de criptografia (P) por Curvas Elípticas, Criptografia Quântica, RSA ou qualquer outro algoritmo gerador de chaves assimétricas de criptografia.

[0074] Em uma concretização, o dispositivo (DM) recebe do servidor (S) uma chave privada (CH2) mantendo-a em armazenamento oculto. Ainda, em uma concretização, o processador de criptografia (P) pode estar compreendido no dispositivo (DM) e no mesmo é realizada a assinatura digital, sendo que, nesta concretização, a chave privada (CH2) é gerada no próprio dispositivo (DM), não necessitando que esta seja enviada pelo servidor (S).

[0075] A estrutura (LDS) compreende um entre: dados de identificação, HASH (HF) de imagem, imagem do indivíduo, número de identificação (NI) e chave criptográfica pública (CH1).

[0076] Em uma concretização, como pode ser observado na Figura 5, o servidor (S) recebe então, os dados biográficos (D) e a foto provenientes do banco de dados (BD), bem como o par de chaves de criptografia de autenticação ativa (CH1 e CH2) provindas do processador dedicado de criptografia (P). No servidor (S) os dados (D), o HASH da foto, o número de identificação (NI) do dispositivo (DM) e uma chave pública (CH1), compreendida no par de chaves de criptografia, são reunidos em uma estrutura (Logical Data Structure - LDS).

[0077] Em outra concretização, o servidor (S) envia os dados biográficos (D) e a foto provenientes do banco de dados (BD) para o dispositivo (DM), e o mesmo envia chave pública (CH1) do processador de criptografia (P) para o

servidor (S).

[0078] Ainda, adicionalmente o servidor (S) calcula o HASH (HF) da imagem proveniente do banco de dados (BD) para formação de estrutura (LDS). Em uma concretização, o dispositivo (DM) calcula o HASH (HF) da imagem para formação de estrutura (LDS). Conforme descrito anteriormente, a dita imagem se refere à imagem do indivíduo, sendo esta compreendida nos dados (D), buscado no banco de dados (BD).

[0079] Assinatura digital da estrutura (LDS) no processador de criptografia (P), gerando estrutura assinada (LDSA)

[0080] A estrutura (LDS) é enviada do servidor (S) para o processador de criptografia (P) onde é efetuada a assinatura do pacote para formação do pacote assinado (LDSA). Essa assinatura digital pode ser realizada por meios convencionais, que garantem a segurança da informação que está sendo assinada, neste caso a estrutura (LDS). Assim, a estrutura assinada (LDSA) é, então, enviada ao dispositivo (DM), seja enviada diretamente pelo processador de criptografia (P) ou pelo servidor (S), de modo que, para esta segunda opção, o processador (P) retorna com a estrutura assinada (LDSA) ao servidor (S) antes deste enviar ao dispositivo (DM).

[0081] Em uma concretização, o dito processador de criptografia (P) está compreendido no dispositivo (DM) ou na infraestrutura do órgão emissor (OE) do documento.

[0082] Em uma concretização, conforme figuras 5 e 6, por meio da estrutura assinada (LDSA) é formado o código base legível por máquina (CBB).

[0083] Geração de um código base legível por máquina (CBB)

[0084] Com a estrutura assinada (LDSA) pelo processador de criptografia (P), é gerado um código base legível por máquina (CBB). O dito código (CBB) pode compreender informações referentes aos dados (D) do documento, a imagem do usuário, HASH de imagem de usuário, número de identificação (NI) do dispositivo, e chave pública (CH1), visto que estas informações podem estar compostas diretamente na estrutura assinada

(LDSA), conforme detalhado anteriormente.

[0085] Em uma concretização, o código base (CBB), o pacote assinado (LDSA), a foto e a chave criptográfica privada (CH2), do par de chaves de criptografia, são enviados ao dispositivo móvel (DM), conforme esquema revelado na Figura 8.

[0086] Em uma concretização, conforme fluxograma da Figura 11, o código base (CBB) é gerado no servidor (S) e enviado dispositivo (DM) para leitura posterior. Em outra concretização, conforme fluxograma da Figura 12, o código base (CBB) é gerado no dispositivo (DM) após recebimento de estrutura (LDS). Dessa forma, tanto a assinatura quanto a geração do código base (CBB) podem ser feitas na infraestrutura do órgão emissor (OE) ou no próprio dispositivo (DM). Ademais, ambos os casos retratados acima podem ocorrer conjuntamente.

[0087] Etapa de geração de código de autenticação legível por máquina (CBA)

[0088] Para reforçar a segurança do documento eletrônico, a presente invenção compreende a geração de um código de autenticação (CBA) no próprio dispositivo (DM), o qual, assim como o código base (CBB), também é um tipo de código legível por máquina. O código de autenticação (CBA) é gerado por meio de um algoritmo de senhas descartáveis, tal como um algoritmo gerador de OTP (One Time Password). Em uma concretização, este código de autenticação (CBA) é assinado digitalmente pela chave criptográfica privada (CH2) que, conforme descrito anteriormente, é par da chave pública (CH1). Deste modo, nesta concretização, para que este código (CBA) possa ser lido há a necessidade de se conhecer a referida chave pública (CH1).

[0089] O código compreende ao menos um entre o horário equivalente à solicitação de geração do código de autenticação (CBA) e o número de identificação do dispositivo (NI). Dessa forma, o documento garante que o código foi gerado naquele momento por aquele dispositivo (DM).

[0090] Etapa de geração de código de imagem legível por máquina (CBI)

[0091] Ainda, a presente invenção compreende a geração de um código de imagem (CBI) legível por máquina. O código de imagem (CBI), assim como o código de autenticação (CBA), mencionado anteriormente, também é gerado pelo dispositivo (DM). O referido código (CBI) compreende a imagem de identificação para que seja possível verificar a autenticidade da imagem fornecida pelo documento eletrônico. A referida imagem para a geração do dito código (CBI) é obtida a partir da estrutura (LDS). Para fins da presente invenção, a imagem de identificação contida na estrutura (LDS) é a imagem contida nos dados (D), buscados no banco de dados (BD), conforme definido anteriormente.

[0092] Dessa forma, o presente método de provisionamento de documento compreende ferramentas para geração de um código base (CBB), um código de autenticação (CBA) e código de imagem (CBI).

[0093] Em uma concretização, a solicitação de geração dos códigos de autenticação (CBA) e de imagem (CBI) ocorre após a exibição do código base legível por máquina (CBB), sendo estes exibidos sequencialmente para exibição do documento integralmente. Ainda, os códigos de autenticação (CBA) e de imagem (CBI) podem ser exibidos independentemente entre si, após a exibição do código base (CBB).

[0094] Em uma concretização, o código base (CBB), o código de autenticação (CBA), o código de imagem (CBI) são exibidos em uma interface compreendida no dispositivo (DM).

[0095] Em uma concretização, os dados biográficos (D) e a foto são exibidos em uma interface do dispositivo (DM). Dessa forma, é possibilitada a consulta “tradicional” ao documento no qual são exibidos, por exemplo, datas e números de registro (Figura 9). Em uma concretização, a imagem de identificação contida nos dados biográficos (D) e a foto são enviadas ao dispositivo (DM) e exibidas na interface do dito dispositivo (DM).

[0096] Em um terceiro objeto, a presente invenção apresenta um método de verificação de autenticidade de documento eletrônico compreendendo ao

menos as etapas de recepção de chave de autenticação de emissor (CH3), provinda de um servidor (S), por um segundo dispositivo (DA) e leitura de um código base legível por máquina (CBB) utilizando o referido segundo dispositivo (DA).

[0097] Adicionalmente, o método de verificação compreende ao menos uma entre as etapas de leitura de código de autenticação legível por máquina (CBA) pelo segundo dispositivo (DA) e leitura de código de imagem legível por máquina (CBI) por segundo dispositivo (DA). Ou seja, com isso, o presente método de verificação permite a leitura do código base (CBB) e, em sequência, a leitura dos códigos (CBA) e/ou (CBI).

[0098] O presente método pode ser implementado na verificação do documento eletrônico provisionado e autenticado de acordo com o método de provisionamento e assinatura de documento eletrônico definido anteriormente.

[0099] Etapa de leitura de código base legível por máquina (CBB)

[0100] A etapa de leitura do código base (CBB) compreende, em uma concretização, a verificação de assinatura digital do documento eletrônico por meio da chave de autenticação do emissor (CH3).

[0101] Ainda, a leitura do código base (CBB) pode compreender a verificação de veracidade de dados (D) do primeiro dispositivo (DM) com base na informação lida no código base legível por máquina (CBB).

[0102] Além disso, esta etapa de leitura pode compreender a verificação de veracidade de número de identificação (NI) do primeiro dispositivo (DM) com número de identificação lido no código base legível por máquina (CBB).

[0103] Dessa forma, qualquer uma das etapas acima pode ser efetuada para análise da validade do documento eletrônico. Ainda, todas as etapas podem ser executadas para garantir uma maior autenticidade dos parâmetros do documento.

[0104] Dessa forma, o usuário verificador, analisa a veracidade da assinatura digital da estrutura (LDS), checando por meio da chave de autenticação do emissor (CH3), além de conseguir ler todas as informações

inseridas no dito código base (CBB). Em uma concretização, o segundo dispositivo (DA) lê e armazena a chave púbica (CH1) contida no código base (CBB).

[0105] Etapa de leitura de código de autenticação legível por máquina (CBA)

[0106] A etapa de leitura do código de autenticação por máquina (CBB) compreende, em uma concretização, a verificação de veracidade de assinatura digital do código de autenticação legível por máquina (CBA), utilizando a chave criptográfica pública (CH1) obtida no código base legível por máquina (CBB).

[0107] Ainda, compreende a verificação de horário (T) de solicitação de geração de código de autenticação legível por máquina (CBA).

[0108] Além disso, pode compreender a verificação de veracidade do número de identificação (NI) obtido no código de autenticação legível por máquina (CBA) com o número de identificação (NI) obtido no código base legível por máquina (CBB).

[0109] Portanto, qualquer uma das ditas etapas podem ser executadas para verificação de validade do código (CBA), em que, a execução de todas as etapas descritas garante uma maior confiabilidade na verificação da autenticidade do documento.

[0110] Etapa de leitura de código de imagem legível por máquina (CBI)

[0111] A etapa de leitura do código de imagem (CBI) compreende o cálculo do HASH da imagem de identificação lida no código de validação de imagem (CBI) e comparação do HASH calculado com o HASH (HF) lido no código base legível por máquina (CBB).

[0112] Dessa forma, o método verifica a autenticidade dos dados referentes à imagem do indivíduo.

[0113] Em uma realização preferencial, os códigos base (CBB), de autenticação (CBA) e de imagem (CBI) são verificados sequencialmente para aumentar a confiabilidade do processo e verificar o documento integralmente.

[0114] Ainda, a verificação dos códigos de imagem (CBI) e código de

autenticação (CBA) pode ser realizada de forma independente, sendo executada a verificação de autenticidade do documento eletrônico de forma parcial.

[0115] Em uma concretização, o segundo dispositivo (DA) é um dispositivo de uma autoridade a fim de executar a verificação do documento de um cidadão, verificando a validade e autenticidade do mesmo por meio do método e sistema previamente descritos.

[0116] Portanto, durante uma atividade de verificação da autenticidade de documento a autoridade é capaz de verificar se os dados exibidos no dispositivo do cidadão condizem com as etapas e os dados utilizados no momento do provisionamento e assinatura do documento eletrônico de identificação no órgão emissor mediante a autorização de um funcionário do local. Um documento falsificado, quando implementado no proposto pela presente invenção, gera códigos incompatíveis com os dados a serem comparados e, desta forma, é identificado facilmente como não autêntico pela autoridade.

[0117] O presente objeto permite a utilização de um grande número de aparelhos de comunicação móvel. A verificação da autenticidade dos documentos a ser realizada entre um cidadão e uma autoridade pode ser realizada sem a necessidade de sincronização do dispositivo do cidadão com o da autoridade. E ainda pode ser efetuada off-line sem necessidade de acesso a algum banco de dados remoto e de sinal de comunicação. Este fato se dá visto que tanto o cidadão quanto a autoridade apresentam dispositivos dotados de chaves criptográficas já armazenadas em seus dispositivos, além de algoritmos para prevenção de eventuais fraudes.

[0118] O presente projeto propõe uma solução para a concretização da identificação digital de indivíduos solucionando problemas em relação à operação off-line, à vulnerabilidade a falsificações dos dados e também da imagem de identificação, e ainda propõe um método de verificação da autenticidade do documento sem a necessidade de contato físico da autoridade

verificadora com o dispositivo portando o documento a ser verificado.

[0119] O documento digital pode ser personalizado no órgão emissor rapidamente. Ainda, os métodos e sistemas previamente descritos promovem uma rapidez na verificação da autenticidade do mesmo, uma vez que basta executar a leitura dos códigos por um dispositivo eletrônico.

Exemplos - Concretizações

[0120] Os exemplos aqui mostrados têm o intuito somente de exemplificar uma das inúmeras maneiras de se realizar a invenção, contudo sem limitar, o escopo da mesma.

Exemplo I – Assinatura de documento eletrônico no dispositivo (DM)

[0121] Em uma concretização, o processador de criptografia (P) está compreendido em um primeiro dispositivo (DM) para o qual é enviado o documento eletrônico. Dessa forma, o dispositivo (DM) solicita o provisionamento do documento para um servidor (S) pelo meio de comunicação seguro provido pelo órgão emissor do documento. Então, o servidor (S) busca as informações referentes ao usuário que solicitou o documento na base de dados (BD) e forma uma estrutura (LDS). A estrutura (LDS) é enviada ao dispositivo (DM) para ser assinada no processador de criptografia (P), a estrutura (LDSA) assinada é utilizada, então, para a geração do código base legível por máquina (CBB).

Exemplo II – Assinatura de documento eletrônico externa ao dispositivo (DM)

[0122] Em uma concretização, o processador de criptografia (P) pertence á infraestrutura do órgão emissor (OE) do documento ao primeiro dispositivo (DM) para o qual é enviado o documento eletrônico. Dessa forma, o dispositivo (DM) solicita o provisionamento do documento para um servidor (S) pelo meio de comunicação seguro provido pelo órgão emissor do documento. Então, o servidor (S) busca as informações referentes ao usuário que solicitou o documento na base de dados (BD) e forma uma estrutura (LDS). A estrutura (LDS) é enviada ao processador de criptografia (P) para ser assinada, a

estrutura (LDSA) assinada é enviada para o dispositivo (DM), e então, é utilizada para a geração do código base legível por máquina (CBB).

Exemplo III – Leitura de código base (CBB)

[0123] Em uma concretização, uma autoridade portando um dispositivo compreendendo meios de leitura de código Machine Readable Code executa a verificação da autenticidade do documento de identificação que foi provisionado digitalmente por meio do método de provisionamento previamente descrito. O dito dispositivo do segundo elemento (DA) compreende uma chave de autenticação (CH3) que corresponde á assinatura da estrutura (LDS) executada no órgão emissor (OE).

[0124] O segundo elemento, então executa a leitura do código base (CBB) por meio do dispositivo e verifica a veracidade da assinatura digital da estrutura (LDS). Ainda, verifica a veracidade das informações obtidas com a leitura do código (CBB) com os dados exibidos no documento remontado na interface do dispositivo DM. Ademais, nesta leitura do código base (CBB), o dispositivo da autoridade, ou segundo dispositivo (DA), recebe informações como: dados (D) do documento do cidadão, HASH da imagem do usuário e/ou a própria imagem do usuário, número de identificação (NI), ou IMEI, do dispositivo (DM) do usuário e chave pública (CH1) provindo do processador de criptografia (P) na etapa de assinatura de documento eletrônico.

Exemplo IV – Leitura de código de autenticação (CBA)

[0125] Em uma concretização, uma autoridade solicita a geração do código de autenticação (CBA) para prosseguir com a execução da verificação de autenticidade da documentação executada no Exemplo III.

[0126] Após a geração do código de autenticação (CBA), a autoridade executa a leitura do mesmo a fim de verificar se a chave privada (CH2), provindo do processador de criptografia (P), utilizada pelo dispositivo (DM) para assinar o conteúdo do código de autenticação (CBA), é par da chave pública (CH1) obtida com a leitura do código base (CBB). O segundo elemento, então, compara o número de identificação (NI) obtido no código base (CBB) com o

número de identificação (NI) obtido no código de autenticação (CBA) e, ainda, verifica se o horário (T) de geração do código de autenticação (CBA) lido é compatível com o horário em que o primeiro elemento executou a solicitação de geração do código de autenticação (CBA).

Exemplo V – Leitura de código de imagem (CBI)

[0127] Em uma concretização, a autoridade verifica a autenticidade da documentação digital por meio da leitura do código de imagem (CBI), na qual a imagem de identificação do usuário é obtida. O segundo elemento calcula o HASH da imagem obtida na leitura e o compara com o HASH (HF) obtido na leitura do código base (CBB) conforme descrição no exemplo III.

Exemplo VI – Leitura dos códigos base (CBB), de autenticação (CBA) e de imagem (CBI)

[0128] Em uma concretização, a autoridade, se passando pelo segundo elemento, executa a leitura de acordo com os exemplos III, IV e V. Dessa forma, a autoridade executa a leitura do documento integralmente.

[0129] Com isso, essa verificação dificulta as fraudes e réplicas de documentos, uma vez que o código de autenticação (CBA) a ser lido contém informações referentes ao tempo (T) em que foi gerado e ao número de identificação (NI) do dispositivo (DM), portanto é avaliado como autêntico se o número de identificação (NI) lido for o mesmo do que o enviado ao servidor (S) na etapa de solicitação de provisionamento e personalização de documento eletrônico de identificação, se o tempo lido na verificação for o mesmo que o tempo (T) de geração do código de autenticação (CBA) e ainda, se a chave de autenticação ativa privada (CH2) utilizada para autenticação do código de autenticação (CBA) é par da chave de autenticação ativa pública (CH1). Ainda, protege a alteração da imagem de identificação da documentação uma vez que por meio da leitura do código de imagem (CBI) é possível a comparação do HASH da imagem exibida na documentação digital com o HASH (HF) calculado com a imagem de identificação armazenada no banco de dados (BD) do órgão emissor pelo servidor (S).

Exemplo VII – Concretização de provisionamento e verificação de documento eletrônico

[0130] Uma concretização de uma situação de provisionamento e assinatura de um documento eletrônico de identificação (EID) de um cidadão é exemplificada no fluxograma revelado na Figura 13.

[0131] Para instalar a identificação no dispositivo de comunicação móvel do cidadão (DM), este deve baixar o aplicativo da "loja" do seu sistema operacional (Play Store no caso da Google/Android ou App Store no caso da Apple/IOS), e se dirigir a uma unidade indicada pelo órgão emissor do documento de identificação.

[0132] Neste local, seu aparelho de comunicação móvel será conectado em uma rede segura, por exemplo, uma rede Wi-Fi segura, para que possa receber o QR Code (CBB), contendo a estrutura (LDS) assinada digitalmente pelo órgão emissor (LDSA), a foto do cidadão, a chave de autenticação ativa privada (CH2) e a estrutura LDSA (Figura 8).

[0133] Quando o cidadão precisar apresentar sua identificação no seu aparelho de comunicação móvel para uma autoridade, ele abre o aplicativo que remonta o documento e o apresenta na tela como se fosse uma cópia do documento impresso (Figura 9).

[0134] O cidadão, então, rola a tela onde está a imagem do documento e aparece o QR Code (CBB) gerado no momento da instalação do documento de identificação feita no órgão emissor (Figura 10). Este QR Code (CBB) possui os dados biográficos do cidadão, o HASH da foto calculada pelo servidor (S) do órgão emissor, a identificação única do dispositivo de comunicação móvel e a chave pública de autenticação ativa de curvas elípticas do aparelho (CH1), conjunto com a assinatura digital do órgão emissor (Figura 7).

[0135] Também aparece nesta tela um botão que, quando tocado, gera um segundo QR Code de autenticação (CBA), dinâmico, que perde a validade após determinado tempo (Figura 13). O CBA tem conteúdo assinado pela chave de autenticação ativa privada do dispositivo (CH2) e contendo a hora (T)

e o IMEI (NI) do dispositivo de comunicação móvel (Figura 14). Este segundo QR Code de autenticação é gerado a cada vez que o documento é apresentado.

[0136] O dispositivo de comunicação móvel da autoridade faz a leitura dos dois QR Codes apresentados na tela do aparelho de comunicação móvel do cidadão. Pela assinatura do órgão emissor no CBB, o aplicativo da autoridade verifica a validade e a integridade dos dados contidos no conjunto.

[0137] A utilização do segundo QR Code (CBA) garante para a autoridade a autenticidade da identificação apresentada, evitando que uma cópia da imagem da identidade e do primeiro QR Code sejam apresentados e utilizados como verdadeiros (“spoofing”).

[0138] Um terceiro QRCode (CBI) pode, opcionalmente, ser gerado tocando-se novamente no botão da tela (Figura 14). O CBI contém a foto do cidadão recebida, pelo aparelho de comunicação móvel do cidadão, do servidor do órgão emissor em um ambiente seguro (Figura 16).

[0139] O aparelho de comunicação móvel da autoridade faz a leitura de CBI, calcula internamente o "HASH" da foto e o compara com o "HASH" da foto que foi gerado no servidor do órgão emissor e por ele assinado. Este passo garante que a foto que está sendo apresentada no documento na tela do aparelho móvel do cidadão realmente é a foto do cidadão possuidor daqueles dados biográficos.

[0140] Os versados na arte valorizarão os conhecimentos aqui apresentados e poderão reproduzir a invenção nas modalidades apresentadas e em outras variantes, abrangidas no escopo das reivindicações anexas.

Reivindicações

1. Sistema de provisionamento, assinatura e verificação de documento eletrônico **caracterizado** por compreender ao menos:

a. um primeiro dispositivo (DM);

b. um banco de dados (BD);

c. um servidor (S);

d. um processador de criptografia (P);

em que;

- o servidor (S) está associado ao primeiro dispositivo (DM) e ao banco de dados (BD) por meio de canais seguros de comunicação;
- o processador de criptografia (P) é comunicante ao servidor (S) e compreende gerador de chaves criptográficas de autenticação; e
- o dispositivo (DM) compreende armazenamento oculto de chave criptográfica, algoritmo gerador de senhas descartáveis e de códigos legíveis por máquina.

2. Sistema de provisionamento, assinatura e verificação de documento eletrônico, de acordo com a reivindicação 1, **caracterizado** pelo fato de compreender um segundo dispositivo (DA), compreendendo ao menos um entre:

- meios de leitura de código legível por máquina; e
- chave de criptografia do órgão emissor (CH3).

3. Sistema de provisionamento, assinatura e verificação de documento eletrônico, de acordo com qualquer uma das reivindicações 1 e 2, **caracterizado** pelo fato de um algoritmo calculador de HASH (HF) ser implementado em ao menos um entre:

a. servidor (S);

b. primeiro dispositivo (DM); e

c. segundo dispositivo (DA).

4. Método de provisionamento e assinatura de documento eletrônico

caracterizado pelo fato de ser implementado no sistema conforme definido nas reivindicações 1 a 3 e por compreender as etapas de:

a. solicitação de documento eletrônico por primeiro dispositivo (DM) a um servidor (S);
b. busca por dados (D) em banco de dados (BD) por servidor (S);
c. envio de dados (D) provenientes do banco de dados (BD) para o servidor (S);
d. formação de estrutura (LDS) no servidor (S) compreendendo os dados (D);
e. assinatura digital da estrutura (LDS) no processador de criptografia (P), gerando uma estrutura assinada (LDSA);
f. geração de um código base legível por máquina (CBB);

em que,

- o código base legível por máquina (CBB) compreende a estrutura assinada (LDSA); e

- ao menos um entre o servidor (S) ou o primeiro dispositivo (DM) é configurado para geração de código base legível por máquina (CBB).

5. Método de provisionamento e assinatura de documento eletrônico, de acordo com a reivindicação 4, **caracterizado** pelo fato de a etapa de envio de dados (D) provenientes do banco de dados (BD) para o servidor (S) compreender adicionalmente o envio, do processador de criptografia (P) para o servidor (S), de ao menos:

a. uma chave criptográfica; ou
b. um par de chaves criptográficas compreendido por uma chave criptográfica pública (CH1) e uma chave criptográfica privada (CH2).

6. Método de provisionamento e assinatura de documento eletrônico, de acordo com qualquer uma das reivindicações de 4 e 5, **caracterizado** por compreender adicionalmente uma etapa de cálculo de HASH (HF) de imagem elaborado pelo servidor (S) e/ou pelo dispositivo (DM), em que a dita imagem é

compreendida nos dados (D).

7. Método de provisionamento e assinatura de documento eletrônico, de acordo com qualquer uma das reivindicações de 4 a 6, **caracterizado** pelo fato da estrutura (LDS) compreender ao menos um entre:

a. dados de identificação;
b. HASH (HF) de imagem;
c. imagem;
d. número de identificação (NI); e
e. chave criptográfica pública (CH1).

8. Método de provisionamento e assinatura de documento eletrônico, de acordo com qualquer uma das reivindicações de 4 a 7, **caracterizado** por compreender adicionalmente o envio de dados (D) e/ou da chave de criptografia privada (CH2) e/ou da estrutura assinada (LDSA) do servidor (S) para o primeiro dispositivo (DM).

9. Método de provisionamento e assinatura de documento eletrônico, de acordo com qualquer uma das reivindicações de 4 a 8, **caracterizado** por compreender etapa de geração de código de autenticação legível por máquina (CBA) no primeiro dispositivo (DM), compreendendo a codificação de conteúdo, sendo o dito conteúdo ao menos um entre:

a. horário (T), equivalente à solicitação de geração do código de autenticação legível por máquina (CBA), e/ou
b. número de identificação (NI) do dispositivo (DM);

em que, o conteúdo é assinado digitalmente pela chave de criptografia privada (CH2) e o código é gerado por meio de algoritmo gerador de senhas descartáveis.

10. Método de provisionamento e assinatura de documento eletrônico, de acordo com qualquer uma das reivindicações de 4 a 9 **caracterizado** por compreender etapa de geração de código de imagem legível por máquina (CBI) no primeiro dispositivo (DM) compreendendo a imagem contida da estrutura (LDS).

11. Método de verificação de autenticidade de documento eletrônico **caracterizado** por compreender ao menos as etapas de:

a. recepção de chave de autenticação de emissor (CH3), provinda de um servidor (S), por um segundo dispositivo (DA); e

b. leitura de um código base legível por máquina (CBB) utilizando o referido segundo dispositivo (DA);

em que, o referido método de verificação de autenticidade de documento eletrônico compreende adicionalmente ao menos uma das etapas de:

- leitura de código de autenticação legível por máquina (CBA) pelo segundo dispositivo (DA); e
- leitura de código de imagem legível por máquina (CBI) por segundo dispositivo (DA).

12. Método de verificação de autenticidade de documento eletrônico, de acordo com a reivindicação 12, **caracterizado** por ser implementado na verificação do documento eletrônico provisionado e autenticado conforme definido nas reivindicações 4 a 10.

13. Método de verificação de autenticidade de documento eletrônico, de acordo com qualquer uma das reivindicações 11 a 12, **caracterizado** pelo fato da etapa de leitura de código base legível por máquina (CBB) por segundo dispositivo (DA) compreender ao menos uma entre as etapas de:

a. verificação de assinatura digital do documento eletrônico por meio da chave de autenticação do emissor (CH3);

b. verificação de veracidade de dados (D) do primeiro dispositivo (DM) com dados lidos em código base legível por máquina (CBB); e

c. verificação de veracidade de número de identificação (NI) do primeiro dispositivo (DM) com número de identificação lido no código base legível por máquina (CBB).

14. Método de verificação de autenticidade de documento eletrônico de acordo com qualquer uma das reivindicações de 11 a 13 **caracterizado** pelo fato da etapa de leitura de código de autenticação legível por máquina (CBA)

por segundo dispositivo (DA) compreender ao menos uma entre as etapas de:

a. verificação de compatibilidade de assinatura digital do código de autenticação legível por máquina (CBA), utilizando a chave criptográfica pública (CH1) obtida no código base legível por máquina (CBB);

b. verificação de horário (T) de solicitação de geração de código de autenticação legível por máquina(CBA); e

c. verificação de compatibilidade do número de identificação (NI) obtido no código de autenticação legível por máquina (CBA) com o número de identificação (NI) obtido no código base legível por máquina (CBB).

15. Método de verificação de autenticidade de documento eletrônico, de acordo com qualquer uma das reivindicações de 11 a 14, **caracterizado** pelo fato da etapa de leitura de código de imagem legível por máquina (CBI) por segundo dispositivo (DA) compreender as etapas de:

a. cálculo do HASH da imagem de identificação lida no código de imagem legível por máquina (CBI); e

b. comparação do HASH calculado com o HASH (HF) lido no código base legível por máquina (CBB).

FIGURAS

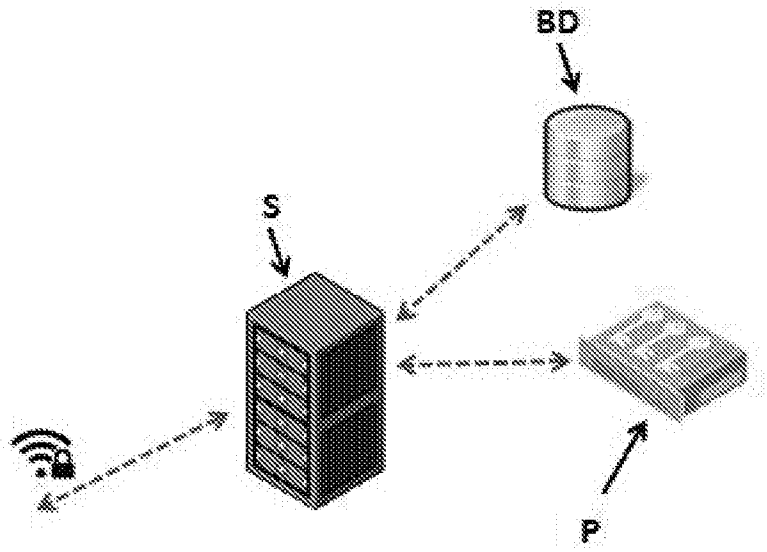

Figura 1

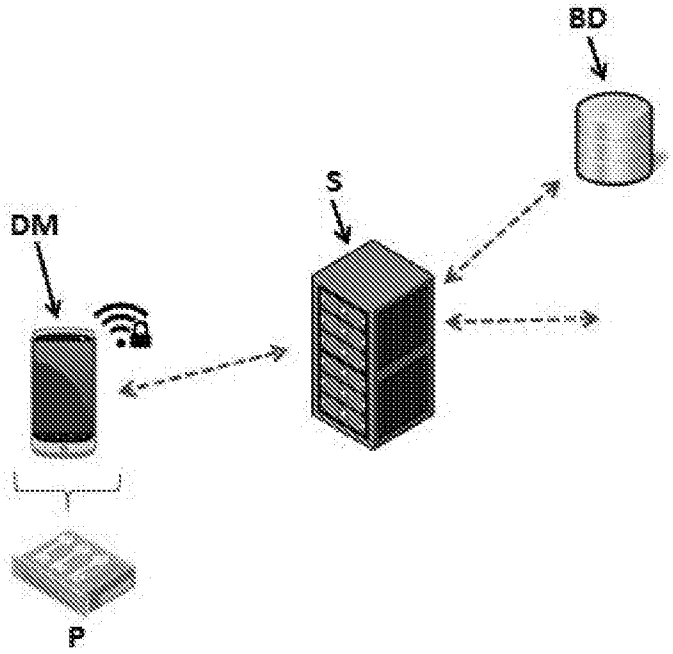

Figura 2

Figura 3

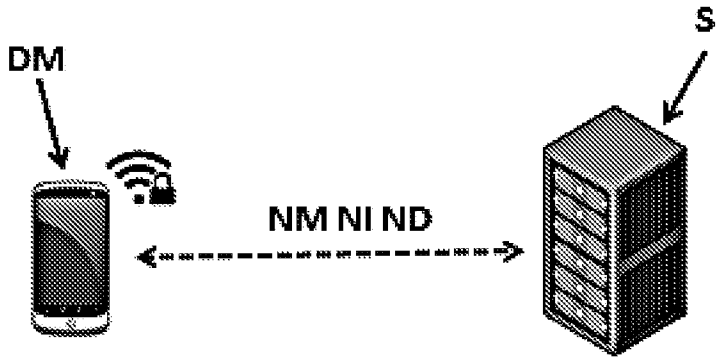

Figura 4

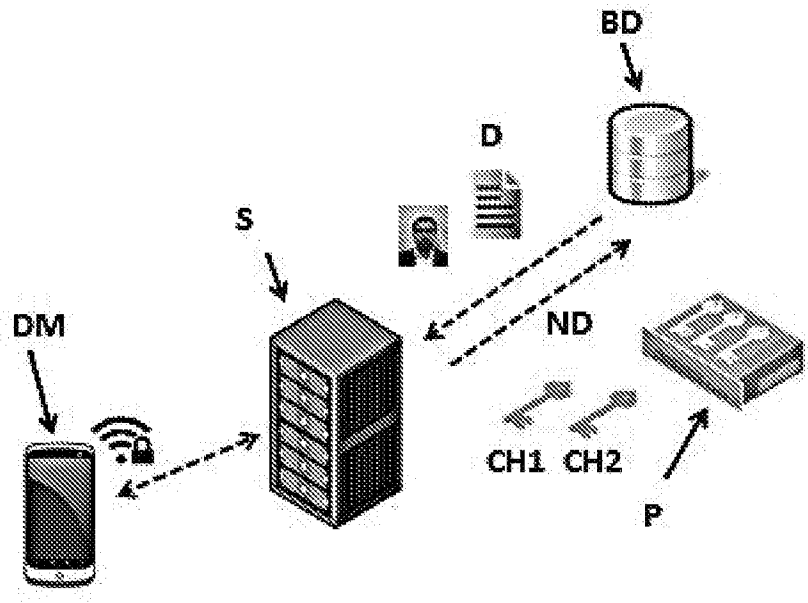

Figura 5

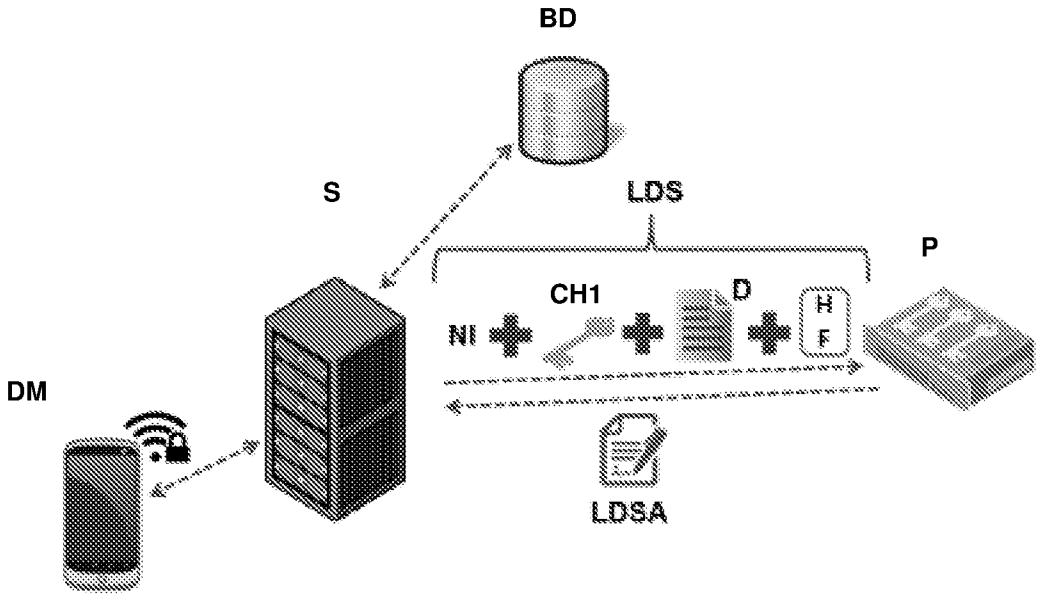

Figura 6

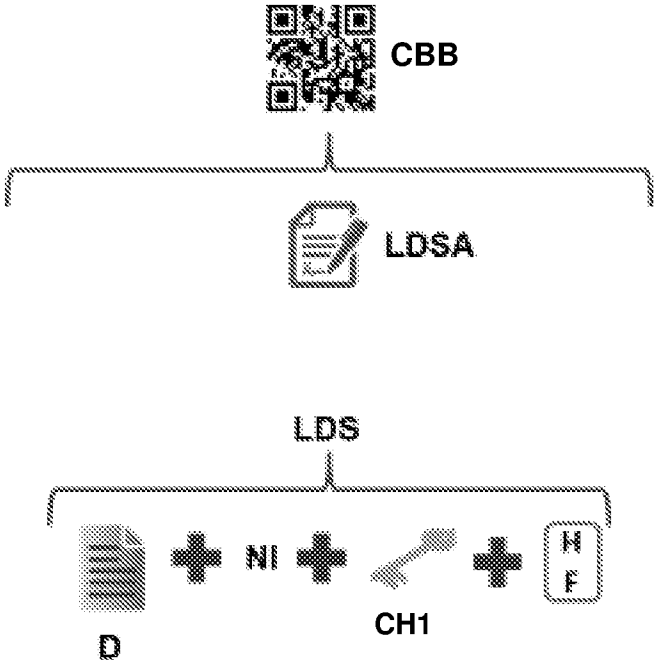

Figura 7a

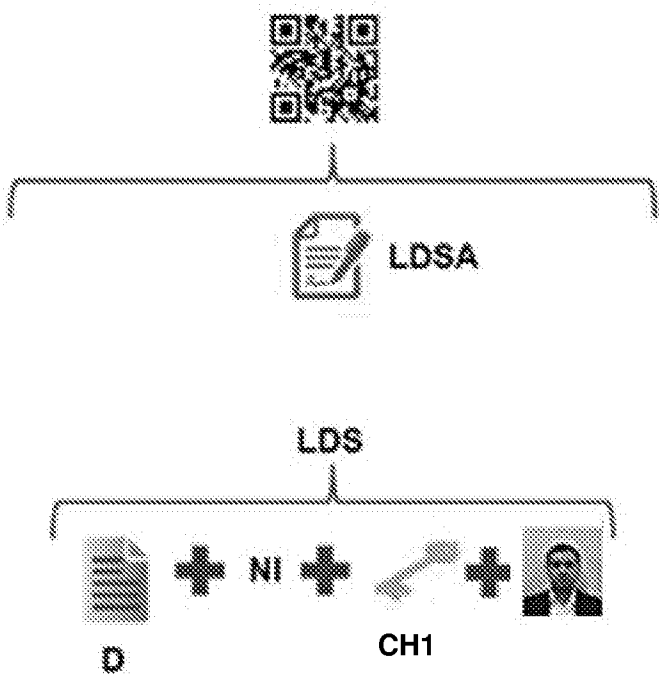

Figura 7b

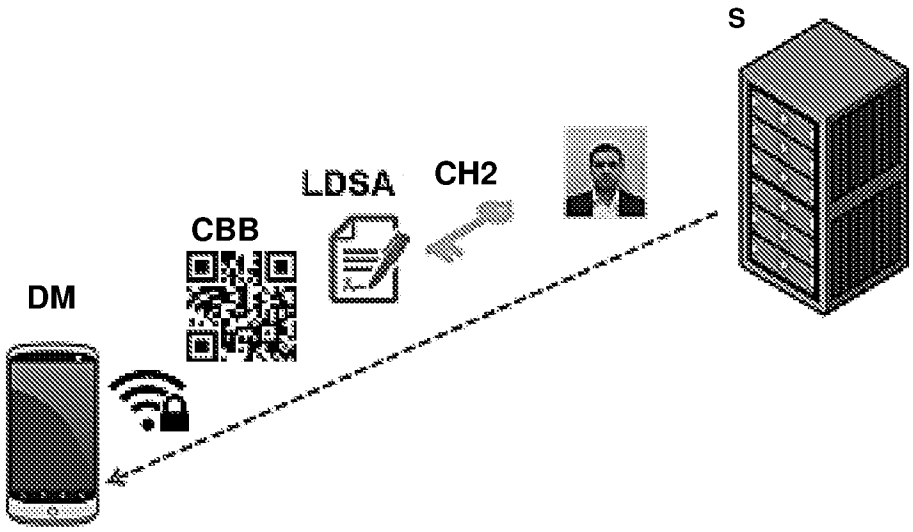

Figura 8

Figura 9

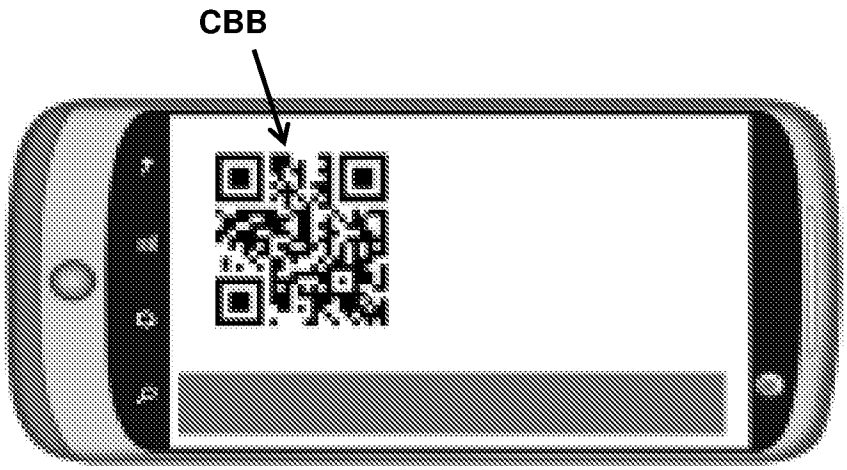

Figura 10

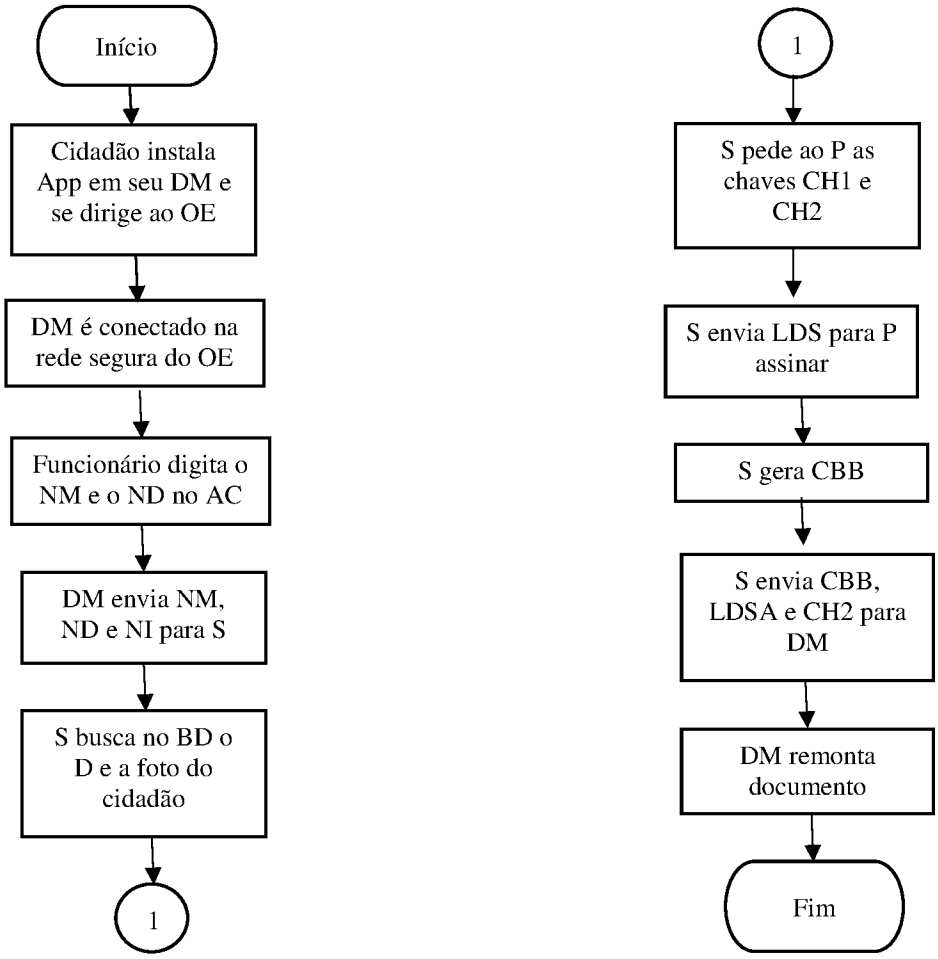
Início
Cidadão instala App em seu DM e se dirige ao OE
DM é conectado na rede segura do OE
Funcionário digita o NM e o ND no AC
DM envia NM, ND e NI para S
S busca no BD o D e a foto do cidadão
1
1
S pede ao P as chaves CH1 e CH2
S envia LDS para P assinar
S gera CBB
S envia CBB, LDSA e CH2 para DM
DM remonta documento
Fim

Figura 11

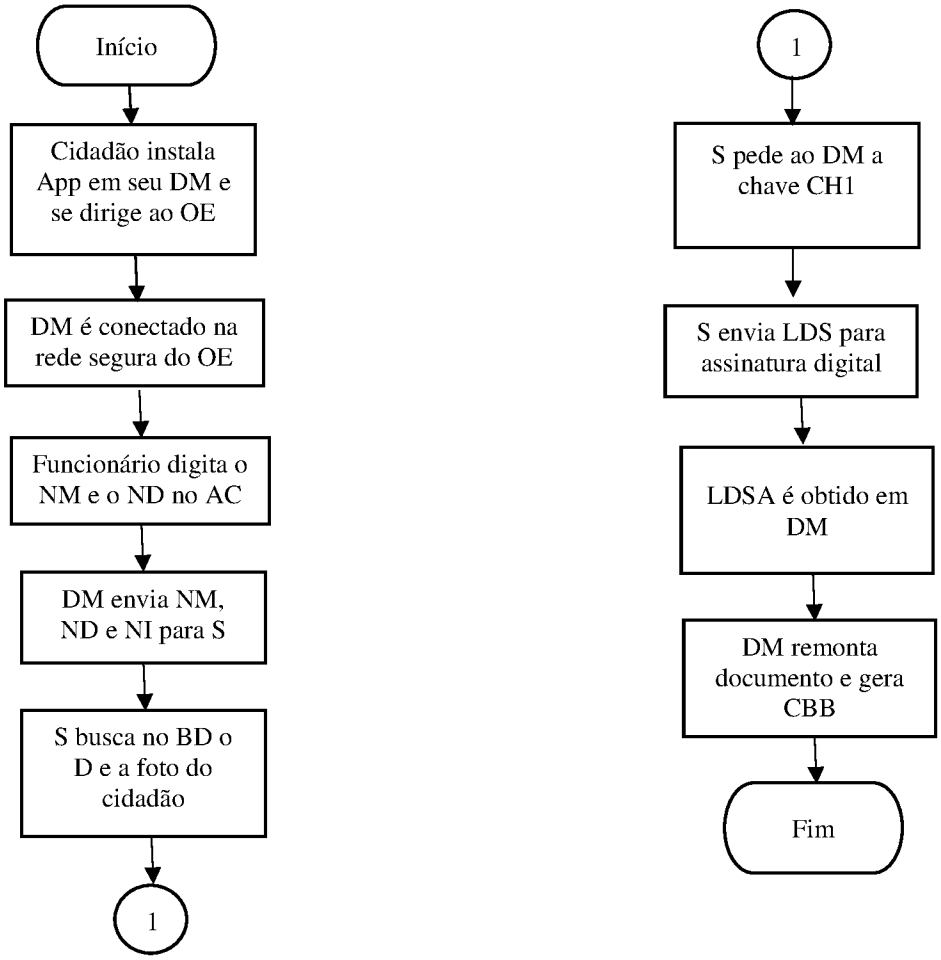
Início
Cidadão instala App em seu DM e se dirige ao OE
DM é conectado na rede segura do OE
Funcionário digita o NM e o ND no AC
DM envia NM, ND e NI para S
S busca no BD o D e a foto do cidadão
1
1
S pede ao DM a chave CH1
S envia LDS para assinatura digital
LDSA é obtido em DM
DM remonta documento e gera CBB
Fim

Figura 12

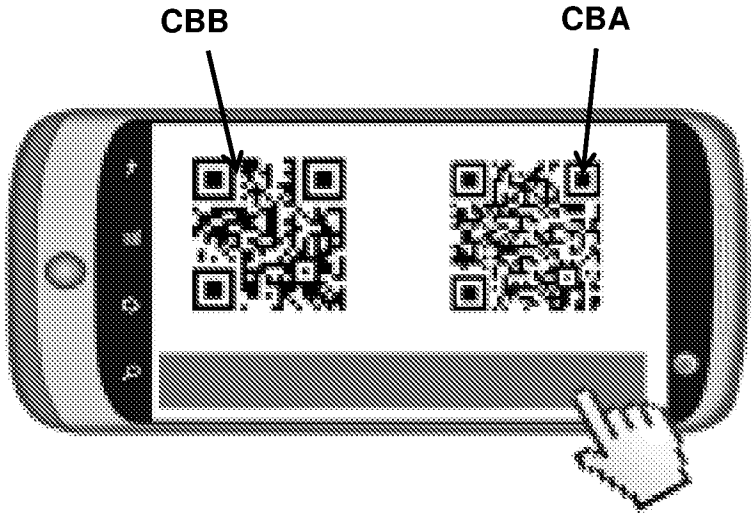

Figura 13

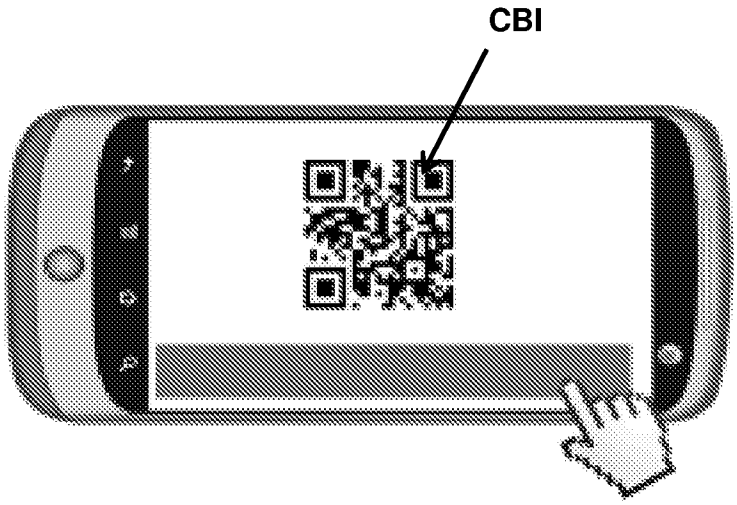

Figura 14

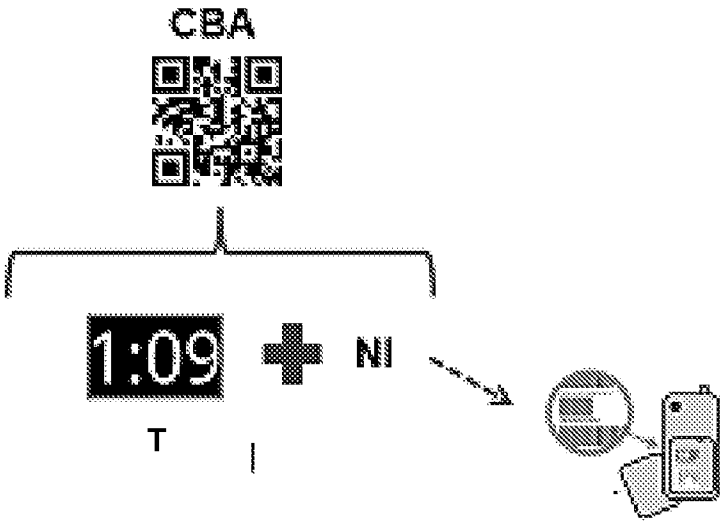

Figura 15

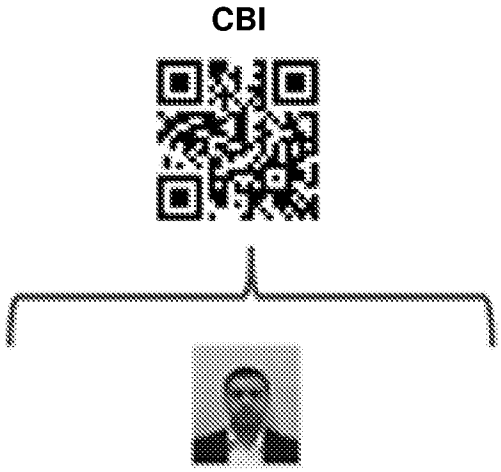

Figura 16

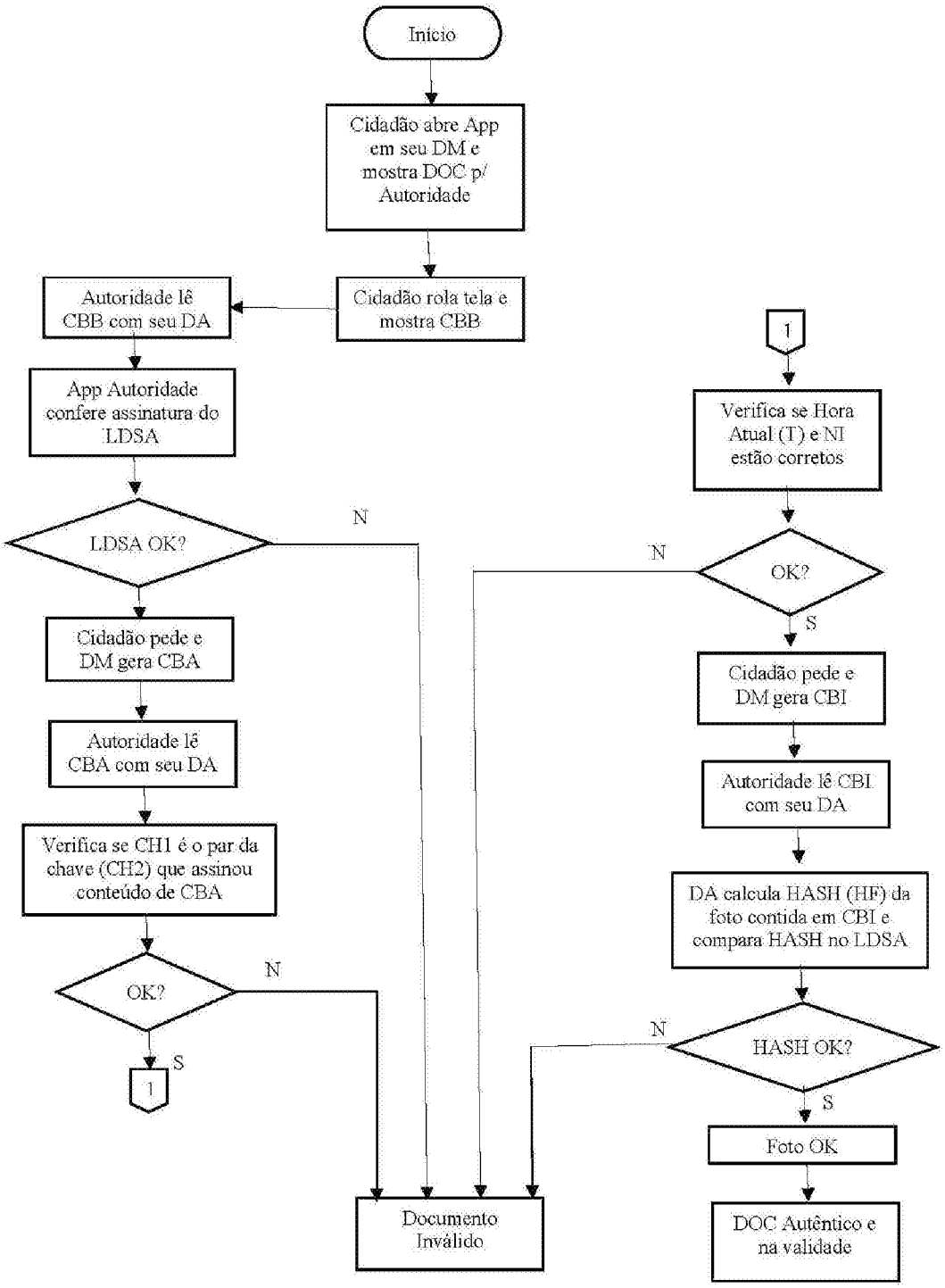
Início
Cidadão abre App em seu DM e mostra DOC p/ Autoridade
Cidadão rola tela e mostra CBB
Autoridade lê CBB com seu DA
App Autoridade confere assinatura do LDSA
LDSA OK?
N
Cidadão pede e DM gera CBA
Autoridade lê CBA com seu DA
Verifica se CH1 é o par da chave (CH2) que assinou conteúdo de CBA
OK?
N
S
1
1
Verifica se Hora Atual (T) e NI estão corretos
OK?
N
S
Cidadão pede e DM gera CBI
Autoridade lê CBI com seu DA
DA calcula HASH (HF) da foto contida em CBI e compara HASH no LDSA
HASH OK?
N
S
Foto OK
DOC Autêntico e na validade
Documento Inválido

Figura 17

INTERNATIONAL SEARCH REPORT

International application No.
PCT/BR2017/050204

A. CLASSIFICATION OF SUBJECT MATTER

G06F21/33 (2013.01), G06F21/34 (2013.01), G06F21/64 (2013.01), G06K19/067 (2006.01), H04L9/32 (2006.01)

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC G06F21/33, G06F21/34, G06F21/64, G06K19/067, H04L9/32

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPODOC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	International Civil Aviation Organization. Doc. 9303 – Machine Readable Travel Documents [online]. Part 10 – Logical Data Structure (LDS) for Storage of Biometrics and Other Data in the Contactless Integrated Circuit (IC) [online]. Seventh Edition. ICAO, 2015 [access on 14/Nov/2017]. Retrieved from <https://www.icao.int/publications/Documents/9303_p10_cons_en.pdf>. ISBN: 978-92-9249-799-6. (the whole document)	1 to 15
X	International Civil Aviation Organization. Doc. 9303 – Machine Readable Travel Documents [online]. Part 11 – Security Mechanisms for MRTDs [online]. Seventh Edition. ICAO, 2015 [access on 14/Nov/2017]. Retrieved from <https://www.icao.int/publications/Documents/9303_p11_cons_en.pdf>. ISBN: 978-92-9249-799-6. (p.8; p.21; p.23 a 26; 'Appendix C')	1 to 15

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
16/Nov/2017	22/11/2017

Name and mailing address of the ISA/ **BR**
INSTITUTO NACIONAL DA PROPRIEDADE INDUSTRIAL
Rua Sao Bento nº 1, 17º andar
cep: 20090-010, Centro - Rio de Janeiro/RJ

Facsimile No. +55 21 3037-3663

Authorized officer

Ricardo Affonso Grings Herbert

Telephone No. +55 21 3037-3493/3742

Form PCT/ISA/210 (second sheet) (January 2015)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/BR2017/050204

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	International Civil Aviation Organization. Doc. 9303 – Machine Readable Travel Documents [online]. Part 12 – Public Key Infrastructure for MRTDs [online]. Seventh Edition. ICAO, 2015 [access on 14/Nov/2017]. Retrieved from <https://www.icao.int/publications/Documents/9303_p12_cons_en.pdf>. ISBN: 978-92-9249-799-6. (the whole document)	1 to 15
X	US 2013243266 A1 (L 1 SECURE CREDENTIALING INC [US]) 19 September 2013 (2013-09-19) (the whole document)	1 to 8; 10 to 12; 15
A	WO 2014080210 A1 (BARCLAYS BANK PLC [GB]) 30 May 2014 (2014-05-30)	
A	US 2014089682 A1 (APPLE INC [US]) 27 March 2014 (2014-03-27)	

US 2013243266 A1	2013-09-19	CA 2867002 A1 EP 2825993 A1 WO 2013138589 A1	2013-09-19 2015-01-21 2013-09-19
US 2014089682 A1	2014-03-27	US 8832465 B2	2014-09-09
WO 2014080210 A1	2014-05-30	None	

RELATÓRIO DE PESQUISA INTERNACIONAL

Depósito internacional Nº
PCT/BR2017/050204

A. CLASSIFICAÇÃO DO OBJETO

G06F21/33 (2013.01), G06F21/34 (2013.01), G06F21/64 (2013.01), G06K19/067 (2006.01), H04L9/32 (2006.01)

De acordo com a Classificação Internacional de Patentes (IPC) ou conforme a classificação nacional e IPC

B. DOMÍNIOS ABRANGIDOS PELA PESQUISA

Documentação mínima pesquisada (sistema de classificação seguido pelo símbolo da classificação)

IPC G06F21/33, G06F21/34, G06F21/64, G06K19/067, H04L9/32

Documentação adicional pesquisada, além da mínima, na medida em que tais documentos estão incluídos nos domínios pesquisados

Base de dados eletrônica consultada durante a pesquisa internacional (nome da base de dados e, se necessário, termos usados na pesquisa)

EPODOC

C. DOCUMENTOS CONSIDERADOS RELEVANTES

Categoria*	Documentos citados, com indicação de partes relevantes, se apropriado	Relevante para as reivindicações Nº
X	International Civil Aviation Organization. Doc. 9303 – Machine Readable Travel Documents [online]. Part 10 – Logical Data Structure (LDS) for Storage of Biometrics and Other Data in the Contactless Integrated Circuit (IC) [online]. Seventh Edition. ICAO, 2015 [acesso em 14/Nov/2017]. Recuperado de <https://www.icao.int/publications/Documents/9303_p10_cons_en.pdf>. ISBN: 978-92-9249-799-6. (todo o documento)	1 a 15
X	International Civil Aviation Organization. Doc. 9303 – Machine Readable Travel Documents [online]. Part 11 – Security Mechanisms for MRTDs [online]. Seventh Edition. ICAO, 2015 [acesso em 14/Nov/2017]. Recuperado de <https://www.icao.int/publications/Documents/9303_p11_cons_en.pdf>. ISBN: 978-92-9249-799-6. (p.8; p.21; p.23 a 26; 'Appendix C')	1 a 15

☒ Documentos adicionais estão listados na continuação do quadro C ☒ Ver o anexo de famílias das patentes

* Categorias especiais dos documentos citados:

"A" documento que define o estado geral da técnica, mas não é considerado de particular relevância.

"E" pedido ou patente anterior, mas publicada após ou na data do depósito internacional

"L" documento que pode lançar dúvida na(s) reivindicação(ões) de prioridade ou na qual é citado para determinar a data de outra citação ou por outra razão especial

"O" documento referente a uma divulgação oral, uso, exibição ou por outros meios.

"P" documento publicado antes do depósito internacional, porém posterior a data de prioridade reivindicada.

"T" documento publicado depois da data de depósito internacional, ou de prioridade e que não conflita com o depósito, porém citado para entender o princípio ou teoria na qual se baseia a invenção.

"X" documento de particular relevância; a invenção reivindicada não pode ser considerada nova e não pode ser considerada envolver uma atividade inventiva quando o documento é considerado isoladamente.

"Y" documento de particular relevância; a invenção reivindicada não pode ser considerada envolver atividade inventiva quando o documento é combinado com um outro documento ou mais de um, tal combinação sendo óbvia para um técnico no assunto.

"&" documento membro da mesma família de patentes.

Data da conclusão da pesquisa internacional	Data do envio do relatório de pesquisa internacional:
16/Nov/2017	22/11/2017

Nome e endereço postal da ISA/**BR**	Funcionário autorizado
INPI INSTITUTO NACIONAL DA PROPRIEDADE INDUSTRIAL Rua Sao Bento nº 1, 17º andar cep: 20090-010, Centro - Rio de Janeiro/RJ	**Ricardo Affonso Grings Herbert**
Nº de fax: +55 21 3037-3663	Nº de telefone: +55 21 3037-3493/3742

C. DOCUMENTOS CONSIDERADOS RELEVANTES

Categoria*	Documentos citados, com indicação de partes relevantes, se apropriado	Relevante para as reivindicações Nº
X	International Civil Aviation Organization. Doc. 9303 – Machine Readable Travel Documents [online]. Part 12 – Public Key Infrastructure for MRTDs [online]. Seventh Edition. ICAO, 2015 [acesso em 14/Nov/2017]. Recuperado de <https://www.icao.int/publications/Documents/9303_p12_cons_en.pdf>. ISBN: 978-92-9249-799-6. (todo o documento)	1 a 15
X	US 2013243266 A1 (L 1 SECURE CREDENTIALING INC [US]) 19 setembro 2013 (2013-09-19) (todo o documento)	1 a 8; 10 a 12; 15
A	WO 2014080210 A1 (BARCLAYS BANK PLC [GB]) 30 maio 2014 (2014-05-30)	
A	US 2014089682 A1 (APPLE INC [US]) 27 março 2014 (2014-03-27)	

RELATÓRIO DE PESQUISA INTERNACIONAL
Informação relativa a membros da família da patentes

Depósito internacional Nº
PCT/BR2017/050204

Documentos de patente citados no relatório de pesquisa	Data de publicação	Membro(s) da família de patentes	Data de publicação
US 2013243266 A1	2013-09-19	CA 2867002 A1 EP 2825993 A1 WO 2013138589 A1	2013-09-19 2015-01-21 2013-09-19
US 2014089682 A1	2014-03-27	US 8832465 B2	2014-09-09
WO 2014080210 A1	2014-05-30	Nenhum	