República Federativa do Brasil

Ministério do Desenvolvimento, Indústria, Comércio e Serviços

Instituto Nacional da Propriedade Industrial

(21) BR 102022012874-0 A2

(22) Data do Depósito: 28/06/2022

(43) Data da Publicação Nacional: 09/01/2024

(54) Título: PROCESSO PARA ASSINATURA E VERIFICAÇÃO DE ASSINATURA DIGITAL

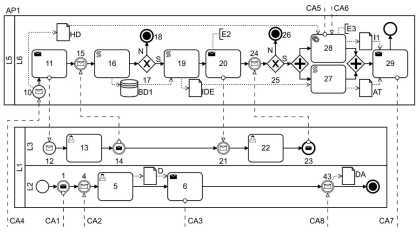
(51) Int. Cl.: H04L 9/32; H04L 9/40.

(52) CPC: H04L 9/3247; H04L 9/3213; H04L 63/0823; H04L 63/126.

(71) Depositante(es): UNIVERSIDADE FEDERAL DE SANTA CATARINA; INSTITUTO FEDERAL DO RIO GRANDE DO SUL.

(72) Inventor(es): FREDERICO SCHARDONG; LUCAS MAYR DE ATHAYDE; RICARDO FELIPE CUSTÓDIO.

(57) Resumo: PROCESSO PARA ASSINATURA E VERIFICAÇÃO DE ASSINATURA DIGITAL. A presente invenção se refere a um novo processo para assinar digitalmente documentos digitais (exemplo, um texto feito em um editor de texto e salvo no formato PDF). A assinatura digital atualmente pode ser realizada de diversas formas, a mais amplamente aceita é através de um certificado digital (exemplo eCNPJ). A assinatura digital é análoga a assinatura física (a próprio punho) de um documento físico. O diferencial em relação ao estado da técnica é a criação do conceito de certificado de uso único. Através dele, um documento é associado ao certificado e este certificado não pode ser utilizado para nada a não ser assinar digitalmente este documento específico. Outro diferencial é associar a validade de uma assinatura a existência de três registros em uma blockchain, um para cada entidade envolvida na assinatura (IDP, SAD e AC). Desta forma, só é possível fraudar uma assinatura se as três entidades forem corrompidas, com incremento da segurança da assinatura.



“PROCESSO PARA ASSINATURA E VERIFICAÇÃO DE ASSINATURA DIGITAL”

CAMPO DA INVENÇÃO

[01] A presente invenção se refere a um novo processo para assinar digitalmente documentos digitais (exemplo, um texto feito em um editor de texto e salvo no formato PDF). A assinatura digital atualmente pode ser realizada de diversas formas, a mais amplamente aceita é através de um certificado digital (exemplo eCNPJ). A assinatura digital é análoga a assinatura física (a próprio punho) de um documento físico. A invenção aumenta a segurança das assinaturas digitais e ao mesmo tempo apresenta para o usuário interações mais simples do que a maneira que assinatura digital é feita hoje.

ANTECEDENTES DA INVENÇÃO

[02] Num ambiente cada vez mais conectado a assinatura eletrônica permite que um usuário assine um documento em meio digital de modo conveniente, sendo importante destacar que no Brasil um documento com a assinatura digital tem a mesma validade de um documento com assinatura física. Várias soluções têm sido propostas no estado da técnica.

[03] O documento WO2014033695, por exemplo, revela um método para assinatura remota de pelo menos um documento eletrônico, compreendendo as etapas de: definir pelo menos uma estação administradora e pelo menos uma estação cliente; estabelecer uma chamada de vídeo entre o referido administrador e as estações cliente; afixar assinaturas digitais ao referido pelo menos um documento eletrônico na referida pelo menos uma estação de cliente e carimbos de hora na referida pelo menos uma estação de administrador e na referida pelo menos uma estação de cliente; gravar a referida chamada de vídeo e afixar um carimbo de hora na mesma.

[04] O documento CN109190347, por sua vez, revela um método de assinatura eletrônica que compreende as etapas de realização de autenticação via

cliente por um usuário; gerar e armazenar uma assinatura eletrônica de um usuário autenticado pelo cliente; gerar um código bidimensional a ser assinado pelo servidor em um documento eletrônico a ser assinado; escanear o código bidimensional a ser assinado gerado na etapa 3 pelo cliente, anexar os dados de assinatura eletrônica gerados na etapa 2 ao documento eletrônico a ser assinado e gerar simultaneamente um código bidimensional de verificação para verificar a autenticidade no documento eletrônico a ser assinado; a varredura percorre o código bidimensional de verificação gerado na etapa 4 pelo cliente para verificar a autenticidade da assinatura eletrônica. O método de assinatura eletrônica realiza a antiviolação e rastreabilidade da assinatura por certificado digital, identificação biométrica e verificação de código bidimensional, solucionando os problemas de segurança e conveniência no processo de assinatura remota do usuário.

[05] Já o documento CN107579827 revela um método de assinatura de documento eletrônico baseado em um terceiro confiável e na tecnologia de reconhecimento facial compreende uma etapa de inicialização e uma etapa de assinatura. Uma plataforma de assinatura e um terceiro confiável restringem-se mutuamente; a plataforma de assinatura controla a origem de uma tarefa de assinatura de documento eletrônico e os direitos de login dos usuários; e o terceiro é responsável pela conclusão da certificação da assinatura e do ato de assinatura, e a tarefa de assinar não pode ser concluída se nenhuma das partes for confiável. O método da presente invenção utiliza o reconhecimento biológico em vez da verificação de senha comum para certificação do sujeito, o que não só torna o reconhecimento mais seguro, mas também torna a assinatura do documento eletrônico fortemente vinculada às informações biológicas do sujeito e pode fornecer uma "não capacidade de repúdio" quando a disputa ocorre.

[06] Os produtos e documentos já conhecidos no estado da técnica têm em comum o armazenamento e reutilização do certificado digital e chave privada para

realizar assinatura digital. A principal desvantagem do armazenamento do certificado e sua chave privada é que não é possível saber se estão sendo usados para assinar outros documentos ou para outros fins sem o consentimento e conhecimento do usuário. O dano que pode ser causado caso ocorra o comprometimento da chave privada pode ser desastroso, visto que documentos eletrônicos assinados digitalmente com certificados digitais têm valor legal semelhante (ou igual, caso o certificado seja qualificado) a uma assinatura a próprio punho.

[07] Outras desvantagens dos trabalhos do estado da técnica em relação a nossa invenção são decorrentes do uso de certificados digitais reutilizáveis (i.e. que podem assinar um número indeterminado de documentos): (i) o processo de backup de Autoridades Certificadoras (ACs), i.e. as entidades que geram e revogam certificados, e chaves privadas é delicado e deve ser feito regularmente, implicando no uso de mais hardware para o gerenciamento de ACs; (ii) as ACs precisam realizar cerimônias de emissão de listas de certificados revogados mesmo quando nenhum novo certificado foi revogado; (iii) o processo de verificação de assinaturas digitais exige consultar listas de certificados revogados, o que aumenta a complexidade do processo de verificação de assinaturas.

SUMÁRIO DA INVENÇÃO

[08] A presente invenção se refere a um novo processo para assinar digitalmente documentos digitais (exemplo, um texto feito em um editor de texto e salvo no formato PDF). A assinatura digital atualmente pode ser realizada de diversas formas, a mais amplamente aceita é através de um certificado digital (exemplo eCNPJ). A assinatura digital é análoga a assinatura física (a próprio punho) de um documento físico. A invenção aumenta a segurança das assinaturas digitais e ao mesmo tempo apresenta para o usuário interações mais simples do que a maneira que assinatura digital é feita hoje.

[09] A presente invenção se vale de identidade eletrônica para identificar e autenticar usuários, mais do que um fator de autenticação é usado. O usuário não precisa gerir certificado algum, pois um novo certificado é criado e usado para assinar um documento que o usuário envia ao sistema. O documento assinado é devolvido ao usuário e o certificado e sua chave são descartados pelo servidor.

BREVE DESCRIÇÃO DOS DESENHOS

[010] A Figura 1 é um diagrama BPMN com a descrição detalhada do processo de assinatura digital de documentos eletrônicos, mais especificamente a primeira parte do processo de assinatura (AP1) envolvendo o usuário (L1) e o provedor de identidade (L5).

[011] A Figura 2 é um diagrama BPMN com a descrição detalhada do processo de assinatura digital de documentos eletrônicos, mais especificamente a segunda parte do processo de assinatura (AP2) envolvendo o serviço de assinatura de documentos (L4) e a autoridade certificadora (L8).

[012] A Figura 3 é um diagrama BPMN com a descrição detalhada do processo de assinatura digital de documentos eletrônicos, mais especificamente a terceira parte do processo de assinatura (AP3) envolvendo a *blockchain* (L7).

[013] A Figura 4 é um diagrama BPMN com a descrição detalhada do processo de verificação de assinatura digital de documentos eletrônicos realizada com o processo de assinatura proposto na presente invenção, mais especificamente a parte inicial do processo de verificação (VP1) envolvendo o verificador da assinatura (L9).

[014] A Figura 5 é um diagrama BPMN com a descrição detalhada do processo de verificação de assinatura digital de documentos eletrônicos realizada com o processo de assinatura proposto na presente invenção, mais especificamente a parte intermediária (VP2) e final (VP3) do processo de verificação envolvendo o verificador da assinatura (L9) e a *blockchain* (L7).

DESCRIÇÃO DETALHADA DA INVENÇÃO

[015] O principal objetivo da presente invenção é criar um processo de assinatura de documentos eletrônicos de mais fácil utilização e de maior segurança que o estado da técnica e o estado da arte e um processo de verificação de assinatura que confira maior segurança. Os objetivos secundários são: (i) associar a assinatura de documentos eletrônicos a identidades eletrônicas, que por sua vez controlam a geração de certificados digitais; e (ii) modificar o ciclo de vida dos certificados digitais, permitindo que certificados sejam gerados para uso único e, desta forma, são irrevogáveis, consequentemente simplificando os processos relacionados a gestão de certificados digitais.

[016] A invenção consiste primariamente em um novo processo de assinatura digital remota de documentos eletrônicos (Figuras 1, 2 e 3). Adicionalmente, é proposto um novo processo de verificação de assinatura digital de documentos eletrônicos (Figuras 4 e 5).

[017] O novo processo de assinatura digital remota de documentos eletrônicos envolve cinco entidades: o usuário (L1), um provedor de identidade (IDP) (L5), um Serviço de Assinatura Digital de documentos eletrônicos (SAD) (L4), uma AC (L8) e uma *blockchain* (L7). Apesar da escolha do IDP, do SAD e da AC caber ao usuário, ele só precisa confiar em uma dessas entidades, pois as outras entidades envolvidas não conseguem forjar uma assinatura se ao menos uma entidade for honesta. O novo processo depende do usuário ser cadastrado (i.e. ter uma identidade eletrônica) em um IDP (como Google, Facebook, gov.br, etc). Diversos fatores de autenticação podem ser utilizados (senha, OTP, biometria facial, íris, impressão digital, etc) na autenticação do usuário para aumentar a confiança que o usuário é de fato dono e controlador da identidade eletrônica em questão. Recomendamos o uso de pelo menos dois fatores de autenticação distintos (por exemplo, senha + OTP, ou senha + biometria). O novo processo é descrito a seguir.

[018] Primeiro, o usuário acessa o SAD (1,2,3,4) e faz o upload do documento (D) a ser assinado (5,6,7). O SAD calcula o resumo criptográfico do documento (8) a ser assinado (HD). Resumo criptográfico é uma sequência de bits que unicamente identifica o documento com base em seu conteúdo.

[019] Segundo, o SAD encaminha para o IDP o resumo criptográfico do documento (HD) a ser assinado na solicitação (9,10) de autenticação do usuário e autorização de acesso aos atributos (AT) do usuário (por exemplo nome, e-mail e CPF). No portal do IDP (11, 12), o usuário se autentica usando os fatores de autenticação previamente cadastrados (13, 14, 15, 16, 17, 19). O IDP então solicita autorização do usuário para compartilhar o conjunto de dados solicitados pelo SAD (20, 21). Ao aceitar compartilhar os atributos (22, 23, 24, 25), um bloco é salvo na blockchain pelo IDP (28) contendo o resumo criptográfico do documento a ser assinado (HD). O bloco inserido na *blockchain* possui um identificador único (I1), doravante chamado de identificador do bloco do IDP (I1), e é enviado para o SAD (29) junto com os atributos do usuário (27, AT, 30).

[020] Terceiro, o SAD gera um par de chaves (31) (chave pública (PK) e chave privada (SK)) para assinar o documento digitalmente (39), enviando (32) o resumo criptográfico do documento a ser assinado (HD), a chave pública (PK), os atributos do usuário (AT) e o identificador do bloco do IDP (I1) para a autoridade certificadora.

[021] Quarto, a autoridade certificadora recebe (33) o resumo criptográfico do documento a ser assinado (HD), a chave pública (PK), os atributos do usuário (AT) e o identificador do bloco do IDP (I1) e emite (34) um certificado digital de uso único (U) contendo o resumo criptográfico do documento a ser assinado (HD), a chave pública (PK), e os atributos do usuário (AT). O certificado digital de uso único (U) tem prazo de validade igual ao da AC que o emitiu (geralmente 20, 30 ou 40 anos), pois é impossível que seja utilizado para outra finalidade devido ao resumo criptográfico do documento (HD) que ele está associado. O certificado digital de uso único (U) não

contém um link para uma lista de certificados revogados, pois a AC que o emitiu não possui lista de revogação, já que os certificados têm uso único e não precisam ser revogados. A AC calcula (35) o resumo criptográfico do certificado digital de uso único (HU) e o insere em um bloco na *blockchain* (36) juntamente com o identificador do bloco do IDP (I1). Este novo bloco possui um identificador único (I2), doravante chamado de identificador do bloco da AC (I2).

[022] Quinto, o certificado digital de uso único (U) e o identificador do bloco da AC (I2) são retornados para o SAD (37, 38), que utiliza o certificado (U) para realizar a assinatura digital (39) juntamente com a chave privada (SK) e imediatamente descarta a chave privada e o certificado. O SAD calcula (40) o resumo criptográfico do documento eletrônico assinado digitalmente (HDA), e o insere na *blockchain* (41) juntamente com o identificador do bloco da AC (I2). O novo bloco possui um identificador único (I3) e é doravante chamado de identificador do bloco do SAD (I3). Por fim, o documento eletrônico assinado digitalmente (DA) com o certificado digital de uso único (U) é retornado para o usuário (42). O documento eletrônico assinado digitalmente (DA) recebido pelo usuário (43) respeita os padrões existentes de assinatura de documentos eletrônicos (ISO 32000) e pode ser validado normalmente como qualquer outro documento eletrônico assinado seguindo o estado da técnica.

[023] O novo processo de verificação (Figuras 4 e 5) envolve duas entidades: o verificador (L9) e a blockchain (L7). O processo é descrito a seguir.

[024] Primeiro, o verificador recebe (44) um documento eletrônico assinado digitalmente (DA), extraindo (46,50) o certificado digital de uso único (U), a assinatura digital (AD) e o documento eletrônico (D). Também é calculado (45,49,51) o resumo criptográfico do documento eletrônico assinado digitalmente (HDA), o resumo criptográfico do certificado digital de uso único (HU), e o resumo criptográfico do documento eletrônico (HD). São extraídos (47,48) do certificado digital de uso único (U) a chave pública (PK) e o resumo criptográfico do documento eletrônico (HD').

[025] Segundo, a chave pública (PK), a assinatura digital (AD) e o resumo criptográfico do documento eletrônico calculado (HD) são submetidos a uma função de criptografia que testa se a assinatura digital é válida (52). Caso não for válida, o processo é encerrado com erro (53, 54). Caso for válida, o resumo criptográfico do documento eletrônico calculado (HD) e o resumo criptográfico extraído do certificado digital de uso único (HD') são comparados (55, 56). Caso sejam diferentes, o processo é encerrado com erro (54). Caso sejam iguais, o processo de verificação continua (CV1).

[026] Terceiro, uma busca é realizada na *blockchain* (57) pelo resumo criptográfico do documento eletrônico assinado digitalmente (HDA). Caso não seja encontrado (58), o processo se encerra com erro de verificação (54). Caso seja encontrado (58), significa que um SAD criou este bloco (B3), e consequentemente, o bloco contém o identificador do bloco da AC (I2) e algum tipo de identidade que permita verificar qual SAD criou este bloco (IDS). Estas duas informações são extraídas do bloco (59).

[027] Quarto, uma busca é realizada na *blockchain* (57) pelo bloco da AC (B2) através do identificador do bloco da AC (I2). Caso não seja encontrado (58), o processo é encerrado com erro (54). Caso seja encontrado (58), significa que uma AC criou este bloco (B2), e consequentemente, o bloco (B2) contém o resumo criptográfico do certificado digital de uso único (HU'), o identificador do bloco do IDP (I1) e algum tipo de identidade (IDA) que permita verificar qual AC criou este bloco (B2). Estas três informações (HU', I1, IDA) são extraídas (60) do bloco (B2). O resumo criptográfico do certificado digital de uso único extraído do bloco da AC (HU') é comparado (55) com o resumo criptográfico do certificado digital de uso único extraído do documento eletrônico assinado digitalmente no início do processo (HU). Caso sejam diferentes (56), o processo é encerrado com erro (54). Caso sejam iguais, o processo de verificação de assinatura continua.

[028] Quinto, uma busca é realizada na *blockchain* (57) pelo bloco do IDP através do identificador do bloco do IDP (I1) obtido anteriormente (60). Caso não for encontrado (58), o processo é encerrado com erro (54). Caso seja encontrado (58), significa que um IDP criou este bloco, e consequentemente, o bloco contém o resumo criptográfico do documento eletrônico (antes de ser assinado) (HD''), e algum tipo de identidade (IDI) que permita verificar qual IDP criou este bloco. Estas duas informações são extraídas do bloco. O resumo criptográfico do documento eletrônico (HD'') é comparado com o resumo criptográfico do documento eletrônico (HD) extraído do documento eletrônico assinado digitalmente (DA) no início do processo de verificação (51). Caso sejam diferentes (56), o processo é encerrado com erro (54). Caso sejam iguais (56), o processo de verificação continua (62).

[029] Sexto, é verificado se a AC é confiável (62, 63). Essa verificação usa como base a lista de ACs confiáveis (por exemplo uma lista conforme especificado na norma ETSI TS 119 612). Caso a AC (IDA) esteja presente na lista, ela é confiável (63) e o processo de verificação é encerrado retornando um artefato (AR) que explicita que a assinatura eletrônica no documento é válida (64, 65). Caso a AC não seja confiável (63), é testado se o IDP é confiável (66, 67). Caso o IDP seja confiável, o processo é encerrado retornando um artefato que explicita que a assinatura eletrônica é válida (64, 65). Caso o IDP não seja confiável, é testado se o SAD é confiável (68, 69). Caso o SAD seja confiável, o processo é encerrado retornando um artefato que explicita que a assinatura eletrônica é válida (66, 67). Caso o SAD não seja confiável, o processo é encerrado retornando erro de verificação (54). O artefato (AR) pode ser um documento eletrônico contendo um relatório das tarefas executadas pelo verificador, bem como apenas uma afirmação que a assinatura em questão é válida. O artefato deve ser assinado digitalmente pelo verificador, de forma que sua identidade possa ser verificada bem como a integridade do artefato.

[030] É importante observar que o processo de verificação verifica apenas uma assinatura em um documento. Caso existam múltiplas assinaturas, o processo deve ser repetido para cada uma. O artefato resultante da verificação de múltiplas assinaturas pode ser compilado em um único documento assinado digitalmente pelo verificador atestando o resultado do processo de verificação.

[031] As vantagens em relação ao estado da técnica e da arte são: (i) maior usabilidade, pois o usuário precisa apenas informar um documento para ser assinado e se autenticar perante seu IDP, não sendo apresentado com interfaces e interações para emissão ou escolha de certificado digital ou desbloqueio de chave privada; e principalmente (ii) maior segurança, já que é impossível reutilizar um certificado digital de uso único para outros propósitos pois o resumo criptográfico associa unicamente o certificado digital de uso único a um único documento eletrônico. Por fim, a segurança é maior pois todas as entidades envolvidas no processo de assinatura registram suas atividades na *blockchain*. Caso haja suspeita de fraude, basta buscar na *blockchain* por um bloco contendo o resumo criptográfico de um documento eletrônico assinado digitalmente, e a partir do identificador deste bloco (identificador do bloco do SAD), encontrar os outros dois blocos associados a este documento (bloco da AC e o bloco do IDP). Se ao menos uma das três entidades envolvidas (IDP, AC, SAD) for ilibada e íntegra, não será possível falsificar uma assinatura. Em outras palavras, é necessário que as três entidades sejam corruptas para falsificar uma assinatura e criar os três blocos.

[032] O sistema de acordo com a presente invenção permite: (i) a criação do conceito de certificado digital de uso único, onde cada certificado é unicamente associado a um documento eletrônico através do resumo criptográfico do documento eletrônico a ser assinado. Esta característica permite que o certificado tenha data de validade tão longa quanto o certificado da AC que o emite (geralmente 20, 30 ou 40 anos), já que ele nunca será revogado pois não pode ser usado para outros fins a não

ser assinar o documento eletrônico a qual está atrelado. Como o certificado nunca será revogado, é possível omitir completamente a lista de certificados revogados do certificado digital de uso único, bem como eliminar a necessidade de carimbo do tempo na assinatura digital. Por fim, a presente invenção prevê, ainda: (ii) o uso de *blockchain* para adicionar uma camada extra de segurança ao processo de verificação de assinatura. Como a *blockchain* traz um registro imutável de dados, quem recebe um documento eletrônico assinado digitalmente através da presente invenção valida-o buscando na blockchain os blocos que registram as atividades das entidades participantes no processo de assinatura. Caso não existam três blocos seguindo o esquema descrito acima, a assinatura do documento não será válida.

[033] A descrição detalhada da presente invenção também pode ser entendida através de diagramas BPMN, detalhando todas as entidades, artefatos, comunicações e etapas envolvidas.

[034] As figuras 1 a 5, cada uma com um diagrama BPMN, explicam os dois processos propostos: (i) o processo de assinatura digital de documentos eletrônicos; e (ii) o processo de verificação de assinatura de documentos eletrônicos assinados usando o processo de assinatura proposto.

[035] É importante observar que a presente invenção pode ser implementada com compatibilidade com os padrões atuais de assinatura de documentos eletrônicos (ISO 32000). Para isso é necessário: (i) incluir nos certificados digitais de uso único um ponteiro para uma lista de certificados revogáveis (LCR); e (ii) incluir um carimbo do tempo no processo de assinatura digital do documento eletrônico. Com estas duas adições, documentos eletrônicos assinados através do processo de assinatura que inventamos são inteiramente compatíveis com os padrões atuais (ISO 32000), ou seja, a verificação de uma assinatura realizada seguindo o processo descrito na ISO 32000 será realizada com sucesso. Entretanto, somente através do processo de verificação

proposto é possível verificar os registros na *blockchain*, e consequentemente ter certeza que todas as entidades envolvidas no processo de assinatura são idôneas.

[036] É importante destacar que, quando a presente invenção é colocada em prática, podem ser feitas modificações em relação a certos detalhes de construção e forma, sem se afastar dos princípios fundamentais que estão claramente fundamentados no contexto das reivindicações, entendendo-se que a terminologia empregada não pretende limitar a invenção.

RELAÇÃO DOS SINAIS DE REFERÊNCIA

S	Sim
N	Não
L1	Usuário
L2	Assinatura
L3	Autenticação e autorização
L4	Serviço de Assinatura de Documentos (SAD)
L5	Provedor de Identidade (IDP)
L6	Autenticação e autorização
L7	Blockchain
L8	Autoridade Certificadora (AC)
L9	Verificador de Assinatura
AP1	Processo de assinatura parte 1
AP2	Processo de assinatura parte 2
AP3	Processo de assinatura parte 3
CA1	(continuação do processo de assinatura parte 1)
CA2	(continuação do processo de assinatura parte 2)
CA3	(continuação do processo de assinatura parte 3)
CA4	(continuação do processo de assinatura parte 4)
CA5	(continuação do processo de assinatura parte 5)

CA6	(continuação do processo de assinatura parte 6)
CA7	(continuação do processo de assinatura parte 7)
CA8	(continuação do processo de assinatura parte 8)
CA9	(continuação do processo de assinatura parte 9)
CA10	(continuação do processo de assinatura parte 10)
CA11	(continuação do processo de assinatura parte 11)
VP1	Processo de verificação parte 1
VP2	Processo de verificação parte 2
VP3	Processo de verificação parte 3
CV1	Sim (continuação do processo de verificação parte 1)
CV2	(continuação do processo de verificação parte 2)
D	Documento eletrônico
HD	Resumo criptográfico do documento eletrônico
HD'	Resumo criptográfico do documento eletrônico oriundo do certificado de uso único
HD''	Resumo criptográfico do documento eletrônico oriundo do bloco do IDP
BD1	Banco de dados de identidades eletrônicas
BD2	Registro imutável
IDE	Identidade eletrônica
IDS	Identidade do SAD
IDI	Identidade do IDP
IDA	Identidade da AC
AT	Atributos
I1	Identificador do bloco do IDP
I2	Identificador do bloco da AC
I3	Identificador do bloco do SAD

B2	Bloco da AC
B3	Bloco do SAD
SK	Chave privada
U	Certificado digital de uso único
HU	Resumo criptográfico do certificado digital de uso único
HU'	Resumo criptográfico do certificado digital de uso único oriundo do bloco da AC
DA	Documento eletrônico assindo digitalmente
HDA	Resumo criptográfico do documento eletrônico assindo digitalmente
AD	Assinatura digital
AR	Artefato que irrefutavelmente ateste a corretude da assinatura no documento eletrônico assinado digitalmente
1	Requisição de assinatura digital de documento
2	Recebe requisição de assinatura digital
3	Solicita documento eletrônico para ser assinado
4	Recebe requisição de documento
5	Escolhe documento eletrônico
6	Envia o documento eletrônico escolhido
7	Recebe o documento eletrônico
8	Calcula o resumo criptográfico do documento eletrônico
9	Envia requisição
10	Recebe requisição de autenticação
11	Página ou formulário de autenticação
12	Recebe solicitação de autenticação
13	Fornece informações solicitadas (senha, biometria, OTP)
14	Envia resposta de autenticação
15	Recebe informações de autenticação

16 Verifica as informações de autenticação

17 Informações estão corretas?

18 Erro de autenticação

19 Recupera identidade eletrônica do banco de dados

20 Página ou formulário de autorização de compartilhamento de atributos

21 Recebe solicitação de autorização

22 Autoriza ou não compartilhar seus atributos

23 Envia resposta de autorização

24 Recebe resposta do pedido de autorização

25 Usuário autorizou compartilhar seus atributos?

26 Erro de autorização

27 Extrai os atributos da identidade eletrônica

28 Registra o resumo criptográfico na blockchain

29 Envia os atributos e identificador do bloco

30 Recebe os atributos da identidade eletrônica e o identificador do bloco

31 Gera um par de chaves criptográficas

32 Resumo criptográfico, chave pública, atributos, identificador

33 Recebe resumo criptográfico, chave pública, atributos e identificador do bloco do IDP

34 Gera certificado digital de uso único

35 Calcula o resumo criptográfico do certificado de uso único

36 Registra o resumo criptográfico e o identificador na blockchain

37 Envia o certificado digital de uso único e identificador do bloco da AC

38 Recebe certificado e identificador do bloco da AC

39 Assina digitalmente o documento com a chave privada

40 Calcula o resumo criptográfico do documento assinado

41 Registra o resumo criptográfico e o identificador na blockchain

42 Envia documento assinado digitalmente para o usuário

43 Recebe documento assinado digitalmente

44 Recebe um documento eletrônico assinado digitalmente

45 Calcula o resumo criptográfico do documento eletrônico assinado digitalmente

46 Extrai o certificado digital de uso único do documento eletrônico assinado digitalmente

47 Extrai o resumo criptográfico do documento associado ao certificado de uso único

48 Extrai a chave pública do certificado de uso único

49 Calcula o resumo criptográfico do certificado

50 Extrai o documento eletrônico e a assinatura digital

51 Calcula o resumo criptográfico do documento eletrônico

52 Testa se a assinatura digital é válida

53 É válida?

54 Erro de verificação

55 Testa se os resumos criptográficos são iguais

56 São iguais?

57 Busca na Blockchain

58 Existe bloco?

59 Extrai o identificador do bloco da AC e a identidade do SAD

60 Extrai resumo criptográfico do certificado de assinatura única, identificador do bloco do IDP e identidade da AC

61 Extrai o resumo criptográfico do documento eletrônico e a identidade do IDP

62 Testa se a AC é confiável

63 AC é confiável?

64 Confecção de artefato assinado digitalmente

65 Assinatura digital de documento eletrônico verificada com sucesso

66 Testa se o IDP é confiável

67 IDP é confiável?

68 Testa se o SAD é conviável

69 SAD é confiável?

E1 Envia requisição de autenticação e autorização de compartilhamento de atributos para geração de certificado de uso único para assinatura do documento eletrônico informando o resumo criptográfico do mesmo.

E2 Atributos como nome, e-mail e CPF e identificador único perante o IDP.

E3 O registro de alguma informação na Blockchain resulta na criação de um novo bloco. Todo bloco tem um identificador único, que é referenciado por um bloco futuro para garantir a imutabilidade dos registros. Todo bloco também é assinado digitalmente, sendo possível identificar e autenticar as entidades que escrevem na blockchain. O resumo criptográfico do documento a ser assinado é inserido em um bloco.

E4 Além dos atributos do usuário fornecidos pelo IDP, também é incluído no certificado digital de uso único informações do o IDP como seu nome e domínio. Algum dos atributos do usuário deve identificá-lo unicamente perante o IDP, e.g. e-mail ou login.

E5 O certificado digital de uso único é um certificado digital x509 irrevogável, que contém uma extensão não-crítica informando o resumo criptográfico do documento eletrônico assinado digitalmente com esse certificado.

E6 Ambos resumo criptográfico do certificado digital de uso único e identificador do bloco criado pelo provedor de identidade são registrados em um novo bloco. O resultado dessa operação na Blockchain é a criação de um bloco contendo estas duas informações. Este novo bloco também tem um identificador (chamado de identificador do bloco da AC), que é retornado pela Blockchain após a inserção.

E7 Ambos resumo criptográfico do documento eletrônico assinado digitalmente e identificador do bloco da AC (que registra o certificado digital de uso único criado pela AC) são registrados em um novo bloco na Blockchain.

E8 Busca na Blockchain por um bloco do que contém o resumo criptográfico do documento eletrônico assinado digitalmente. Se o bloco existir, terá sido criado por um SAD.

E9 O bloco registrado na Blockchain pelo SAD tem duas informações: o resumo criptográfico do documento eletrônico assinado digitalmente e o identificador do bloco da AC.

E10 A identidade do SAD, AC e IDP podem ser implementadas de diferentes formas. Uma maneira é utilizando certificado x509.

E11 Busca na Blockchain pelo bloco cujo identificador é igual ao identificador do bloco da AC.

E12 O bloco registrado na Blockchain pela AC contém duas informações: o resumo criptográfico do certificado digital de uso único utilizado para assinar o documento eletrônico e o identificador do bloco do IDP.

E13 ACs confiáveis são consultadas em listas de serviços confiáveis.

E14 Confecção de um artefato enviado ao usuário contendo uma prova irrefutável de que o verificador verificou com sucesso o status de uma

assinatura em um documento. Este artefato é assinado digitalmente pelo verificador, incluindo obrigatoriamente a data e hora da verificação.

E15 IDPs confiáveis são consultadas em listas de serviços confiáveis

E16 SADs confiáveis são consultados em listas de serviços confiáveis

REIVINDICAÇÕES

1. Processo de assinatura digital remota de documentos eletrônicos **caracterizado** pelo fato de compreender cinco entidades: o usuário, um provedor de identidade (IDP), um Serviço de Assinatura Digital de documentos eletrônicos (SAD), uma Autoridade Certificadora (AC) e uma *blockchain*, em que, numa primeira etapa, o usuário acessa o SAD e faz o upload do documento a ser assinado, sendo que o SAD calcula o resumo criptográfico do documento a ser assinado; numa segunda etapa, o SAD encaminha para o IDP o resumo criptográfico do documento a ser assinado e solicita a autenticação do usuário juntamente com a requisição de acessar atributos do usuário; numa terceira etapa o SAD gera um par de chaves para assinar o documento digitalmente, enviando o resumo criptográfico do documento a ser assinado, a chave pública, os atributos do usuário e o identificador do bloco do IDP para a AC; numa quarta etapa a autoridade certificadora emite um certificado digital de uso único contendo o resumo criptográfico do documento a ser assinado, a chave pública, e os atributos do usuário; e uma quinta etapa em que o certificado digital de uso único e o identificador do bloco da AC são retornados para o SAD, que utiliza o certificado para realizar a assinatura digital juntamente com a chave privada e imediatamente descarta a chave privada e o certificado, sendo que o SAD calcula o resumo criptográfico do documento eletrônico assinado digitalmente, e o insere na *blockchain* juntamente com o identificador do bloco da AC, sendo que o novo bloco possui um identificador único e o documento eletrônico assinado digitalmente com o certificado digital de uso único é retornado para o usuário.

2. Processo, de acordo com a reivindicação 1, **caracterizado** pelo fato de que, na segunda etapa, no portal do IDP, o usuário se autentica usando os fatores de autenticação previamente cadastrados e o IDP, então, solicita autorização do usuário para compartilhar o conjunto de dados solicitados pelo SAD. Ao aceitar compartilhar os atributos, um bloco é salvo na blockchain pelo IDP contendo o resumo criptográfico

do documento a ser assinado, sendo que o bloco inserido na *blockchain* possui um identificador único, doravante chamado de identificador do bloco do IDP, e é enviado para o SAD junto com os atributos do usuário.

3. Processo, de acordo com qualquer uma das reivindicações 1 ou 2, **caracterizado** pelo fato de que, na quarta etapa, o certificado digital de uso único tem prazo de validade igual da AC que o emitiu e o certificado digital de uso único é livre de um *link* para uma lista de certificados revogados, e a AC calcula o resumo criptográfico do certificado digital de uso único e o insere em um bloco na *blockchain* juntamente com o identificador do bloco do IDP, este novo bloco possuindo um identificador único.

4. Processo de verificação de assinaturas digitais **caracterizado** pelo fato de que envolve duas entidades: o verificador e a *blockchain*, compreendendo as estas de: numa primeira etapa, o verificador recebe um documento eletrônico assinado digitalmente, extraindo o certificado digital de uso único, a assinatura digital e o documento eletrônico; uma segunda etapa em que a chave pública, a assinatura digital e o resumo criptográfico do documento eletrônico calculado são submetidos a uma função de criptografia que testa se a assinatura digital é válida; uma terceira etapa em que uma busca é realizada na *blockchain* pelo resumo criptográfico do documento eletrônico assinado digitalmente; uma quarta etapa em que uma busca é realizada na *blockchain* pelo bloco da AC através do identificador do bloco da AC; uma quinta etapa em que uma busca é realizada na *blockchain* pelo bloco do IDP através do identificador do bloco do IDP obtido na etapa anterior e uma sexta etapa em que é verificado se a AC é confiável, a verificação usando como base a lista de ACs confiáveis.

5. Processo, de acordo com a reivindicação 4, **caracterizado** pelo fato de que na primeira etapa também é calculado o resumo criptográfico do documento eletrônico assinado digitalmente, o resumo criptográfico do certificado digital de uso único, e o

resumo criptográfico do documento eletrônico e de que são extraídos do certificado digital de uso único a chave pública e o resumo criptográfico do documento eletrônico.

6. Processo, de acordo com qualquer uma das reivindicações 4 ou 5, **caracterizado** pelo fato de que, na quarta etapa, o resumo criptográfico do certificado digital de uso único extraído do bloco da AC é comparado com o resumo criptográfico do certificado digital de uso único extraído do documento eletrônico assinado digitalmente no início do processo.

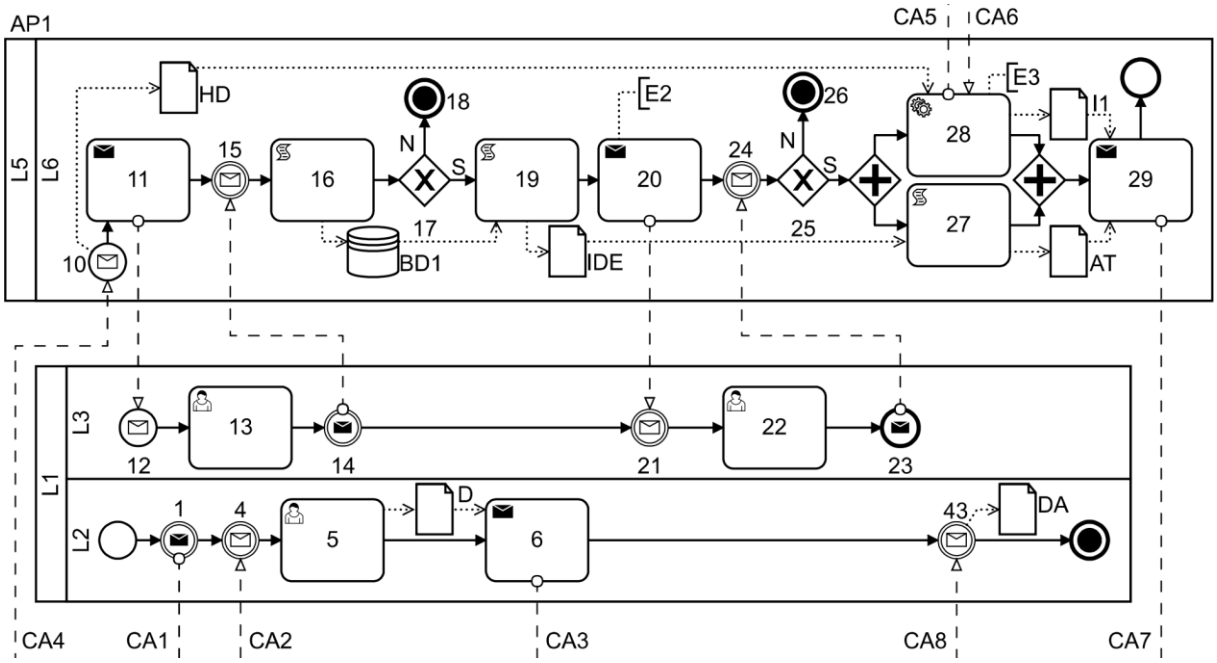


FIGURA 1

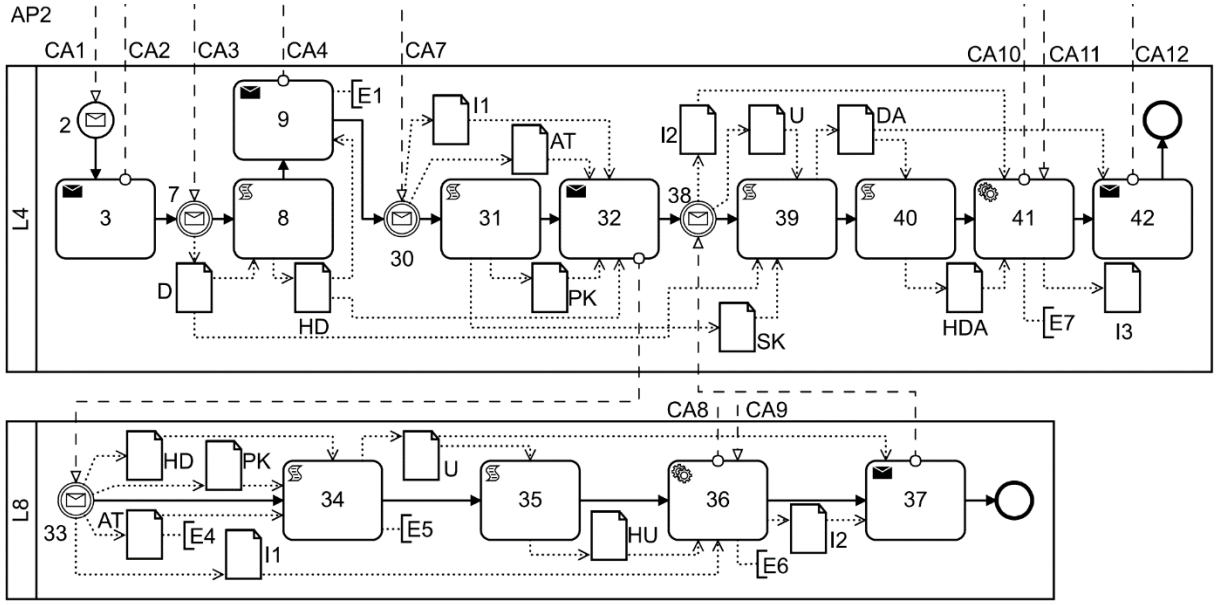


FIGURA 2

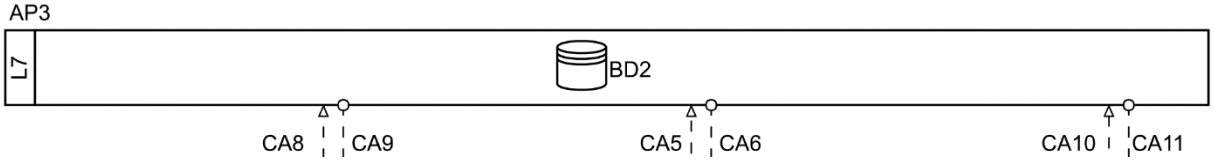


FIGURA 3

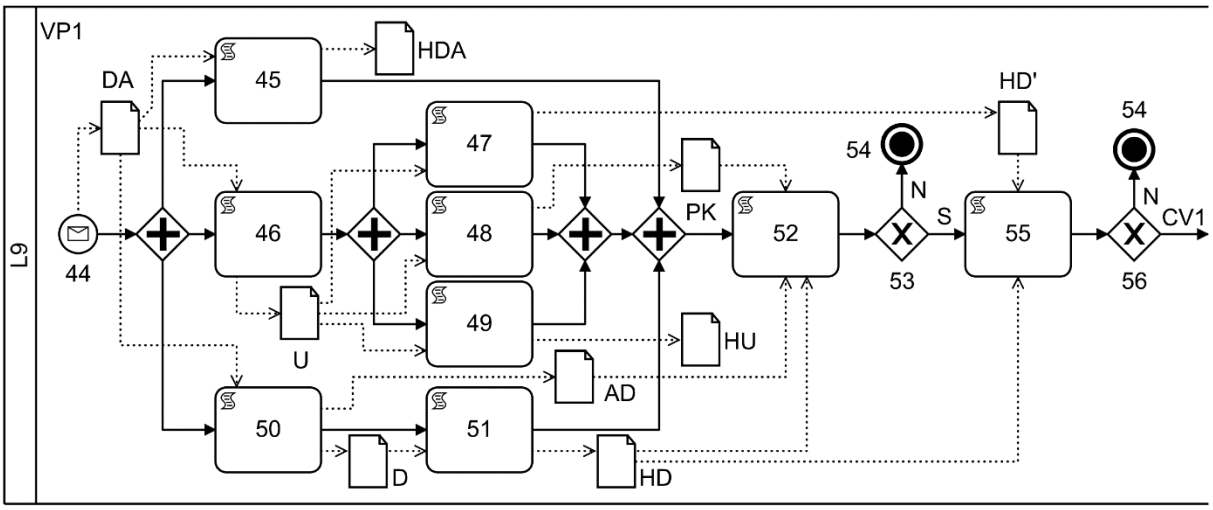


FIGURA 4

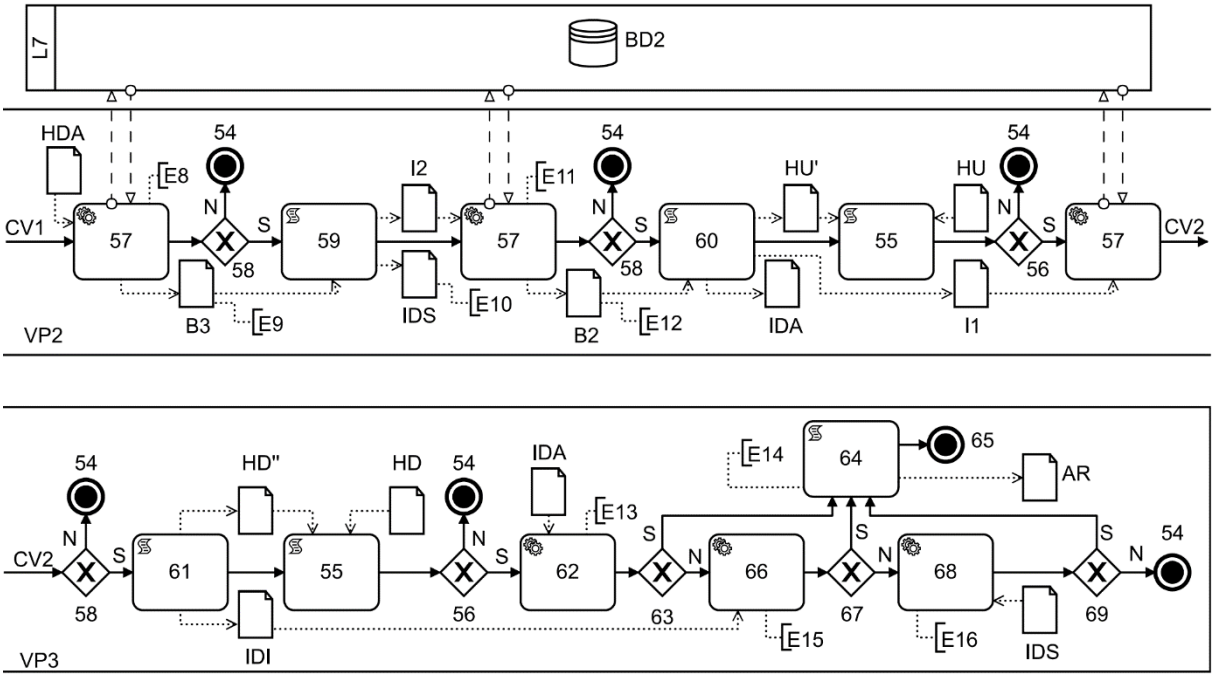


FIGURA 5

RESUMO

“PROCESSO PARA ASSINATURA E VERIFICAÇÃO DE ASSINATURA DIGITAL”

A presente invenção se refere a um novo processo para assinar digitalmente documentos digitais (exemplo, um texto feito em um editor de texto e salvo no formato PDF). A assinatura digital atualmente pode ser realizada de diversas formas, a mais amplamente aceita é através de um certificado digital (exemplo eCNPJ). A assinatura digital é análoga a assinatura física (a próprio punho) de um documento físico. O diferencial em relação ao estado da técnica é a criação do conceito de certificado de uso único. Através dele, um documento é associado ao certificado e este certificado não pode ser utilizado para nada a não ser assinar digitalmente este documento específico. Outro diferencial é associar a validade de uma assinatura a existência de três registros em uma *blockchain*, um para cada entidade envolvida na assinatura (IDP, SAD e AC). Desta forma, só é possível fraudar uma assinatura se as três entidades forem corrompidas, com incremento da segurança da assinatura.