



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

(11) PI 0312774-5 B1

(22) Data do Depósito: 17/07/2003

(45) Data de Concessão: 06/02/2018



(54) Título: "MÉTODO DE PROVER UM SERVIÇO DE ESTADO DE CERTIFICADO ("CSS") PARA CONFERIR VALIDADES DE CERTIFICADOS DE AUTENTICAÇÃO EMITIDOS POR RESPECTIVAS AUTORIDADES DE CERTIFICAÇÃO ("CA")"

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

(52) CPC: H04L 9/3268, H04L 9/3247

(30) Prioridade Unionista: 16/07/2003 US 10/620,817, 18/07/2002 US 60/397,178

(73) Titular(es): EORIGINAL, INC.

(72) Inventor(es): STEPHEN F. BISBEE; JACK J. MOSKOWITZ; KEITH F. BECKER; WALTER J. HILTON; JOSHUA D. SZEKENYI

“MÉTODO DE PROVER UM SERVIÇO DE ESTADO DE CERTIFICADO (“CSS”) PARA CONFERIR VALIDADES DE CERTIFICADOS DE AUTENTICAÇÃO EMITIDOS POR RESPECTIVAS AUTORIDADES DE CERTIFICAÇÃO (“CA”)”

FUNDAMENTOS

[001] A invenção dos Solicitantes refere-se a sistemas e métodos para prover uma cadeia verificável de evidência e segurança para a criação, execução, manutenção, transferência recuperação e destruição de objetos de informação original eletrônicos, como documentos Electronic Original™.

[002] Esta invenção usa, vantajosamente, o Utilitário de Custódia Confiável dos Solicitantes, que contem registros originais eletrônicos e funções de sistema comparáveis como um cofre eletrônico virtual na validação do direito de um indivíduo efetuar uma ação obrigatória, a autenticidade de objetos de informação eletrônicos submetidos, e o status dos certificados de autenticação usados nos processos de verificação de assinatura digital e de autenticação de usuário. Tais TCUs e operações estão descritos nas patentes US 5.615.268; 5.748.738; 6.237.096 e 6.367.013.

[003] A lista a seguir de abreviações é usada nesta descrição:

Abreviações

CA	Autoridade de Certificação
CRL	Lista de Anulação de Certificado
CSS	Serviço de Status de Certificado
HTML	Linguagem de Marcação de Hipertexto
ID	Identificação
IETF	Força-Tarefa de Engenharia da Internet
ITU	União Internacional de Telecomunicações
LDAP	Protocolo Rápido de Acesso a Diretório
OCSP	Protocolo de Status On-Line, IETF-RFC 2560 X.509 Protocolo de Status On-Line de Infra-estrutura de Senha Pública – OCSP,

Junho, 1999

PIN	Número de Identificação Pessoal
PKCS	Normas Criptográficas de Senha Pública
PKI	Infra-estrutura de Senha Pública
PKIX	Infra-estrutura de Senha Pública (X.509)
S/MIME	Extensões Seguras de Correio Internet de Múltiplas Finalidades
SCVP	Protocolo Simples de Validação de Certificado, Rascunho-IETF-PKIX-SCVP-06, Julho, 2000
SSL	Utilidade de Custódia Confiável
UETA	Aro de Transações Eletrônicas Uniformes
XML	Linguagem de Marcação Extensível

[004] A legislação US de Assinaturas Eletrônicas no Aro de Comércio Global e Nacional (ESIGN) e leis estaduais US modeladas após a UETA esboçada pela Conferência Nacional de Comissários de Leis Estatais Uniformes e aprovadas e recomendadas para decretação em 1999, provêm garantias de representação legal para objetos de informação assinados eletronicamente (documentos eletrônicos) que geraram atividade governamental, bancária e de comércio eletrônico visando a concretização de eficiência e economia destas transações potencialmente totalmente eletrônicas.

[005] PKI e a CA são os elementos básicos de tecnologia de assinatura digital usados na criação de registros de fonte eletrônica. Uma PKI é uma coleção de CAs onde a confiança é estabelecida entre usuários e organizações de usuários pela criação de uma relação hierárquica entre CAs ou através de certificação cruzada entre CAs cooperantes. Uma CA tem o poder de emitir certificados de autenticação que associa uma identidade de indivíduo ou de entidade a sua senha pública (verificadora), onde apenas o indivíduo recebe acesso à senha privada casada (assinatura). No momento deste relatório, os certificados normalmente são conformados à norma de

certificado ITU X.509 e são eles mesmos digitalmente assinados pela CA emissora. Estes certificados estão ilustrados na Fig. 10 da patente US 6.237.096, por exemplo, citada e incorporada acima. Estes certificados de autenticação contêm um número de série, informação de identificação do sujeito (usuário) e emissor (CA), o período de validade do certificado (data e hora antes e depois das quais ele não pode ser usado), a senha pública do sujeito, e informação de algoritmo criptográfico necessária para criar e verificar assinaturas digitais.

[006] Para criar uma assinatura digital, um objeto de informação passa por hash (processado usando-se uma função criptográfica de sentido único que pode detectar uma alteração tão pequena quanto um bit no objeto) e o hash é então criptografado usando-se a senha privada (secreta) do indivíduo. A verificação de assinatura digital é obtida invertendo-se este processo. A assinatura digital é descriptografada pelo uso da senha pública do indivíduo recuperada de seu certificado de autenticação e o resultado é comparado com um re-hash do objeto de informação original. Estes processos podem variar quando se usa diferentes algoritmos de assinatura digital. Assinaturas digitais são tão confiáveis quanto a confiança que existe entre as partes dependentes e as CAs emissoras; e o nível de garantia obtido pelos controles físicos, práticas e procedimentos implementados pelas CAs.

[007] A finalidade da tecnologia PKI é criar e manter um ambiente tanto seguro como confiável para partes em comunicação. Estas partes dependem da PKI para estabelecer a identidade de usuários e notificá-los quando um certificado de usuário não é mais viável. Certificados são anulados quando um indivíduo deixa uma organização, quando um certificado substituto é emitido, ou quando uma senha de assinatura é perdida, furtada ou cedida. Vendedores reportam o status do certificado usando uma ampla variedade de métodos. Estes diversos métodos tornam mais difícil os usuários obterem status de certificado para outros usos.

[008] A formação de relação de confiança e interoperabilidade é ditada pelo certificado PKI e políticas de segurança e aplicação das mesmas. A política de certificado determina o nível de checagem pessoal (ou seja, o processo para validar a lisura da informação de solicitação de certificado e a identidade do recipiente do certificado pretendido) necessário (por exemplo, dois formulários de foto de ID, cheque de crédito) para obter aprovação para emissão de um certificado. A política de segurança dita os controles físicos, de procedimentos e processual necessários para suportar o ambiente de aplicação.

[009] Há dois modelos prevalentes para criar e organizar CAs. O primeiro é um modelo hierárquico de CA que se assemelha a uma árvore invertida cuja copa é a CA de raiz. A CA de raiz assina seus certificados de CA imediatamente subordinados. Estas CAs assinam então seus certificados de CA subordinados, e assim por diante. Estas relações criam cadeias de certificados que formam galhos da árvore. Duas CAs provam que uma relação de confiança existe entre elas por “acompanharem” suas respectivas cadeias de certificados até que um nó comum seja alcançado. As CAs podem ser agrupadas e associadas a um ou mais canais de despacho de serviço, verticais de indústria, organizações ou empresas.

[0010] No segundo modelo, uma CA é criada para uma única empresa e provê serviços de CA a uma ou mais entidades dentro desta empresa. Uma CA de empresa não tem, normalmente, nenhuma relação de confiança pré-estabelecida com qualquer CA ou uma outra empresa. Ação explícita tem que ser tomada para permitir interoperabilidade em forma de certificação cruzada de CA, por meio do que duas ou mais CAs que concordam em confiar uma na outra assinam o certificado uma da outra e usam estes certificados de certificação cruzada durante verificação de assinatura digital. Certificados emitidos por uma CA podem então, ser validados pela outra CA de certificação cruzada e seus usuários.

[0011] CAs anulam certificados quando, entre outras razões, a informação contida nos mesmos se tornam inválidas, quando a senha privada do usuário se torna comprometida, ou quando é necessário terminar privilégios de aplicação baseados em certificado de usuário. As CAs não podem simplesmente apagar ou recuperar um certificado de seu proprietário se ele já estiver de posse de seu proprietário. Em vez disso, o certificado é marcado como “anulado” no banco de dados da CA e o status do certificado é publicado. Usuários da PKI podem, então, conhecer a validade de um certificado solicitando o status do certificado da CA emissora ou repositório (diretório) de status identificado.

[0012] Um método antigo usado para reportar status de certificado era por meio de publicação de uma lista de certificados anulados de uma CA, conhecida como uma CRL. CRLs são baixadas por aplicações e partes confiáveis para determinar se um certificado de usuário particular foi anulado e, por extensão, se esta assinatura digital de usuário é ainda válida ou não. Com o tempo, as CRLs ficam mais longas, incorrendo em sobrecarga de comunicação e processamento de dados. Uma desvantagem adicional desta abordagem é o fato de CRLs serem com frequência, publicadas a intervalos infrequentes (por exemplo, uma ou duas vezes por dia). Por esta razão, as CRLs ficam, muitas vezes, desatualizadas após publicação. Certificados anulados só são removidos das CRLs após a expiração do certificado.

[0013] Uma ponte PKI é um método de prover interoperabilidade entre CAs pela coordenação da distribuição de CRLs. Uma tal ponte é um repositório de CRL central que, com efeito, une um conjunto de CAs que concordam em aceitar certificados e políticas de segurança entre si. Todas as CAs postam suas CRLs na ponte. Isto permite validação centralizada de qualquer certificado de indivíduo ou entidade. Se o certificado não tiver sido anulado previamente, então ele é ainda considerado válido. A maior desvantagem para as pontes PKI é o fato delas terem que ser acessíveis por

qualquer CA ou usuário dependente da ponte para status de certificado. Os requisitos de largura de faixa, computação e armazenamento podem ser dispendiosos.

[0014] Um método mais recente para obter status de certificado é OCSP IEFT, que faz uma indagação direta a banco de dados que possa prover status de certificado em tempo real. Entretanto, alguns vendedores implementaram respondedores de OCSP baseados em CRLs. Status de certificado reportados por este tipo de respondedor é apenas tão conveniente quanto CRL sobre a qual se baseiam. Tentativas de obter status de certificado em tempo real, como SCVP IETF continuam a ser desenvolvidas. No momento desta invenção, a mistura e casamento de métodos de checagem de status não é prática em um ambiente PKI aberto.

[0015] Qualquer abordagem a validação de certificado é uma decisão de tudo ou nada para a CA que emitiu os certificados. Todos os usuários que tenham certificados emitidos por uma das CAs-membro são válidos/habilitados, a não ser que seus certificados tenham sido suspensos ou anulados ou tenham expirado. O tema comum para controlar participação é se um certificado consegue ser emitido. Emissões são governadas por políticas de certificados de segurança e regras comerciais.

[0016] O ambiente de confiança pode variar de totalmente aberto, onde qualquer capaz de pagar o preço de admissão recebe um certificado, fechado ou limitado, exigindo filiação em uma empresa ou comunidade de interesse. Em qualquer caso, o certificado de CA e ou políticas de segurança governam se interoperabilidade é permitida.

[0017] A invenção dos Solicitantes aborda o problema de interoperabilidade de PKI e CA por um ponto de vista totalmente diferente dos acima descritos. O foco dos Solicitantes está no estabelecimento de um ambiente de confiança adequado à criação, execução, manutenção, transferência, recuperação e destruição de objetos de informação original

eletrônicos que possam ser também registros transferíveis (a propriedade pode mudar de mãos). Para concretizar tais objetivos, o sistema controlando um original eletrônico ou cópia autorizada tem que tornar possível identificar o original de qualquer de suas cópias. Como acontece com originais em papel, só pode haver um original. Exemplos de registros transferíveis são instrumentos e cauções eletrônicos negociáveis. Um registro original eletrônico pode ser qualquer registro fonte, seja qualificado como registro transferível ou não. Transferência de registros originais eletrônicos entre sistemas tem que ocorrer usando métodos que garantam a existência apenas de um original.

[0018] Esta invenção cria um registro original eletrônico pela colocação de custódia deste registro nas mãos de uma parte independente confiável, funcionária ou operada por TCU para o benefício do proprietário do registro. Criar um ambiente de confiança é necessário, mas não suficiente para manter registros de fonte eletrônicos. Para os fins desta invenção, um ambiente de confiança é criado pela formação de uma comunidade de interesse que tenha uma afiliação fechada ou limitada e na qual a identidade de membros prospectivos, organizações e seus usuários seja assegurada pelo uso de procedimentos de verificação apropriados que governam a aceitação de admissão à comunidade. Além disso, uma organização, participação, desempenho, e atributos individuais são definidos no momento de inscrição no TCU.. Indivíduos tem que ser identificados com exclusividade para o sistema e em seus certificados de autenticação. Em adição, tem que ser possível remover indivíduos e organizações da comunidade e tornar esta ação conhecida por outros membros da comunidade. Abordagens tradicionais à interoperabilidade de CA não obtêm adequadamente estes objetivos.

[0019] O exame cuidadoso, no mínimo, requer que uma organização e/ou indivíduo seja apresentado por um membro conhecido da comunidade. Adicionalmente, uma classificação como Dun and Bradstreet para

organização ou uma checagem de crédito como Equifax para indivíduos, ou um histórico equivalente de crédito e pagamento, pode ser utilizado para avaliar a aceitabilidade de sócios potenciais de negócio, clientes e fregueses. Tanto a organização de exame cuidadoso como seus usuários apresentados têm que ser considerados dignos de confiança antes da inscrição ao TCU ser permitida. Após uma organização aceitar os termos contratuais definindo a inscrição como membro, seus indivíduos apresentados receberão, cada um, um identificador e senha exclusivos que os habilitarão a acessar o TCU.

[0020] Uma vez que um indivíduo este inscrito em um ou mais TCUs, eles podem ser chamados de participantes de uma transação pelo proprietário desta transação e receber acesso específico a todos ou a um subconjunto identificado de registros de fonte com base em suas identidades, papel e/ou responsabilidade. Para facilitar identificação e autenticação e possibilitar que as transações ocorram de forma totalmente eletrônica, um subconjunto selecionado desta informação de identificação é incluído no certificado de autenticação do participante. O certificado de autenticação une a identidade do usuário com sua senha pública usada para validar assinaturas digitais geradas usando sua senha privada de assinatura casada.

[0021] Um certificado ou apólice de segurança trata das exigências de prova de identidade (por exemplo, duas formas de ID de imagem, cheque de crédito, apresentação pessoal) necessárias antes de um certificado ser emitido. Este certificado será limitado à conta de TCU do usuário caso exigido pela autoridade de assinatura digital. O enlace deverá incluir um subconjunto de elementos de dados de certificado que identificam exclusivamente o usuário (por exemplo, ID de certificado, nome de CA emissora, nome comum de usuário). Uma vez associado a uma conta de usuário, o certificado pode ser usado em conjunto com sua assinatura digital para fornecer a prova de identidade necessária para possibilitar um conjunto de ações autorizadas predeterminado e verificar a assinatura digital do usuário em objetos de

informação submetidos. Isto é particularmente verdade quando o proprietário ou agente de proprietário controlando um conjunto de registros eletrônicos instrui o TCU a transferir a propriedade (ou seja, uma transação interna) e/ou transferir a custódia (ou seja, uma transação externa) dos registros eletrônicos para um outro TCU.

[0022] Como descrito anteriormente, certificados de autenticação e criptografia de senha pública são usados para suportar tanto autenticação de usuário como verificação de assinatura digital. O certificado é assinado digitalmente pela CA emissora, um processo pelo qual a identidade do recipiente é selada com sua senha pública. A CA expressa, na emissão de um certificado, que o indivíduo identificado no certificado é o portador da senha privada casada usada para assinar digitalmente objetos de informação ou fragmentos dos mesmos.

[0023] Esta invenção difere de outras soluções de comércio eletrônico (e-commerce) baseado em PKI, uma vez que a PKI só é vista como habilitadora e não é a única base do ambiente confiável. Patrocínio, contratação de adesão, e inscrição são os fatores principais. Embora o certificado e uso de criptografia de senha pública sejam vistos como tecnologia de habilitação, certificados devem exclusivamente identificar e estar ligados aos usuários específicos antes deles poderem ser restritos a esta conta TCU de usuário.

[0024] Quando os certificados são empregados, a conta só pode ser ativada uma vez que esta união entre certificado e conta de usuário esteja completada. Esta união pode ser tão simples como adicionar a ID de Certificado e emitir CA para informação de conta de usuário ou pode usar outra informação conduzida pelo certificado, como componentes do nome distinguido de usuário (ver norma ITU X.509). A informação de união pode ser conduzida em um formulário de inscrição ou extraída diretamente do certificado, como pela política de segurança de sistema TCU. Uma

conferência de correspondência pode ser usada para assegurar que a descrição de usuário no certificado case com a de dados de inscrição sempre que o certificado for usado. O certificado de usuário é assinado pelo CA emissor e sua integridade e autenticidade são validadas pelo uso de certificado de CA emissor e senha pública. O conjunto coletivo de componentes usados para identificação tem que ser provadamente exclusivo. Uma vez que esta união de conta TCU e certificado de usuário esteja completa, o TCU só precisa saber aonde ir para conferir o status do certificado. Em ambientes centrados em CA, uma única PKI, certificação cruzada, ou criação de pontes de PKI (um sistema complexo que efetua conferência de status de certificado quando produtos de múltiplos vendedores são usados por numerosas CAs) é necessária para interoperabilidade. O elemento comum é o fato de todos os certificados terem o mesmo valor. Certificados podem conduzir diferentes níveis de confiabilidade e aplicações em um ambiente aberto têm que ter a capacidade de interpretar e usar estes níveis de confiabilidade de modo diferente. Esta filosofia pode ser caracterizada como “construiremos estradas que levarão você a qualquer lugar desejado”. Usuários são verificados quando de inscrição em CA usando uma variedade de critérios (por exemplo, conferência de crédito, meios de pagamento, custo do certificado).

[0025] Um TCU, inversamente, refere-se unicamente a um conhecido conjunto de “CAs aprovadas” e, dentro deste conjunto, apenas aqueles certificados que estão associados a contas de seus usuários. Qualquer outro certificado será ignorado. Esta filosofia pode ser caracterizada como “as únicas estradas que estarão abertas para você serão aquelas necessárias para conduzir seu negócio”. Usuários são verificados duas vezes, uma para satisfazer a política de certificado de CA e uma segunda vez para provar que a uma necessidade de negócio para eles de serem inscritas com um TCU. Regras de negócios obrigadas pelo TCU podem acomodar certificados emitidos em diferentes níveis de confiabilidade.

SUMÁRIO

[0026] Até o momento, todos os serviços de reportar status de certificado usam um único meio de reportar status de certificado, seja ele CRLs, OCSP, LDAP etc. Esta invenção difere pelo fato de possibilitar interoperabilidade com qualquer CA ou PKI para a finalidade de recuperar e reportar status de certificado. Para a maior parte, ela também reduz dependência de conectividade contínua em tempo real entre os sistemas ou TCUs e os elementos de reportagem de status de certificado CA, por criar cache de status de certificado.

[0027] Em um aspecto da invenção do Solicitante, um método de prover um CSS para conferir validades de certificados de autenticação emitidos por respectivas CAs inclui as etapas de identificar informação necessária para recuperar um status de um certificado de autenticação de uma CA emissora que emitiu o certificado de autenticação; configurar um conector baseado na informação identificada para comunicação com a CA emissora; comunicar com a CA emissora de acordo com o conector configurado, e recuperar o status do certificado de autenticação. O CA emissor e o conector são designados através de uma lista de CAs aprovadas em um armazenamento de configuração.

[0028] Uma data e hora local podem ser conferidas quanto a estarem dentro de um período de validade indicado no período de validade do certificado de autenticação. A CA emissora pode ser incluída na lista de CAs aprovadas pela verificação e aprovação da CA emissora de acordo com regras de negócios predeterminadas, e se a CA emissora for verificada e não aprovada, a CA emissora pode ser designada através de uma lista de CAs não-aprovadas no armazenamento de configuração. Verificar e aprovar a CA emissora pode incluir registrar uma representação de um certificado de autenticação acreditado com o CSS e adição de pelo menos a representação, status e elemento de dados sobrevida para uma memória de cache local. Um

conector é, então, configurado para recuperar o status adicionado quando o status do certificado de autenticação acreditado é questionado. Comunicação com CAs emissoras também pode ser feita de acordo com uma sequência de conectores.

[0029] O método pode incluir ainda conferir uma memória cache local quanto ao status, e se o status for encontrado na memória cache local e a data e hora local estiverem dentro do período de validade, recuperar o status da memória cache local. Se o status não for encontrado na memória cache local ou se a data e hora local não estiverem no período de validade, o CSS estabelece uma sessão de comunicação com um componente de reportagem de status de certificado da CA emissora, compor uma solicitação de status de certificado de acordo com o conector configurado, recuperar o status do componente de reportagem de status de certificado, fechar a sessão de comunicação com o componente de reportagem de status de certificado, e adicionar pelo menos a identificação de certificado de autenticação, status, e sobrevida para a memória cache local.

[0030] O status de certificado pode ser indicado por uma CRL e, de acordo com um esquema de publicação da CA emissora, o CSS recupera o CRL de um componente de reportagem de status de certificado listado no armazenamento de configuração, o CSS limpa uma memória cache associada à CA emissora, e o CSS determina o status do certificado de autenticação a partir do CRL e armazena o status na memória cache associada à CA emissora.

[0031] Status de certificado também pode ser indicado por uma Lista de Anulação de Certificado Delta (“CRL”), e pela notificação pela CA emissora de que uma CRL está disponível, o CSS recupera a CRL de um componente de reportagem de status de certificado listado no armazenar de configuração; se a CCRL for uma CRL completa, então o CSS limpa uma memória cache associada à CA emissora, determina o status da CRL, e

armazena o status na memória cache.

[0032] Em um outro aspecto da invenção do Solicitante, um método de recuperar um status de um certificado de autenticação emitido por uma CA emissora em resposta a uma indagação de uma TCU para um CSS para validar o status de certificado de autenticação inclui as etapas de localizar e reportar o status, caso o status esteja presente e corrente em uma memória cache do CSS; e, de outro modo, efetuar as etapas de obter um tipo de status e método de recuperação de um armazenamento de configuração de CSS; caso o tipo de status seja CRL e o status não seja encontrado na memória cache, então, reportar o status como válido; caso o tipo de status não seja CRL, então, compor uma solicitação de status de certificado de acordo com o tipo de status; estabelecer uma sessão de comunicação com a CA emissora; recuperar o status de um componente de reportagem de status da CA emissora usando o método de recuperação obtido e terminar a sessão de comunicação; interpretar o status recuperado; associar, com o status recuperado interpretado, um valor de sobrevida representando um período especificado por uma política CSS para o tipo de status; adicionar pelo menos a identificação do certificado de autenticação, status, e valores de sobrevida à memória cache; e reportar o status ao TCU em resposta à indagação.

[0033] Em um outro aspecto ainda da invenção do Solicitante, um CSS para prover indicações de status precisas e oportunamente de certificados de autenticação emitidos pelas CAs emissoras inclui prover um status de um certificado de autenticação indicado por uma CRL quando a CA emissora de certificado usar CRLs para indicar o status. De outro modo, o status indicado por uma memória cache, quando a memória cache incluir um status e um elemento de sobrevida não excedido, é provido. Se o elemento de sobrevida for excedido, o status é apagado da memória cache, e o status é solicitado e recuperado pelo uso de um protocolo de reportagem de status de certificado em tempo real quando o status não estiver na memória cache. Pelo menos a

identificação de certificado, status e elemento de dados de sobrevida são adicionados à memória cache, e o status recuperado é provido.

[0034] Um elemento de dados de contador de uso de status pode ser adicionado à memória cache e incrementado e decrementado toda vez que o status de certificado for conferido. Se o elemento de dados de contador de uso de status passar de um limiar, então o status é provido e a memória cache é apagada com relação ao status. Um elemento de dados acessados por último de status também pode ser adicionado à memória cache, e o elemento de dados últimos acessados de status em conjunto com o elemento de dados de contador de uso de status possibilita a determinação de um nível de atividade do status de certificado.

[0035] Quando uma solicitação é feita ao CSS para recuperar um status de um novo certificado e a memória cache tiver alcançado um limite de tamanho de buffer alocado, o CSS busca na memória cache por um elemento de dado por último acessado indicando uma data mais antiga e apaga a respectiva entrada de memória cache; e o CSS recupera, então, o status solicitado, coloca-o na memória cache, e provê o status solicitado.

[0036] Em um outro aspecto ainda da invenção do Solicitante, um método de executar uma transação entre uma primeira parte e uma segunda parte pela transferência de controle de um objeto de informação autenticado tendo uma trilha de evidência verificável inclui recuperar de um repositório acreditado um objeto de informação autenticado que inclui um primeiro bloco de assinatura digital de uma parte submissora e um primeiro certificado de autenticação relatando pelo menos uma identidade e uma senha criptográfica para a parte submissora, executando o objeto de informação autenticado recuperado pela segunda parte pela inclusão no objeto de informação autenticado recuperado o bloco de assinatura digital da segunda parte, e encaminhar o objeto de informação autenticado recuperado executado a um TCU.

[0037] O TCU verifica as assinaturas digitais e valida os certificados de autenticação associados às assinaturas digitais por, pelo menos, recuperando status dos certificados de autenticação de um CSS. O TCU rejeita um bloco de assinatura digital se a respectiva assinatura digital não for verificada ou o status do respectivo certificado de autenticação estiver expirado ou for anulado, e se pelo menos um bloco de assinatura no objeto de informação não for rejeitado, o TCU anexa o bloco de assinatura digital de TCU e um indicador de data e hora ao objeto de informação e assume controle do objeto em nome da primeira parte.

BREVE DESCRIÇÃO DOS DESENHOS

[0038] As várias características e vantagens da invenção do Solicitante se tornarão aparentes pela leitura desta descrição em conjunto com os desenhos, nos quais:

A Fig. 1 ilustra um processo de validação de objeto de informação eletrônica de TCU que emprega a CSS;

A Fig. 2 ilustra processamento CSS de bastidores por meio do que CRLs e CRLs são adicionadas ao armazenamento de status de certificado;

A Fig. 3 ilustra a criação de cache separado de CRLs analisadas, respostas de OCSP e status derivados de outros métodos de reportagem de status de certificado;

A Fig. 4 ilustra uma sintaxe extensível de um bloco de assinatura contendo os elementos de dados de exemplo onde uma assinatura digital está sendo aplicada a fragmentos de objeto de informação e dados anexados (atributos autenticados);

A Fig. 5 ilustra interação de TCU com um CSS e recuperação de CSS de status de certificado via a Internet de CAs membro e estranha;

A Fig. 6 ilustra um processo de inscrição de usuário de TCU terminando em uma etapa de conferência de status de certificado, onde a validação de assinatura digital demonstra inscrição bem-sucedida;

A Fig. 7 ilustra um processo de inscrição de usuário de TCU, onde uma CA estranha emitiu o certificado de autenticação, terminado em uma etapa de conferência de status de certificado, onde a validação de assinatura digital demonstra inscrição bem-sucedida; e

A Fig. 8 ilustra um exemplo de leasing de automóvel que mostra como um CSS pode ser utilizado no comércio eletrônico.

DESCRIÇÃO DETALHADA

[0039] A conferência de status de certificado é um elemento crítico para um sistema ou aceitação por TCU de qualquer submissão de objeto de informação eletrônico. De modo a que a submissão seja aceita, o status de certificado tem que ser reportado como válido. Indagação por status de certificado normalmente exige que comunicações ocorram entre o TCU e a fonte do status de certificado. A frequência destas comunicações crescerá proporcionalmente ao número de submissões a TCU.

[0040] A conferência de status de certificado pode ser um requisito em tempo real e indagações de status são efetuadas a cada submissão. Entretanto, status pode não ser atualizado em tempo real como é o caso com CRLs. Rodas as CRLs são publicadas a intervalos especificados, normalmente uma ou duas vezes ao dia. Recuperação de CRL e análise repetida podem ter um impacto negativo sobre o desempenho do sistema. Esta invenção reduz significativamente os requisitos diretos computacionais e de comunicação pelo descarregamento do grosso do trabalho para um CSS. UM único protocolo de status de certificado é implementado entre o TCU e o CSS. Este protocolo de status pode ter atributos similares ao OCSP IETF que permite uma aplicação indagar uma CA pelo status de um único certificado e, assim, minimizar sobrecarga de processamento.

[0041] O CSS é provido e mantém suficiente informação sobre a localização, os meios de comunicação e status de certificado de processamento para cada CA necessária para ser interoperada. O CSS, desse

modo, torna possível estabilizar e otimizar o projeto de aplicação. O CSS, vantajosamente, analisa e faz cache de status de certificado para minimizar tempo de resposta de status a uma indagação de status por TCU. O CSS, por conseguinte, elimina a necessidade de qualquer uma das formas tradicionais de interoperabilidade de PKI. Recuperação de acordo potencial é grandemente realçada, uma vez que uma conta de usuário de TCU pode ser facilmente desativada ou um conjunto de usuários eliminado pela remoção da CA da lista de CSS de CAs aprovadas.

Uso de certificados de autenticação:

[0042] Após registro no TCU, um participante pode ser solicitado para se autenticar adicionalmente através do uso de criptografia de senha pública e seu certificado de autenticação. Esta autenticação pode ser associada a estabelecimento de sessão segura, solicitações por serviços de TCU ou assinatura digital e submissão de um objeto de informação eletrônico.

[0043] Antes de alguém poder interagir com um TCU, quatro condições devem ser satisfeitas: 1) Precisam, primeiro ser inscritas como um usuário do sistema; 2) devem ter recebido e estar de posse de um par de chaves públicas e seu certificado de autenticação casado se tiverem recebido mais do que acesso só para leitura; 3) certificados devem ser emitidos por uma CA aprovada; e 4) o certificado de usuário não deve ter expirado ou ser reportado como inativo ou anulado. Esta última condição exige, normalmente, que o TCU dirija uma indagação à CA emissora para recuperar status de certificado. Devido à existência de uma grande variedade de normas e implementações de CA para reportar status de certificado, esta não é uma tarefa simples ou fácil.

[0044] Como mencionado na seção anterior, normalmente alguma forma de interoperabilidade de PKI é necessária quando múltiplas CAs ou PKIs estão envolvidas. Esta invenção elimina esta necessidade pela criação de um Serviço de Status de Certificado Cerificação cruzada ou ponte de CA é

desnecessária uma vez que o único conhecimento necessário pelo CSS é a lista de CAs emissoras aprovadas, seus endereços de IP ou similar, e seus meios de reportar status de certificado.

[0045] Para recuperar status de certificado, um conector ou módulo de programa é definido para cada método de status de certificado. Cada certificado de autenticação contém ambos os campos de objeto (usuário) e emissor (CA). O campo de emissor é usado para direcionar uma indagação de TCU ao CSS que, então, confere seu cache quanto à presença do status de certificado. SE o status estiver presente no cache de CSS, ele é retornado para o TCU. SE o status não estiver presente, o CSS invocará o conector apropriado para recuperar o status de certificado. Qualquer número de métodos será usado para reportar e recuperar status de certificado: LDAP, OCSP, CRL etc.

[0046] Para efetuar qualquer ação de TCU, o usuário tem, primeiro, que se registrar em um TCU. Uma vez feito isso, o usuário pode criar ou selecionar uma transação, se lhe for concedida uma tal autorização. Se obtiver permissão para submeter objetos de informação eletrônica, ele pode fazer isso agora. Ao receber um objeto de informação eletrônica, o TCU efetua as necessárias etapas e validação de assinatura digital. Uma indagação de status de certificado será composta e enviada à CSS. SE um status válido for retornado, o TCU aceitará e armazenará a submissão como a cópia de autorização, caso contrário, ela será rejeitada.

Processamento de assinatura digital e conferência de status de certificado:

[0047] Assinaturas digitais podem ser aplicadas a um ou mais fragmentos ou ao conteúdo total de um objeto de informação. Assinaturas digitais podem pertencer às partes relativas à transação ou aos agentes que possibilitam que a transação obtenha um estado ou status dentro do contexto de um processo de negócios. Assinaturas digitais podem de fato, ser aplicadas à informação adicional relativa à tarefa sendo executada. Um tal exemplo

poderia ser a notação em registro local de um certificado de propriedade. Um outro exemplo poderia ser a aplicação da assinatura da parte atestando a autenticidade dos objetos de informação sendo submetidos a um TCU. Neste último caso, o submissor é solicitado a envelopar ou selar o objeto de informação pelo fato de sua assinatura digital ser aplicada a todo o conteúdo, impedindo qualquer modificação posterior.

[0048] Sempre que uma assinatura digital é aplicada, o assinante será solicitado afirmar sua intenção de estar obrigado por sua assinatura digital. Esta ação de validação exigida pela legislação recente, pode assumir a forma de texto legível em uma janela de exibição ou tela de logo, e pode exigir a invocação de um botão gráfico e/ou registro de entrada a um objeto de dados criptográfico que é também uma chave criptográfica e armazenamento de certificado. A demonstração real da mencionada concordância de validação é expressa pelo uso de uma aplicação confiável que computa a assinatura digital do usuário usando o conteúdo selecionado e combina a mesma com seu certificado de autenticação para formar um bloco de assinatura. O bloco de assinatura pode conter também elementos de dados autenticados e não-autenticados. Elementos de dados autenticados são incluídos na computação de assinatura digital (por exemplo, data-hora local) e podem ser considerados protegidos pela assinatura digital (integridade). Elementos de dados não-autenticados são adicionados após a computação de ass e não são protegidos. A Fig. 4 mostra uma sintaxe de amostra que contém os elementos de dados e arranjo de um bloco de assinatura. Ela não deve ser interpretada literalmente, uma vez que tem a intenção de ser um exemplo ilustrativo.

[0049] O objeto de informação e qualquer bloco de assinatura podem ser, vantajosamente, colocados em um envelope (S/MIME) ou em etiquetas em uma sintaxe de informação extensível (XML, HTML, XHTML) para conveniência de manuseio e para facilitar processamento de informação. Esta estrutura de dados é, então, enviada ao TCU para validação. Inversamente,

o(s) bloco(s) de assinatura pode(m) ser enviado(s) independentemente ao TCU para serem afixados ao registro de fonte real que nunca sai do TCU. No último caso, cada bloco de assinatura é validado separadamente.

[0050] O processo para validação de assinatura digital difere, no momento de submissão, daquele efetuado em seguida. Uma validação em quatro etapas é efetuada na primeira vez que o TCU vê uma assinatura digital: 1) verifica a assinatura digital, um processo que prova que o conteúdo protegido pela assinatura digital não foi alterado durante a transmissão; 2) confere se a hora de TCU corrente está dentro do período de validade permitido do certificado de autenticação do indivíduo (“nem antes”, “nem depois”); 3) solicita e recupera status de certificado de CA, emissor, CRL, ponto de distribuição, ou outra fonte aprovada de status de certificado usando a CSS alocada localmente; 4) valida que a informação sobre conta do usuário de TCU concorda com a conduzida pelo certificado e que a ação solicitada está autorizada no banco de dados de regras do TCU. Para um submissor do objeto de informação, o processo adiciona uma etapa ainda. Esta quinta etapa confere se a identidade do submissor casa com a da parte que estabeleceu a corrente sessão com o TCU. SE todos os testes forem bem-sucedidos, a ação é permitida e/ou o objeto de informação é aceito e mantido pelo TCU em nome de seu proprietário. SE alguma etapa falhar, o remédio é iniciado.

[0051] Após esta conferência de status de certificado inicial, o ambiente confiável do TCU mantém a autenticidade e integridade de todos os objetos de informação mantidos. Não é antecipado que alguma conferência de status de certificado adicional seja necessária, a não ser que uma nova versão do documento seja submetida.

[0052] Dois aspectos da invenção diferem do curso normal de implementação de PKI. O primeiro, é o fato desta invenção ser baseada na existência de uma solicitação, ou seja, o TCU (ou qualquer solicitação/sistema requerendo validação de status de certificado e sua capacidade de criar e

manter registros eletrônicos de fonte original). O segundo, é o fato de “CA emissor” precisar, apenas, de ser identificada como conformada às políticas governando o ambiente confiável e que nem certificação cruzada de CA, nem ligação por ponte de PKI são necessárias. A justificativa necessária para inclusão de “CA emissora” é uma relação comercial documentada. Durante o processo de inscrição de TCU, uma conta de usuário é criada, a qual referencia informação de certificado específica de usuário que, com efeito, liga a conta de usuário ao certificado de autenticação do usuário.

Uso de TCU:

[0053] Tipicamente, uma vez que uma organização concorde em utilizar os serviços de um TCU, controle sobre acesso a transações desta organização é garantida a agentes desta organização. Os agentes da organização identificam, então, um conjunto de indivíduos que eles apoiarão na efetuação de ações selecionadas com respeito às transações da organização. Todas as ações exigem que o usuário tenha uma conta com o TCU, que esta conta esteja ativa, e que o usuário tenha uma identidade de registro de entrada e seja capaz de prover uma senha apropriada ou resposta a uma frase indagativa. Em adição, cada transação, que é composta de um conjunto de registros de fonte originais eletrônicas vertidos, tem um conjunto de permissões que governa acesso do usuário a diferentes etapas no processo de negócios. Isto é exemplificado pela concessão e remoção de direitos a registros de transação quando a transação prossegue através do curso normal de negócio, ou seja, abertura através de retenção permanente ou destruição. Caso permitido apenas o registro de entrada ao TCU é necessário para ver um registro de fonte eletrônico. Entretanto, qualquer ação em nível de sistemas ou a introdução ou mudança de um registro de fonte eletrônico requer que o indivíduo se autentique pelo uso de criptografia de chave pública ou pela aplicação de sua assinatura digital certificado de autenticação. Em todos os casos, a identidade do indivíduo tem que ser validada. Quando assinaturas

digitais são empregadas, isto acarreta em: 1) que o usuário tenha permissões de acesso apropriadas, 2) descriptografar a assinatura digital e verificar o conteúdo sobre o qual o hash ou sinopse de mensagem subjacente tenha sido aplicado não foi alterado, 3) conferir se o tempo de submissão está dentro do período de validade do certificado, e 4) conferir se o certificado de usuário ainda é válido.

[0054] Conferência de status de certificado exige que a CA emissora ou um defensor de certificado de autenticação seja indagado. Uma vez que esta etapa tem que ser tomada com cada ação autenticada ou submissão de registro de fonte eletrônico, a largura de faixa de comunicação pode se tornar excessiva e há potencial de retardos, trabalho acumulado, e rejeições devido a respostas de status não respondidas ou lentas. Esta invenção trata desses e de outros aspectos de alta segurança de operação de um TCU e assegura a validade de todas as partes interagindo com o TCU.

[0055] No ambiente altamente seguro no qual p TCU é operado, conferência de status de certificado só é necessário quando um serviço for solicitado por um usuário qualificado. Para objetos de informação, status de certificado só precisa ser conferido no momento da submissão. Se todas as assinaturas digitais forem determinadas como válidas, o objeto de informação é considerado autêntico subsequente. Práticas e métodos de segurança e processuais ficam são disponíveis no TCU para impedir ações maliciosas e falhas de hardware que resultem em alteração ou perda não-autorizada de documento. cada submissão resulta na criação de uma nova versão de m registro de fonte eletrônica. O TCU é obrigado a manter conhecimento da última versão do registro de fonte. Esta versão pode ser identificada como o original eletrônico e como registro transferível. O TCU demonstra sua assunção ao controle de um registro de fonte original pela adição de uma marca de data-hora confiável ao registro de fonte e, então, pela aplicação de sua assinatura digital e anexação de seu certificado. Um envelope pode ser

aplicado ao registro de fonte para conveniência de segurança e processamento. Embora este processo de criação de versão crie um registro de evidência autenticado e custódia, registros separados de auditoria redundante são mantidos para corroboração.

[0056] CSS de solicitantes superam as limitações descritas que persistem atualmente com PKI e comércio eletrônico. Informação de fonte, necessária para obter status de certificado de CAs-membros, é registrada com o CSS quando elas são criadas. Informação de fonte para CAs estranhas aprovadas pode ser entrada durante o processo de inscrição de usuário. Há diversos tipos de fontes de status de certificado e o CSS tem necessidade de ter um conector ou método para cada tipo registrado.

[0057] Um método usado por algumas CAs para conduzir status de certificado é a CRL, que inclui uma lista de certificados anulados e a razão para a anulação dos mesmos, o emissor da CRL, quando esta for assinada pela CA emissora ou um assinante designado para assegurar sua integridade e autenticidade. Certificados são removidos da CRL, uma vez que o período de validade dos mesmos esteja vencido.

[0058] Quando CRLs são usadas, o CSS recupera a última interpretação da CRL do ponto de distribuição de CA, por exemplo, um perfil de CRL X.509 v2 (IETF RFC2459, jan;99), valida sua assinatura, analisa a mesma, e cria um cache para armazenar os resultados. O CSS usa um intervalo de publicação CRL de CA para governar ao efetuar o ‘download’ de CRL seguinte. Cada CRL contém um campo de validade que é normalmente estabelecido para permitir algum espaço para efetuar baixamentos. Isto permite congestão de comunicação e tempo parado de CA e forçará o CSS a exigir ação remediativa se este intervalo for excedido. Este remédio pode incluir revalidar qualquer submissão associada a um certificado de anulação recentemente adicionado. Cada nova CRL substitui a CRL anteriormente carregada. A exceção a esta regra é para procissão de CRLs delta. O conteúdo

de CRL delta é anexado ao contudo de cache corrente. O nº CRLN de base de CRL delta refere-se à mais recente CRL total emitida. CRLs desta são publicadas a intervalos menores (minuto, hora) e somente quando uma anulação de certificação tenha ocorrido desde a última CRL total. O CSS é responsável por recuperar CRLs e CRL delta, com base no intervalo de publicação ou notificação e não excedendo o intervalo estabelecido na política de segurança de TCU.

[0059] Um segundo método usado pelas CAs para distribuir status de certificado é o OCSP. Quando OCSP é usado, o CSS indaga o respondedor de OCSP quando solicitado sobre status de certificado. Respostas de OCSP são assinadas para garantir a integridade e autenticidade das mesmas. O CSS analisa a resposta de OCSP e adiciona detalhes e status de certificado para um outro cache. Uma bandeira de tempo-de-partir, determinada pela política de segurança de TCU local, é incluída e determina quando a entrada deverá ser removida do cache. Esta característica destina-se a minimizar sobrecarga de comunicações quando diversos objetos de informação tiverem que ser tele-transmitidos pela mesma parte/entidade para o TCU em um intervalo curto. A bandeira de tempo-de-partir será, normalmente, significativamente mais curto (por exemplo, 5 minutos) do que o intervalo de publicação de CRL normal (duas vezes ao dia, diariamente). O CSS pode conferir status de certificado novamente, se mais de um objeto de informação tiver sido processado, antes de purgar o status de certificado do cache para assegurar que a anulação de certificado não ocorreu. Se anulação de certificado tiver ocorrido durante o intervalo de tempo-de-partir, então o ponto de contato de organização de proprietário tem que ser notificado. Diversos outros métodos de indagação existem, mas não serão descritos por questão de brevidade. Deve ser entendido que cada um deles exige um conector e, potencialmente, um cache separado quando forem utilizados.

[0060] A Fig. 1 mostra o fluxo de processo para criar um original

eletrônico. Para as finalidades desta descrição, o objeto de informação é assumido ser um contrato de vendas. Uma cópia (não executada) do objeto de informação eletrônico é recuperada do TCU ou de um sistema de preparação de documento e é digital ou holograficamente (manuscrita) assinada por partes apropriadas. Rendo –se uma visão geral do processo de execução, o agente do proprietário usa uma aplicação confiável para assinar digitalmente e envelopa o objeto de informação, enviando-o para um TCU.

[0061] Tendo criado executado ou recuperado previamente o documento eletrônico, um submissor assina digitalmente e submete o mesmo ao TCU, como na etapa 101. Neste processo de selagem eletrônica, um envelope que contém o conteúdo assinado e bloco(s) de assinatura digital que contenham ainda a(s) assinatura(s) digital(is) e certificado(s) do submissor e qualquer outro signatário é formado. Há cinco processos representados na Fig. 1: (1) ação quando assinatura(s) digital(is) e ou certificado(s) anulado(s) são encontrados, (2) conferência de status de certificado quando status é localmente colocado em cache, (3) conferência de status de certificado quando status de certificado tem que ser recuperado, (4) recuperação e processamento de CRL, e (5) criação de um original eletrônico quando o documento eletronicamente selado for determinado como autêntico. Na etapa 103, o TCU recebe o documento eletrônico selado eletronicamente. Na etapa 105, o TCU valida se o submissor tem autoridade para adicionar documento eletrônico a uma conta selecionada e/ou transação. Na etapa 107, o TCU verifica criptograficamente qualquer assinatura digital incluída no documento eletrônico digital eletronicamente envelopado. A chave pública, encontrada no certificado de autenticação X.509 do signatário, é usada durante o processo de verificação. Na etapa 109, o período de validade do certificado é extraído do certificado de autenticação de signatário e, na etapa 111, o período de validade é conferido em relação a data e hora corrente. Se qualquer dos testes mencionados falhar, a submissão é rejeitada na etapa 113 e um

reconhecimento negativo pode ser enviado na etapa 114. A ação é registrada na etapa 117.

[0062] Se um teste for bem-sucedido, então o status de certificado de cada certificado contido no envelope é solicitado por um CSS na etapa 119. Nas etapas 121 e 123, o status de certificado é conferido para ver se ele está presente em um armazenamento de status de certificado. Na etapa 125, o status de certificado é recuperado, e a validade do certificado é conferida na etapa 127. SE qualquer certificado for determinado inválido por qualquer razão, a submissão é rejeitada na etapa 113, um reconhecimento negativo pode ser enviado na etapa 115, e a ação é registrada na etapa 117. O submissor é esperado procurar remédio.

[0063] Se na etapa 127 todas assinaturas digitais e certificados forem determinados como sendo válidos para a submissão, então na etapa 129 o TCU aplica um outro envelope que inclui uma marca de data-hora e bloco de assinatura digital de TCU. O TCU assume, então, o controle da submissão como um registro de original eletrônico em nome do proprietário de registro. Na etapa 131, o TCU coloca o original eletrônico em armazenamento persistente protegido; na etapa 133 o TCU envia um reconhecimento positivo e, na etapa 117, o TCU registra as ações recém completadas.

[0064] Se na etapa 123 for determinado que o status de certificado não está presente no armazenamento de status de certificado, então o CSS, na etapa 135, recupera o campo de CA emissor a partir do certificado sendo testado. Na etapa 137, o CSS confere para ver se a CA emissora está na lista de CAs aprovadas, que pode ser mantida e acessada por um Armazenamento de Conector de CA na etapa 139. Se a CA não estiver listada, então um status inválido é retornado e o processo reiniciado na etapa 125 e prossegue pelas etapas 127, 113, 115 e 117, resultando na rejeição da submissão e transmissão de um reconhecimento negativo e entrada de registro. Se a CA emissora for encontrada na lista de CAs aprovadas na etapa 137 e, na etapa 141 for

determinado que o mecanismo de reportagem de status de certificado é uma CRL, então uma indicação de status válido é retornada para a etapa 125. Se a CA for conhecida e status não estiver presente para o certificado em questão, mas o mecanismo de status for uma CRL, então pode-se supor que o status de certificado é válido, provido que uma CRL existe e é corrente para a CA. O processo prossegue, então, pelas etapas 127, 129, 131 e 117, resultando na criação de um original eletrônico, a transmissão de um reconhecimento positivo, e uma entrada de registro para as ações recém completadas.

[0065] Se na etapa 141 o mecanismo de reportagem de status de certificado for determinado como não sendo uma CRL, então a informação de conector obtida na etapa 137 é usada para indagar o mecanismo de reportagem de status de certificado, contida na descrição de conector está toda informação de configuração necessária para indagar o repositório apropriado de status de certificado, seja ele uma CA, um diretório, ou qualquer outro tipo de repositório de status de certificado. Os armazenamentos de status associados às etapas 145, 147, 149 e 151 (ou seja, respectivamente, um diretório LDAP, um respondedor OCSP, um banco de dados, e um servidor) são exemplos de tais repositórios. Em resposta a uma indagação na etapa 143, um destes responde com informação de status de certificado, e o status é adicionado ao armazenamento de status de certificado na etapa 153.

[0066] Pela adição na etapa 153, o processo interno de armazenamento de status de certificado reinicia na etapa 121 e continua pelas etapas 123, 125 e 127 até uma conclusão na qual a submissão é aceita (etapas 129, 131, 133, 117) ou rejeitada (etapas 113, 115, 117).

[0067] CRLs são publicadas na etapa 155 a intervalos predeterminados e, na etapa 157, conforme necessário quando um acordo suspeito é reportado e a política requer uma imediata resposta. Este processo está descrito adicionalmente na Fig. 2.

[0068] SE a CA for conhecida e status não estiver presente, e o

mecanismo de status não for que não a CRL, O Serviço de Status de Certificado seleciona um conector e indaga o mecanismo de status de certificado (etapa 143). O conector contém a informação necessária que torna possível a recuperação e interpretação de status. Qualquer das fontes de status de certificado em tempo real ilustrada nas etapas 145-151 responderá a uma indagação de status de certificado com o status corrente, mas este processo não está limitado apenas a estas fontes. Status é recebido e adicionado ao Armazenamento de Status de Certificado na etapa 153. Quando status é adicionado, uma resposta é gerada e ação retornada para a etapa 123, com o processamento de status reiniciando na etapa 125 e se completando conforme descrito previamente.

[0069] Com referência agora à Fig. 2, o CSS efetua recuperação de CRL como um processo em segundo plano. Uma CRL contém uma lista de todos os certificados anulados ou suspensos até que data e hora correntes estejam além do período de validade contido no certificado. Certificados suspensos são tratados como se tivessem sido anulados, mas eles podem ser retornados a um estado anterior, resultando em sua remoção da CRL. Certificados anulados não podem ser recuperados.

[0070] Na etapa 155, um Administrador de CA configura a CA para publicar CRLs a intervalos predeterminados. Na etapa 157, o Administrador de CA também pode publicar uma CRL Delta conforme ditado pela política de certificado ou segurança local. O Administrador de CA ou CA encaminhará notícia sobre publicação de uma CRL Delta. Uma CRL Delta pode ser gerada sempre que um certificado for anulado ou suspenso durante o intervalo entre publicações de CRLs totais. CRLs Delta podem conter uma lista completa de CRLs anuladas. Na etapa 201, as CRLs e CRLs Delta são publicadas para um repositório ou diretório de CRL.

[0071] Na etapa 203, a CSS recupera o esquema de publicação de CRL ou notícia de CRL Delta, e a etapa 205 representa um cronômetro usado

para recuperação programada. O cronômetro também permite recuperação baseada no campo “atualização seguinte” contido em todas as CRLs. Na etapa 207, a CRL ou CRL delta é recuperada do repositório de CRL. Na etapa 209, a CRL ou CRL Delta é analisada antes de ser adicionada, na etapa 153, a um cache ou lista apropriado no Armazenamento de Status de Certificado na etapa 121 ou diretório baseado no programa estabelecido ou por notificação. A análise de CRLs permite gerencialmente mais fácil e sobrecarga reduzida em busca de entrada de CRL. As etapas 119, 123, 125, 135, 137 e 141 do CSS estão ilustradas na Fig. 2 para completção, e são implementadas como descrito em relação à Fig. 1.

[0072] Com referência agora à Fig. 3, o Armazenamento de Status de Certificado contém um número de cachês que contém status de certificado de diferentes mecanismos de reportagem. Os cachês (cinco dos quais estão ilustrados na Fig. 3) podem mapear CAs individuais (cachês 301, 303) ou coleções de CAs (caches 307, 309). Para status repostados em tempo real, o status permanece no cache até que espaço seja necessário (por exemplo, menos freqüentemente, usado) ou baseado em uma requisição de política (por exemplo, conter apenas um intervalo de tempo especificado). Status é normalmente purgado uma vez que critério seja excedido.

[0073] A finalidade dos cachês é conter status de certificado por um período ditado pela política, reduzindo, desse modo, sobrecarga de comunicações necessária durante recuperação de status de certificado e de CRL. O CSS, por conseguinte, pode cobrir interrupções de comunicações.

[0074] CRLs podem ser analisadas e status individuais de certificados anulados colocados em um cache para reduzir sobrecarga computacional resultante quando a CRL tiver que ser conferida repetidamente. Isto é ilustrado pelos cachês 305, 307. O conteúdo do cache é substituído sempre que uma nova CRL completa é recuperada.

[0075] Com referência agora à Fig. 4, um exemplo de sintaxe é

mostrado, representando alguns dos mais importantes elementos de dados que precisam ser incluídos em um bloco de assinatura digital. A Fig. 4 é um exemplo de forma livre de elementos de dados que constituem uma assinatura digital na qual a assinatura é aplicada a múltiplos fragmentos de mensagem e uma marca de data/hora. Este exemplo tem a intenção de ser ilustrativo da sintaxe que pode ser suada para um bloco de assinatura digital. Pode ser notado que o elemento de dados <Valor Cumulativo de Hash> é aplicado a ValoresHash de um ou mais fragmentos ou conteúdo total e qualquer Dado Autenticado.

[0076] A Fig. 5 ilustra uma arquitetura de comunicações segura mostrando os blocos construtivos que suportam o Serviço de Status de Certificado. A figura mostra a interação entre três CAs, a CSS, e o TCU. O CSS é, de preferência, colocado localmente ao TCU para garantir alta disponibilidade. Sua finalidade primária é prover o TCU com uma interface comum e assegurar provisão segura e oportuna de informação de status de certificado. Sua finalidade secundária é assegurar um nível ou qualidade garantido de serviço pelo gerenciamento de comunicações e sobrecarga computacional necessário para manutenção de informação de status de certificado.

[0077] Como visto na Fig. 5, o servidor de CSS e o TCU, com um roteador e centro de comunicações adequados, são, vantajosamente, dispostos por trás de um 'firewall' de comunicações. O roteador e centro direcionam informação para o CSS e TCU, conforme apropriado. Algumas destas informações compreende submissões de envelopamento eletrônico dirigidas ao TCU e, como descrito acima através de uma rede como a Internet de uma Aplicação de Cliente de Usuário. São também mostradas comunicações CSS e TCU via OCSP.

[0078] A Fig. 5 mostra também três CAs em diferentes exemplos de ambientes atrás das respectivas 'firewalls' de comunicação. Uma CA de

Empresa poderia compreender um servidor interfaceado com uma CA de Indústria de Leasing envolta pelas linhas tracejadas. Um PKI ou Respondedor Estranho pode compreender um servidor interfaceado com entidades como PKI, CA e respondedor de status de certificado. Um Membro Hierárquico PKI poderia incluir um servidor interfaceado com entidades como uma LDAP V3 para CRLs e status de certificado, uma CA Raiz e CAs para as indústrias de hipoteca e leasing, emprestadores, agentes de fechamento e seguradores de título.

[0079] As Figs. 6 e 7 ilustram o uso de Serviço de Status de Certificado durante o processo de inscrição do usuário (signatário e entidade) para ambas CAs membro e CAs estrangeiras, respectivamente. Uma CA membro é uma acreditada para emitir certificados de usuários. CAs estrangeiras são aquelas operadas por entidades externas e que precisam ser aprovadas antes de seus certificados serem usados em conjunto com atividade de TCU. Autorização de identidade de usuário precisa ser rigorosamente imposta por todas as CAs ou delegada a agentes de organizações. Um requisito adicional é o fato de um certificado de usuário precisar estar diretamente associado ou autorizado para uso com uma ou mais contas de organizações de subscrição antes do TCU poder aceitar acesso deste usuário. Uma vez isto realizado, o TCU aceitará a assinatura digital do usuário e confiará no CSS para validação de status de certificado.

[0080] Na Fig. 6, o processo de inscrição de TCU começa na etapa 601 com a recepção por um administrador/agente de organização de informação de inscrição de usuário de um patrocinador. Na etapa 603, este administrador/agente é encarregado de validar a autoridade do patrocinador para fazer a solicitação. Patrocinadores, geralmente só recebem o controle sobre suas contas. Na etapa 605, o administrador/agente inscreve o usuário com o TCU, estabelecendo uma conta de usuário. Na etapa 607, o administrador/agente pode, então, ceder privilégios de transação ao usuário.

Privilégios de transação podem incluir capacidade de submeter, traduzir, transferir etc originais eletrônicos e outros registros de fonte.

[0081] Na etapa 609, um objeto de dados criptográfico (mecanismo de assinatura digital) é inicializado e, na etapa 611, um par de chaves públicas é gerado sobre o objeto de dados. Na etapa 613, uma solicitação de certificado é criada, e na etapa 615 a solicitação é enviada para a CA de organização. Na etapa 617, o certificador é recuperado e colocado sobre o objeto de dados. Na etapa 619, o certificado é limitado ou associado à conta de TCU do usuário.

[0082] Na etapa 621, a identidade do usuário é validada, por exemplo, por aparecer pessoalmente no administrador/agente da organização que pode pessoalmente validar a identidade do usuário. Normalmente, pelo menos duas formas de identificação seriam necessárias. Uma vez que a participação do usuário é patrocinada, isto pode ser suficiente, exceto para transações de alto valor onde alguém conhecido pelo administrador/agente pode ser solicitado a avalizar a identidade do usuário. Na etapa 623, o usuário é solicitado a assinar a aceitação de um contrato pelo qual o usuário concorda que o uso da assinatura digital do usuário é compulsório. Na etapa 625, o usuário recebe um manual de aplicação de usuário e toda instrução considerada necessária. Nas etapas 627 e 629, o usuário é provido de IDs de registro de entrada, senhas temporárias, e o objeto de dados criptográfico.

[0083] Na etapa 631, o usuário registra-se no sistema e, na etapa 633, submete um documento de teste ao TCU. Na etapa 635, o TCU valida a assinatura digital do usuário e certificado. Na etapa 637, o TCU indaga ao CSS informação de status de certificado. Na etapa 639, o TCU recebe status e prossegue conseqüentemente. Se o status de certificado recebido for válido, a inscrição é completada na etapa 641, e o usuário é capaz de acessar e usar o TCU. Se o status de certificado for inválido, a inscrição termina na etapa 643, e o administrador/agente determina a causa do erro e institui o remédio, que pode envolver repetir algumas ou todas as etapas de processo de inscrição

esboçada. O processo confiável esboçado na Fig. 6 assegura que o inscrito está totalmente habilitado na completção.

[0084] Na Fig. 7, o usuário é permitido usar um objeto de dados criptográfico previamente emitido por uma CA estrangeira se as condições ditadas pela política forem satisfeitas. Como descrito acima, as etapas de inscrição 601 a 607 são seguidas. As etapas de verificação de identidade e de contrato 621 a 627 também são seguidas, como descrito acima. Uma vez que o usuário já tenha um objeto de dados, o processo se desvia do descrito na Fig. 6. Na etapa 701, o usuário coloca o objeto de dados em uma leitora compatível e registra a entrada. Na etapa 703, uma aplicação de administrador recupera o certificado de usuário do objeto de dados. Na etapa 705, a informação de certificado é exibida e a informação de identificação de CA emissora é obtida. A informação de CA é usada na etapa 707 para verificar se a CA está na lista aprovada. Se a CA não estiver na lista aprovada, a informação de CA é provida ao administrador de TCU na etapa 709, e o administrador confere com uma Autoridade de Política de Aplicação, na etapa 711, a permissão para continuar a inscrição. Apenas a Autoridade de Política de Aplicação pode autorizar adicionar uma CA estrangeira à lista aprovada.

[0085] Se a permissão for negada na etapa 713, a inscrição termina na etapa 649, dando ao usuário três opções. Uma é solicitar e usar um objeto de dados emitido por uma CA membro. Uma outra opção é solicitar uma revisão da decisão de rejeição de CA. A terceira opção é solicitar os nomes de CAs estrangeiras aprovadas previamente.

[0086] Se a CA emissora for aprovada, mas não estiver na lista na etapa 713, na etapa 715 o administrador adiciona a informação de CA e conector à lista aprovada, configurando o CSS para recuperar status de certificado da CA.

[0087] Na etapa 619, o certificado de usuário é limitado ou associado à conta de usuário recentemente criada. Como na Fig. 8 e etapas 631 a 639, o

usuário é solicitado a fazer uma submissão experimental ao TCU para validar se a conta foi estabelecida corretamente e se o usuário pode acessar o TCU. Se o CSS retornar status inválido, então o administrador determina a causa do erro e instituir remédio, que pode envolver repetir algumas ou todas as etapas de processo de inscrição descritas acima. A causa mais provável de falha pode estar relacionada aos CSSs serem capazes de obter e recuperar corretamente status de certificado da CA estrangeira.

[0088] O CSS desempenha um papel vital na validação de que o certificado do usuário e CA emissora estão ambos autorizados a acessar um TCU um outro sistema. Se uma CA emissora for removida da lista aprovada e seus dados de configuração de conector apagados, todos os usuários associados têm negado acesso adicional ao TCU. Deve ser entendido que o CSS pode trabalhar com outras aplicações e sistemas que exijam status de certificado, incluindo aplicações e sistemas que exigem interfuncionalidade com múltiplas PKIs e CAs.

[0089] Por exemplo, um outro uso do CSS é prover status a certificados de autenticação confiáveis, incluindo certificados auto-assinados, onde um acordo existe entre o cliente procurando serviços e o portador da aplicação. Uma representação de um certificado confiável (por exemplo, PEM, ID de certificado, assinatura digital aplicada) é colocada em cache pelo CSS, e status é indagado usando um conector de certificado confiável. Isto permite que a aplicação tenha um único meio de status de certificado a despeito de se o certificado foi auto-assinado ou emitido por uma CA. Este método de certificado confiável pode ser usado quando um pequeno número de certificados controlados é usado por uma comunidade, em vez de indagar a CA ou CAs da comunidade. Desse modo, será apreciado que os termos “CA” e “CA emissora”, como usados neste relatório, abrangem um tal emissor aceito de certificados auto-assinados, bem como, CAs convencionais.

[0090] Além disso, o CSS pode usar uma combinação de conectores

para recuperar status de certificado. Pelo menos um conector pode ser “virtual”, como este recém descrito para uso com certificados confiáveis. O CSS invoca conectores em uma seqüência predeterminada, por exemplo, ordenada, até que o status de certificado seja adquirido. Este método possibilita a criação de uma hierarquia de fontes de status (por exemplo, mais confiável para menos confiável).

[0091] A Fig. 8 ilustra um exemplo de leasing de automóvel que mostra como o CSS é utilizado no comércio eletrônico. O revendedor de automóvel ou representante do revendedor, adiante chamado de vendedor por simplicidade, recebeu a emissão de um respectivo certificado de autenticação por uma CA Automotiva que está ilustrada como um computador. O arrendatário do carro, que pode estar presente no vendedor de carros, recebeu a emissão de um respectivo certificado de autenticação por um CA de Banco. Um locador remoto recebeu um respectivo certificado de autenticação por uma CA de Financeira. Alternativamente, o arrendatário e o locador podem ter criado um certificado auto-assinado, que o vendedor registrou com a solicitação de leasing e o CSS, por exemplo, devido ao arrendatário ser um freguês regular do vendedor.

[0092] Como explicado neste relatório, o CSS recupera e reporta status para este e outros certificados usando um meio de reportagem de status de certificado que usa um protocolo de reportagem de status aprovado. Na Fig. 8, é assumido que a CA Automotiva e a CA Financeira usam OCSP, que a CA de Banco usa uma CRL, e que o vendedor e arrendatários têm alguma forma de objeto de dados (por exemplo, PKCS#11, PKCS#12, armazenamento de chave de navegador etc) que contêm seus certificados de uma transação; mais ou menos CAs podem ser conectadas, conforme necessário, com comunicações, como necessário, para a transação particular.

[0093] Na etapa 801, o vendedor origina o contrato de leasing ou recupera o mesmo de uma aplicação de leasing, como um programa de

computador rodando localmente na loja do vendedor ou remotamente em outro local, por exemplo, no Servidor da Aplicação. Na etapa 803, o vendedor orquestra a execução do leasing pelo arrendatário e locador. O leasing pode ser exibido para ambos o arrendatário local e o locador remoto neste momento, e o vendedor pode ser solicitado a responder qualquer questão e fazer correções se necessário. O vendedor pode arranjar para exibir o leasing ao locador por prover um URL (localizador de recurso uniforme) ao locador, que possibilita ao mesmo rever e executar o leasing, com a versão executada retornada ao vendedor. Após assinatura local pelo arrendatário e o vendedor, por exemplo, com um tablete de pc que captura a assinatura digital do arrendatário sobre o leasing, e assinatura remota pelo locador, o leasing sendo transmitido (etapa 805) a um Cofre Eletrônico, que é mostrado em comunicação com o Servidor de Aplicação. A assinatura digital pelo arrendatário e vendedor é, vantajosamente, dinâmica, com o Servidor de Aplicação atualizando as exibições pela aplicação de um indicador “digitalmente assinado por” à(s) imagem(s) exibida(s). As assinaturas digitais reais não são, de preferência, exibidas.

[0094] Deve ser reconhecido que o Servidor de Aplicação e Cofre Eletrônico associado podem ser usados pelo vendedor para estagiar o contrato para assinatura remota pelo locador. Nas etapas 807 a 811, o locador recupera o leasing do cofre, concorda com os termos do leasing pela assinatura digital do mesmo, e retorna sua versão digitalmente assinada para o cofre. As etapas 807 a 811 ilustram ambos, a colaboração multi-site e processamento de transação assíncrona.

[0095] Nas etapas 813 a 817, o(s) documento(s) eletrônicos recebidos (o leasing) são conferidos quanto a assinaturas digitais, e se alguma for encontrada, a assinatura digital é verificada e os respectivos certificados de autenticação são validados. Na etapa 817, a hora local é conferida para assegurar que está dentro do(s) período(s) de validade do(s) certificado(s), e

na etapa 819, o CSS é indagado quanto ao status do(s) certificado(s). Em resposta, na etapa 821, o CSS primeiro confere sua memória cache local ou armazenamento de dados quanto a status de certificado, e se um status de certificado estiver presente e corrente, o CSS retorna o status de certificado como “ativo” na etapa 827. Na etapa 823, se o status de certificado não estiver presente ou não corrente, o CSS indaga a CA emissora usando o tipo de conector criado para este fim. Na etapa 825, a CA emissora, por exemplo, a CA de Banco, ou seu meio de reportar status (por exemplo, diretório) retorna status ao CSS, de preferência, usando o mesmo conector, e na etapa 827, o CSS reporta o status de certificado indagado de volta ao Servidor da Aplicação.

[0096] Assumindo que rodas as assinaturas digitais e certificados estão verificados e validados, provendo como autêntico o documento eletrônico, o Servidor de Aplicação assume controle do documento eletrônico e o serve ao Cofre Eletrônico como uma nova versão na etapa 829. Desse modo, será visto que, com as características próprias, o Servidor de Aplicação e Cofre Eletrônico cooperam como um TCU. Na etapa 831, a nova versão é designada como uma cópia oficial, um Original Eletrônico que também pode ser um registro transferível, por anexar uma marca de data-hora e aplicar a assinatura digital do TCU ao documento. Enquanto pelo menos uma assinatura digital sobre um documento for válida, esta etapa ocorre.

[0097] Na etapa 833, se qualquer assinatura digital ou certificador falhar na passagem por todos os testes, o vendedor é alertado a procurar remédio, que tipicamente envolve etapas de repetição 801 a 829 até que assinaturas digitais de substituição válidas sejam aplicadas. O processo de remediar não pode terminar se o status de um certificado de signatário estiver anulado ou expirado até que um novo certificado e material criptográfico sejam emitidos.

[0098] Deve ser entendido que um objeto de informação, como um

leasing de um automóvel, pode ser apresentado em uma forma eletrônica, por exemplo, XML, PDF, PKCS#7, S/MIME etc., que possibilita colocação e detecção de assinaturas digitais e impede modificação não-autorizada. Muitas destas formas, portanto, podem ser consideradas como provendo envelopes ou invólucros para a informação incluída.

[0099] Deve ser entendido também que o CSS pode ser usado para conferir status de certificados, a despeito do uso de chave. Estes certificados incluem, mas não de modo limitativo, aqueles para os quais o uso primário não é identidade e autenticação, por exemplo, chave de concordância/troca, assinatura de certificado, assinatura de CRL, criptografia de chave, criptografia de dados, só criptografia, só descriptografia, e camada de soquetes segura (SSL). Conseqüentemente, deverá ser entendido que, como usado neste relatório, o termo “certificado de autenticação” abrange, geralmente, esses certificados que não são usados para identificação.

[00100] Em adição, um conector CSS pode, vantajosamente, embutir mais de um status de certificado em uma única comunicação. Entre outras coisas, esta capacidade pode ser usada na validação de parte ou de toda uma cadeia de certificados e certificados de CA de usuário/entidade, por exemplo, uma hierarquia de CAs de uma CA raiz até uma CA emissora. Isto provê segurança adicional de que todas as CAs no caminho do certificado ainda estão válidas.

[00101] Este relatório descreveu um método para configurar um Serviço de Status de Certificado (CSS) que inclui as etapas de determinar informação de ajuste necessária para recuperar status de certificado para uma CA emissora de requisito, identificando um conector compatível com uma técnica de consulta de status de certificado usada para recuperar status de certificado da CA emissora, configurando o conector com parâmetros de ajuste e de comunicações específicos para o conector selecionado e a CA emissora, e estabelecendo um mapeamento de CSS entre a CA emissora e o

conector. A designação e conector de CA são adicionados a uma lista de CAs aprovadas em um armazenamento de configuração.

[00102] Um método para executar uma transação pela transferência de objetos de informação autenticados tendo respectivas pistas de evidência verificáveis inclui a etapa de recuperar, por uma primeira parte de um repositório confiável, um objeto de informação autenticado. O objeto de informação autenticado inclui uma primeira assinatura digital da parte submissora, uma data e hora confiáveis, uma assinatura digital do repositório confiável, um certificado relatando pelo menos a identidade e chave criptográfica ao repositório confiável; a assinatura digital e certificado da parte submissora tendo sido validados pelo repositório confiável na submissão atestando autenticidade dos objetos; e o ia tendo sido colocado em armazenamento como um objeto de informação de original eletrônico colocado sob o controle do repositório confiável.

[00103] O método de execução de transação inclui ainda as etapas de requerer qualquer entidade signatária e comprometer ao uso e ser limitada por sua assinatura digital antes de ato de assinar, executando o mencionado objeto de informação por qualquer parte, consiste de inclusão de pelo menos a assinatura digital e certificado de autenticação da parte signatária, criando um bloco de assinatura que contém pelo menos a assinatura digital e certificado de autenticação da parte signatária, associando o bloco de assinatura ao objeto de informação, repetindo as etapas prévias de execução onde múltiplas entidades assinam digitalmente o objeto de informação e/ou envelope, e encaminhando o objeto de informação digitalmente assinado e/ou envelopado a um TCU. O TCU verifica cada assinatura digital e valida cada certificado de autenticação associado e recupera status de um CSS. Os blocos de assinatura são rejeitados se a assinatura digital do signatário não for verificada ou um certificado de autenticação de signatário tiver expirado ou for reportado como anulado. A rejeição de qualquer bloco de assinatura resulta em uma

solicitação por um bloco de assinatura em substituição ou iniciação de remédio. Se pelo menos um bloco de assinatura for determinado como válido, o TCU anexa seu próprio bloco de assinatura, contendo também data e hora confiáveis, ao objeto de informação sujeito, criando um original eletrônico que ele contém e controla em nome do proprietário.

[00104] A criação de um bloco de assinatura digital pode incluir as etapas de computar um ou mais hashes de conteúdo para um ou mais fragmentos de objeto de informação ou para todo o objeto de informação, computando um hash sobre um ou mais hashes de conteúdo e qualquer dado anexado, como data e hora locais, assinatura racional, ou uma instrução, criptografando o hash computado usando a chave privada de parte signatária, formando, desse modo, a assinatura digital do signatário, e colocando a assinatura digital do signatário no bloco de assinatura juntamente com o certificado de autenticação do signatário. Se o dado anexado incluir uma data e hora locais, criar um bloco de assinatura digital pode incluir ainda as etapas de exibir a data e hora locais, solicitar que um signatário afirme que a data e hora estão corretas, e corrigir as mesmas se alguma estiver incorreta, ou confiar em uma data e hora do sistema se estas forem estabelecidas por um serviço de hora confiável e data e hora estiverem protegidas de violação. A data e hora locais podem ser conferidas para assegurar se são precisas e dentro do período de validade do certificado de autenticação do usuário e que a data e hora locais não estão antes nem depois das datas e horas especificadas pelo período de validade.

[00105] Remédio de uma assinatura digital que falha na verificação requer que a assinatura digital seja recomputada e o bloco de assinatura seja retransmitido. A remediação de uma violação de período de validade de um certificado de autenticação inclui notificar o usuário que seu certificado expirou e que tem que ser renovado e notificar o proprietário da transação que a transação está incompleta.

[00106] A colocação de um ou mais blocos de assinatura e a informação contida no mesmo é especificada por pelo menos uma etiqueta de assinatura. Uma ou mais assinaturas manuscritas e datas são digitalizadas e usadas para execução de objeto de informação, e colocação das assinaturas e datas é especificada por pelo menos uma etiqueta de assinatura. Um ou mais blocos de assinatura podem ser enviados ao TCU separadamente juntamente com a designação das etiquetas de assinaturas correspondentes e o TCU pode validar cada bloco de assinatura enviado independentemente ou em grupo. Se a etapa de verificação ou validação de certificado de autenticação de assinatura digital falhar, o TCU rejeita o bloco de assinatura e pode solicitar remédio, e se a etapa de validação de bloco de assinatura for bem-sucedida, o TCU coloca o bloco de assinatura na etiqueta indicada. Para blocos de assinatura enviados separadamente, o TCU pode adicionar uma data e hora confiáveis a cada bloco de assinatura. De acordo com as regras do negócio, o TCU anexa seu próprio bloco de assinatura que contém uma data e hora confiáveis em um envelope que abrange os campos de objeto de informação de sujeito e bloco de assinatura inserido, criando, assim, um objeto de informação de original eletrônico. Blocos de assinaturas de múltiplos usuários podem ser adicionados em um envelope, e envelopes podem ser recorrentemente aplicados para implementar outros processos de negócio e segurança.

[00107] O TCU pode validar a(s) assinaturas digitais e certificado(s) de autenticação presentes em bloco(s) de assinatura que deve(m) estar contido(s) e/ou adicionado(s) ao conteúdo de um objeto de informação original eletrônico por checar no banco de dados de regras comerciais se a entidade signatária identificada pelo certificado de autenticação tem autoridade para efetuar a ação solicitada, verificar a assinatura digital da entidade signatária, conferir se o período de validade do certificado está sobreposto às data e hora confiáveis correntes, conferir se a data e hora locais apresentadas estão dentro

do desvio permitido em relação à data e hora do TCU, e conferir status de certificado usando um CSS. Se qualquer dessas etapas resultar em uma saída inválida ou falsa, a assinatura digital é considerada inválida, a ação solicitada é impedida e remédio cogitado; de outro modo, a assinatura digital é considerada válida e a ação solicitada é permitida.

[00108] Registro de uma CA emissora com um CSS pode incluir as etapas de verificar e aprovar a CA emissora para inclusão em uma base de reconhecimento de CSS como “autorizada” baseado nas regras comerciais de indústria ou organização e política de sistema. Se a etapa de verificação falhar, a CA emissora é adicionada ao armazenamento de objeto de informação de CSS como “não autorizada”, e os parâmetros de comunicação (endereço IP, chave e certificado SSL) e o método usado para reportar status de certificado (OCSP, CRL, LDAP) são adicionados ao armazenamento de configuração de CSS, e o conector para interpretar status de certificado é adicionado caso não já implementado. Desse modo, o CSS possibilita interoperabilidade entre um sistema ou TCU e um conjunto diverso de respondedores de status de certificado.

[00109] Conferência de status de certificado emprega, vantajosamente, um CSS para estabelecer comunicações, recuperar e fazer cache de status de certificado de CAs emissoras de certificado aprovadas. Quando CSS recebe uma indagação de status de certificado de um sistema ou TCU, o CSS primeiro confere seu cache local para ver se o status de certificado está presente e, caso encontrado e dentro do intervalo de tempo-de-sair, então o CSS recupera status solicitando, primeiro, informação de conexão de seu armazenamento de configuração. O CSS estabelece, então, uma sessão de comunicações com componente de reportagem de status de certificado identificado em seu armazenamento de configuração. O CSS compõe uma solicitação de status de certificado pelo método contido no armazenamento de configuração de CSS, e o CSS recupera status de certificado do componente

de reportagem de status de certificado e fecha a sessão com componente. O CSS adiciona pelo menos a ID do certificado, status de certificado e tempo-de-sair para seu cache e retorna status de certificado para o sistema solicitante ou TCU.

[00110] A reportagem de status de certificado pode ser baseada em uma CRL e processamento da CRL. De acordo com o programa de publicação de CA emissora, o CSS recupera a CRL do componente de reportagem de status de certificado listado no armazenamento de configuração de CSS. O CSS apaga sua memória cache associada à CA emissora, analisa status de certificado da CRL, e coloca o status de certificado em seu cache associado a CA emissora. Quando da notificação para uma CA emissora que uma CRL está disponível, o CSS pode recuperar a CRL do componente de reportagem de status de certificado listado no armazenamento de configuração de CSS. Quando for exigido pelas normas que a CRL seja uma CRL completa, então o CSS apaga o cache associado a CA emissora, analisa a CRL, e coloca o status de certificado e informação relativa no cache associado a CA emissora. Quando a CRL contém apenas mudanças ocorrendo após publicação de uma CRL completa, o CSS analisa status de certificado da CRL e coloca o status de certificado e informação relativa no cache associado a CA emissora.

[00111] O uso de um CSS para obter status de certificado que permite um usuário, sistema ou TCU usar um único meio de obter status de certificado pode incluir as etapas de indagar o CSS sobre o status de um certificado de autenticação presente em um bloco de assinatura sobre um objeto de informação, quando a indagação de status pode usar um único meio (por exemplo, OCSP), translada a indagação de status para uma forma exigida pela CA emissora, e recupera e/ou reporta status de certificado. Se status de certificado for anulado, o bloco de assinatura não é usado e remédio é exigido; se a assinatura digital for verificada e status de certificado for válido,

o bloco de assinatura é adicionado ao objeto de informação de original eletrônico.

[00112] O TCU pode indagar o CSS para validar um status de certificado de autenticação de signatário por localizar e reportar status de certificado se o status estiver presente e corrente no cache/armazenamento de dados de CSS, e obter tipo e meios para remover status de certificado do armazenamento de configuração de CSS. Se o método particular de status de certificado for uma CRL e o status de certificado especificado não for encontrado no cache de CA emissora no CSS, então o CSS reporta o status de certificado como válido. SE o método de status de certificado não for uma CRL, então o CSS compõe uma solicitação de status de certificado pelo método contido no armazenamento de configuração de CSS, e estabelece comunicações apropriadas com a CA emissora. O CSS recupera status de certificado do componente de reportagem de status usando o método de conferência de status de certificado identificado e fecha a sessão de comunicação. O CSS analisa ou interpreta o status de certificado recuperado, associa um valor de tempo-de-sair igual ao período especificado pelo tipo de status conforme referido na política de CSS, e adiciona pelo menos a ID de certificado, status, e valores de tempo-de-sair ao cache de status de certificado de CA emissora. O CSS retorna então status de certificado ao sistema solicitante.

[00113] Um método de inscrever usuários em um sistema ou TCUU quando certificados são emitidos por uma CA emissora aprovada conhecida de um CSS inclui verificar o usuário usando procedimentos e critérios de inscrição de membro estabelecidos, entrando informação de inscrição de usuário que tenha também sido assinada por um patrocinador de organização aprovado, e criar e enviar uma solicitação de certificado à CA emissora identificada. O certificado de autenticação de usuário é recuperado, emitido e colocado sobre um objeto de dados para despacho. Assinatura digital,

verificação de assinatura digital e conferência de status de certificado de CSS são executados para assegurar que geração de par de chaves públicas e processo de emissão de certificado foram concluídos corretamente. O usuário é solicitado a assinar o acordo de aceitação de usuário que obriga o usuário a dar o mesmo peso a uso de sua assinatura digital como daria ao uso de sua assinatura manuscrita, o objeto de dados é despachado ao usuário, e o sistema ou conta de TCU do usuário é ativado.

[00114] Um método de inscrever usuários em um sistema ou TCU onde o usuário já tem um certificado emitido por uma CA que não é previamente conhecido de um CSS pode incluir indagar o objeto de dados de usuário para o certificado de autenticação de usuário e obter informação do emissor, e indagar a base de conhecimento de CSS para ver se a CA emissora está contida na mesma. Caso negativo, o administrador de política de indústria ou organização é contatado para determinar se ou não a CA emissora satisfaz as regras de sistema para inclusão de CA. Quando a CA emissora é considerada “não autorizada”, o registro termina, e quando a CA emissora é considerada “autorizada”, a inscrição prossegue conforme descrito acima.

[00115] Uma porção de conteúdo de certificado de autenticação de um usuário pode ser usada para relacionar o certificado a uma conta de usuário por, após aprovar o usuário para acesso ao sistema ou TCU, entrar a informação de inscrição do usuário, inserir o objeto de dados do usuário que contém seu certificado de autenticação em uma leitora de objeto de dados local, recuperar e exibir o conteúdo do certificado, fazer o usuário afirmar que o conteúdo está correto, e adicionar campos selecionados aos dados de inscrição de usuário no TCU, que são extraídos do certificado, como ID de certificado, CA emissora, um subconjunto de nomes distintos de usuário ou outra informação de identificação conduzida nas extensões de certificado (por exemplo, NomeAltsujeito). Os dados extraídos podem ser especificados na política de sistema ou TCU de modo que a extração e entrada de dados

possam ser automatizadas.

[00116] Um método pelo qual um submissor de um objeto de informação avalia a autenticidade de um objeto de informação submetido inclui a etapa de afixar o bloco de assinatura do submissor a um objeto de informação e/ou envelope e encaminhar o mesmo a um sistema ou TCU. Se a validação de bloco de assinatura falhar, o TCU solicita retransmissão ou remédio, e se a validação do bloco de assinatura for bem-sucedida, o TCU confere, então, se a identidade do submissor casa com a do iniciador de sessão de comunicação, rejeitando a submissão se o iniciador e submissor forem diferentes. Se todas as conferências forem bem-sucedidas, o TCU adiciona seu bloco de assinatura à submissão, criando um objeto de informação de original eletrônico.

[00117] Um método em um CSS de manter status de certificado preciso e oportuno para meios de reportar status de certificado em tempo real que empregam um elemento de dado de tempo-de-sair inclui estas etapas. Se um método de status de CRL for usado, então o CSS reporta o status. SE o status de certificado estiver em cache e o elemento de dado de tempo-de-sair não estiver excedido, então o CSS reporta status. Se o elemento de dados de tempo-de-sair for excedido, o CSS apaga a entrada de status de certificado do cache de CA emissora. Se o status for recuperado usando um meio de reportagem de status de certificado em tempo real (por exemplo, OCSP, indagação de LDAP etc.) e status não estiver no cache, status de certificado é solicitado, recuperado e reportado. O CSS adiciona, então, pelo menos a ID de certificado, status de certificado e tempo-de-sair para seu cache e retorna status de certificado ao sistema ou TCU solicitante.

[00118] Um elemento de dado de contador de uso de status de certificado pode ser adicionado a uma entrada de status de certificado no cache de CA emissora de CSS, e o contador de uso de status pode ser incrementado ou decrementado toda vez que um certificado de autenticação

for conferido. Se o contador de uso de status passar de um limiar estabelecido pela política de CSS, então o status de certificado pode ser reportado, mas o CSS apaga, então, a entrada de status de certificado do cache de CA emissora. Se o status de certificado retornado ao CSS for inválido ou anulado, então o sistema ou TCU registra e/ou reporta o erro ao submissor e/ou proprietário de transação, e a ação solicitada é proibida e remédio considerado. De outro modo, a assinatura digital é considerada válida e a ação solicitada é permitida. Um elemento de dado de status de certificado último acessado pode ser adicionado e usado em conjunto com o contador de uso para determinar o nível de atividade do status de certificado.

[00119] Um processo de segundo plano pode fazer com que o CSS recupere automaticamente status de certificado atualizado e estabelecer novos elementos de dados de tempo-de-sair e contador de uso quando um critério na política e CSS for satisfeito. Esta pré-obtenção pode ser possibilitada para encurtar o tempo médio entre solicitação de status de certificado de sistema e TCU e resposta de CSS.

[00120] Se uma solicitação for feita ao CSS para recuperar status de certificado para um novo certificado e o cache de CA emissora tiver alcançado seu limite de tamanho de buffer alocado, o elemento de dado de status de certificado último acessado pode ser adicionado à entrada de status de certificado no cache de CA emissora de CSS. O CSS busca o cache de CA emissora para o elemento de dado último acessado para a data mais antiga (menos frequentemente usada) e apaga esta entrada. O CSS recupera, então, o status de certificado solicitado, coloca o mesmo no local liberado no cache de CA emissora e reporta o status ao sistema ou TCU que atua de acordo com a política.

[00121] Um método de conferência de status em um CSS distribuído inclui coordenação entre CSSs sempre que uma nova CA emissora for introduzida, estabelecendo entradas em todas as bases de reconhecimento de

CSS se um outro CSS tiver responsabilidade primária para indagar uma CA emissora, indagar outros CSSs em vez de uma CA emissora para reduzir comunicação entre o CSS e CAs emissoras, sincronizando e pondo em cache status de certificados contra uma CA emissora, e compartilhando ou transferindo a responsabilidade de indagação se um outro CSS tiver atividade mais pesada com uma dada CA emissora do que o CSS primário original.

[00122] A exclusão de um conjunto de usuários associados a uma CA emissora pela mudança da referência de CA emissora em uma base de reconhecimento de CSS para “não aprovada” pode ser feita solicitando e que aprovação para a CA emissora seja retirada, revendo a solicitação quanto ao mérito e determinando qual, se alguma ação for necessária, e se for determinado que, por qualquer razão, a CA emissora deve ser desabilitada, então mudar o status de CA emissora na base de reconhecimento de CSS para “não aprovada”. Qualquer solicitação adicional de status de um certificado emitido por uma CA listada como “não aprovada” resulta no CSS retornar um status de falha.

[00123] Um método de tornar a habilitar um conjunto de usuários desabilitados por previamente ajustar uma referência de CA emissora para “não aprovada” pode ser feito solicitando que aprovação seja dada para tornar a habilitar a CA emissora, revendo a solicitação sobre o mérito e determinando qual, se alguma ação for necessária, e se for determinado que, por qualquer razão, a CA emissora deve ser novamente habilitada, então mudar o status de CA emissora na base de reconhecimento de CSS para “aprovada”. O CSS processa solicitações de status de certificado para CAs emissoras reinstaladas como faria qualquer outra CA “aprovada”.

[00124] Comunicação com componentes de reportagem de status pode ser estabelecida pela criação de um aparelho modular e reutilizável para cada protocolo de status de certificado usado para localizar, solicitar e recuperar esta informação, usando uma versão do aparelho que é compatível com todas

as CAs e respondedores que compreendem um protocolo de status de certificado particular, e tendo uma versão do aparelho para cada protocolo de reportagem e status que está em uso. O aparelho é designado de modo que seja facilmente adaptável para suportar futuros protocolos de reportagem de status de certificado.

[00125] A execução de uma transação na qual o submissor é um primeiro TCU e a submissão for para transferência de custódia de um ou mais originais eletrônicos para um segundo TCU pode incluir ter o proprietário da transação instruir o primeiro TCU para transferir custódia de um ou mais documentos de original eletrônico para um segundo TCU. O proprietário da transação instrui o segundo TCU a transferir custódia de um ou mais documentos de original eletrônico, e o proprietário provê o primeiro TCU com um manifesto que identifica quais originais eletrônicos devem ser transferidos para o segundo TCU. O primeiro TCU estabelece comunicações como segundo TCU, e identifica a finalidade de suas ações para o segundo TCU. O primeiro TCU ou proprietário pode transmitir o manifesto para o segundo TCU de modo que ele seja capaz de determinar quando a transferência de custódia for completada. O primeiro TCU transfere cada original eletrônico identificado para o segundo TCU, que usa o CSS para assegurar que a assinatura digital do primeiro TCU sobre cada original eletrônico transferido seja válido e que os originais eletrônicos estejam inalterados. SE alguma das assinaturas digitais do primeiro TCU for inválida, então o segundo TCU notifica o primeiro TCU e busca remédio (por exemplo, pede ao primeiro TCU para resignar do uso de certificado de autenticação corrente). Se o primeiro TCU for incapaz de obedecer, o segundo TCU registra o evento e notifica o proprietário da transação que a transferência solicitada de custódia falhou; de outro modo, o segundo TCU cria um novo envelope para cada objeto de informação transferido com sucesso, adicionando uma marca de data-hora e seu bloco de assinatura. O segundo

TCU notifica o primeiro TCU de cada transferência bem-sucedida, e ao terminar, o primeiro TCU pode, à discreção do proprietário, marcar e reter cópias de tal maneira que não possam ser consideradas como sendo originais, ou pode destruir todas as cópias que existam dos objetos de informação transferidos. O processo é repetido até que todos os originais eletrônicos identificados sejam transferidos. Desse modo, o segundo TCU se torna a custódia para os registros transferidos que são as cópias oficiais. O segundo TCU pode anexar uma data/hora confiável, assinar digitalmente, envelopar e armazenar o manifesto para torná-lo um elemento independente da trilha-de-custódia.

[00126] Na execução da transação, a instrução do proprietário pode declarar também que uma transferência de propriedade ocorre, e documentação de transferência de propriedade pode ser colocada no primeiro ou segundo TCU. O TCU responsável valida a autenticidade da transferência de documentos de propriedade por verificar todas as assinaturas digitais, período de validade de certificados, e usar o CSS para conferir status de certificado. O TCU, então, anexa data e hora confiáveis, e assina digitalmente, envelope e armazena estes objetos agora originais eletrônicos, que são adicionados ao manifesto. Quando estes originais eletrônicos são colocados no primeiro TCU, transferência-de-propriedade é implementada antes da transferência-de-custódia, e o manifesto inicial se torna parte da trilha-de-propriedade.

[00127] Alguns dos registros transferidos podem ser simples objetos de informação eletrônicos e não apenas originais eletrônicos. O CSS pode usar qualquer protocolo de status de certificado apropriado para comunicar-se com um sistema ou TCU.

[00128] A invenção pode ser concretizada de muitas formas diferentes sem se afastar de um caráter essencial e, assim, os modos de realização descritos acima devem ser considerados ilustrativos, não restritivos, em todos

os aspectos. É enfatizado que os termos “compreender” e “compreendendo”, como usados neste relatório e nas reivindicações anexas, têm a intenção de especificar a presença de características mencionadas sem impedir a presença de uma ou mais outras características. O escopo pretendido da invenção está apresentado pelas reivindicações a seguir, em vez de pela descrição precedente, e todas as variações que estejam dentro do escopo das reivindicações têm a intenção de serem abrangidas pelas mesmas.

REIVINDICAÇÕES

1. Método de prover um serviço de estado de certificado (“CSS”) para conferir validades de certificados de autenticação emitidos por respectivas autoridades de certificação (“CA”), caracterizado pelo fato de que compreende as etapas de:

comparar uma data e hora locais com um período de validade indicado em um certificado de autenticação (111);

enviar uma resposta de “estado inválido” quando a data e hora locais não estão dentro do período de validade (115);

determinar se uma CA emissora que emitiu o certificado de autenticação é designado em uma lista de CAs aprovadas em um armazenamento de configuração (137);

enviar uma resposta de “estado inválido” quando a CA emissora não está na lista de CAs aprovadas (115);

checar uma memória cache local para um estado do certificado de autenticação (123), e se o estado for encontrado na memória cache local, recuperar o estado da memória cache local (125);

caso contrário, obter, a partir do armazenamento de configuração da CSS, os métodos de reportagem e informações de comunicação necessários para recuperar, a partir das CA's emissoras (137), um certificado de estado de cada certificado de autenticação cujo estado ainda não foi determinado;

configurar um conector baseado na informação identificada para comunicação com a CA emissora (137);

comunicar-se com a CA emissora de acordo com o conector configurado quando o estado do certificado de autenticação for inquirido (143);

recuperar o estado do certificado de autenticação (125);

processar o estado recuperado do certificado de autenticação

de acordo com os métodos de reportagem implementos pelo CSS;

armazenar o estado em uma memória cache associada com a CA emissora (153); e

retornar uma confirmação com base no estado recuperado para um solicitante;

em que a lista de CAs aprovadas é formada através de investigação e aprovação de CAs emissoras de acordo com as regras pré-determinadas; e

em que as CA's emissoras e a informação do conector de comunicações são definidas em uma lista de CA's aprovadas no armazenamento de configuração da CSS.

2. Método de acordo com a reivindicação 1, caracterizado pelo fato de que se a CA emissora for investigada e não aprovada para a lista de CAs aprovadas, a CA emissora é designada em uma lista de CAs não aprovadas no armazenamento de configuração (139).

3. Método de acordo com a reivindicação 2, caracterizado pelo fato de que investigar e aprovar a CA emissora inclui registrar uma representação de um certificado de autenticação confiável com o CSS e adicionar pelo menos a representação, estado e um elemento de dados de sobrevida para uma memória cache local, e um conector ser configurado para recuperar o estado adicionado quando o estado do certificado de autenticação confiável for inquirido (715).

4. Método de acordo com a reivindicação 1, caracterizado pelo fato de que se o estado não for encontrado na memória cache local ou se a data e hora locais não estiverem dentro do período de validade, a CSS estabelece uma sessão de comunicação com um componente de reportagem de estado de certificado da CA emissora, compor uma solicitação de estado de certificado de acordo com o conector configurado (143), recuperar o estado do componente de reportagem de estado de certificado, fechar a sessão de

comunicação com o componente de reportagem de estado de certificado, e adicionar pelo menos a identificação de certificado de autenticação, estado e sobrevida para a memória cache local (153).

5. Método de acordo com a reivindicação 1, caracterizado pelo fato de que o estado do certificado é indicado por uma lista de anulação de certificado (“CRL”) segundo uma programação de publicação da CA emissora, a CSS recupera a CRL de um componente de reportagem de estado de certificado listado no armazenamento de configuração (125), a CSS apaga a memória cache associada com a CA emissora e a CSS determina o estado do certificado de autenticação a partir da CRL e armazena o estado na memória cache associada com a CA emissora.

6. Método de acordo com a reivindicação 1, caracterizado pelo fato de que o estado de certificado é indicado por uma lista de anulação de certificado (“CRL”) Delta; quando da notificação pela CA emissora de que uma CRL está disponível (141), o CSS recupera a CRL de um componente de reportagem de estado de certificado listado no armazenamento de configuração; se a CRL for uma CRL completa, então o CSS limpa uma memória cache associada à CA emissora, determina o estado a partir da CRL, e armazena o estado na memória cache (153); e se a CRL contiver apenas mudanças ocorridas após a publicação de uma CRL completa, o CCSS determina o estado da CRL, e armazena o estado na memória cache (153).

7. Método de acordo com a reivindicação 1, caracterizado pelo fato de que a etapa de comunicação inclui comunicar-se segundo uma sequência de conectores.

8. Método de acordo com a reivindicação 1, caracterizado pelo fato de que um conector embute mais de uma conferência de estado de certificado em uma única etapa de comunicação.

9. Método de acordo com a reivindicação 1, caracterizado pelo fato de que a etapa de identificar compreende obter um tipo de estado e

método de recuperação de um armazenamento de configuração de CSS (143); em que o método compreende ainda:

caso o tipo de estado seja Lista de Anulação de Certificado (“CRL”) e o estado não for encontrado na memória cache, reportar então o estado como válido (125);

caso o tipo de estado não seja CRL, compor, então, uma solicitação de estado de certificado de acordo com o tipo de estado;

estabelecer uma sessão de comunicação com a CA emissora;

recuperar o estado de um componente de reportagem de estado da CA emissora usando o método de recuperação obtido e finalizar a sessão de comunicação (125);

interpretar o estado recuperado (127);

associar, com o estado recuperado interpretado, um valor de sobrevida representando um período especificado por uma política de CSS para o tipo de estado (205);

adicionar pelo menos a identificação, estado, e valores de sobrevida do certificado de autenticação à memória cache (153); e

reportar o estado a um serviço público de custódia confiável (“TCU”) em resposta à indagação (129).

10. Método de acordo com a reivindicação 9, caracterizado pelo fato de que CSS usa um protocolo de estado de certificado na sessão de comunicação.

11. Método de acordo com a reivindicação 9, caracterizado pelo fato de que mais de um estado é recuperado usando o método de recuperação obtido.

12. Método de acordo com a reivindicação 1, caracterizado pelo fato de que a etapa de recuperar o estado a partir da memória cache local compreende:

prover o estado indicado pela memória cache quando a

memória cache incluir um estado e um elemento de dado de sobrevida não estiver excedido (125);

se o elemento de dado de sobrevida estiver excedido, limpar o estado da memória cache;

adicionar pelo menos a identificação de certificado, estado e elemento de dado de sobrevida à memória cache (153); e

prover o estado recuperado (129).

13. Método de acordo com a reivindicação 12, caracterizado pelo fato de que um elemento de dados de contador de uso de estado é adicionado à memória cache; o elemento de dado de contador de uso de estado é incrementado ou decrementado cada vez que o estado de certificado é conferido; e se o elemento de dados de contador de uso de estado passar de um limiar, então o estado é provido e a memória cache é limpa com relação ao estado.

14. Método de acordo com a reivindicação 13, caracterizado pelo fato de que um elemento de dado de estado de último acesso é adicionado à memória cache, e o elemento de dado de estado acessado por último em conjunto com o elemento de dado de contador de uso de estado possibilitam a determinação de um nível de atividade do estado de certificado.

15. Método de acordo com a reivindicação 14, caracterizado pelo fato de que, quando uma solicitação é feita ao CSS para recuperar um estado de um novo certificado e a memória cache tiver alcançado um limite de tamanho de buffer alocado, o CSS pesquisa na memória cache por um elemento de dado de último acesso indicando uma data mais antiga e limpar a respectiva entrada de memória cache; e o CSS, então, recupera o estado solicitado, coloca-o na memória cache, e provê o estado solicitado.

16. Método de acordo com a reivindicação 1, caracterizado pelo fato de que compreende prover um estado de um certificado de autenticação como indicado por uma Lista de Anulação de Certificado

(“CRL”) quando o CA emitindo o certificado utiliza CRLs para indicar o estado (125).

17. Método de acordo com a reivindicação 1, caracterizado pelo fato de que a etapa de recuperar compreende ainda solicitar e recuperar o estado usando um protocolo de reportagem de estado de certificado em tempo real quando o estado não está na memória cache (143).

FIGURA 1

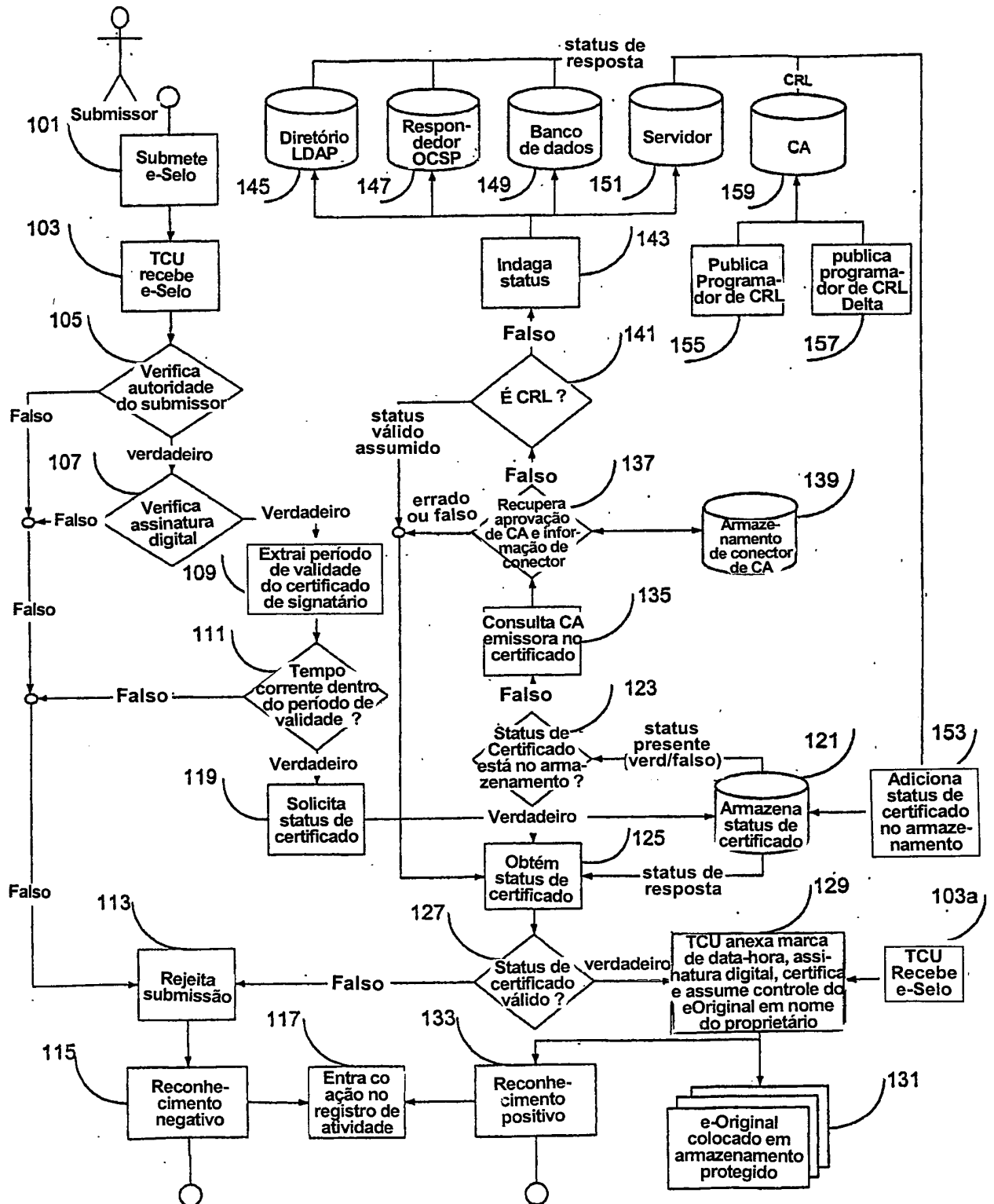


FIGURA 2

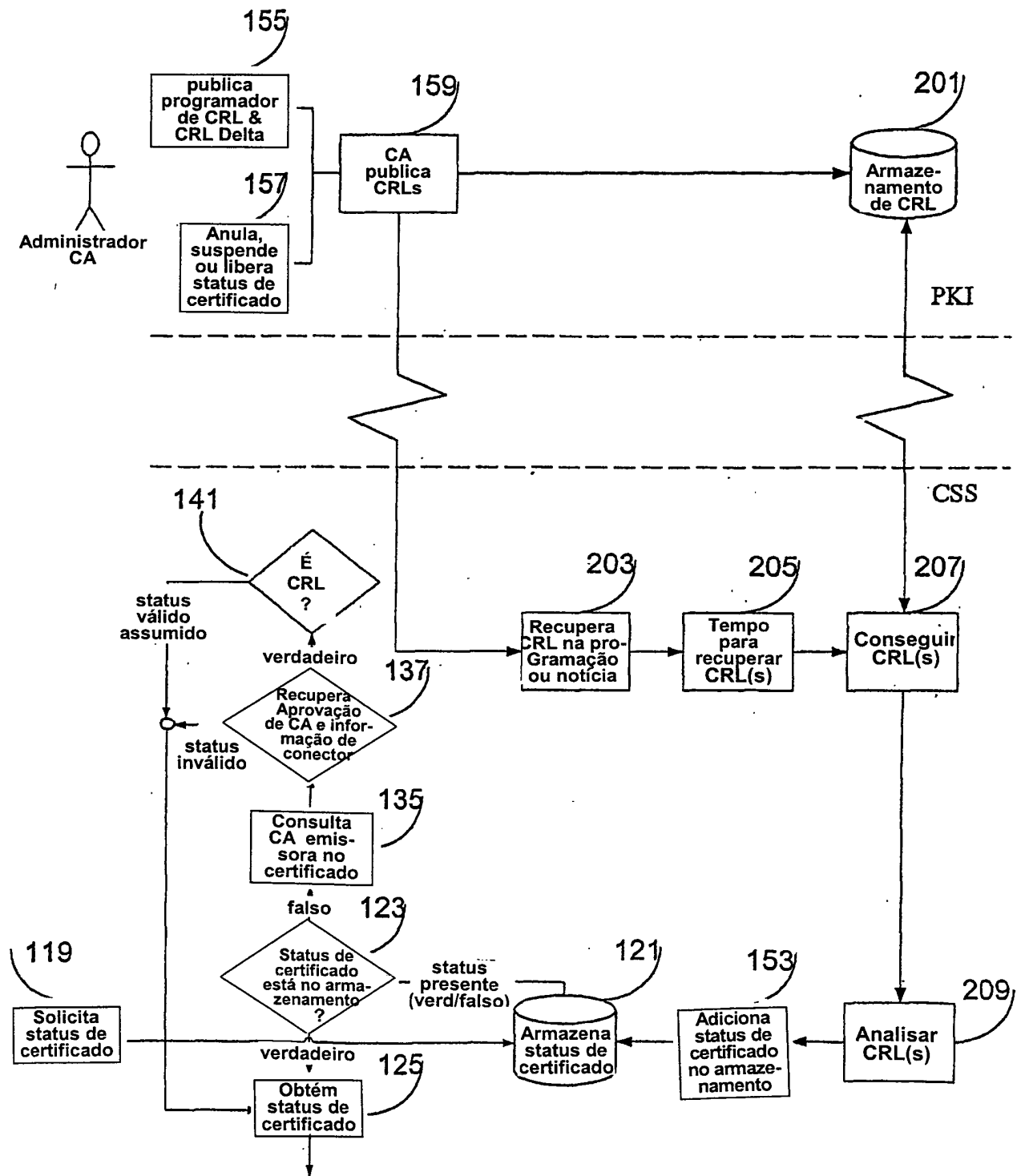


FIGURA 3

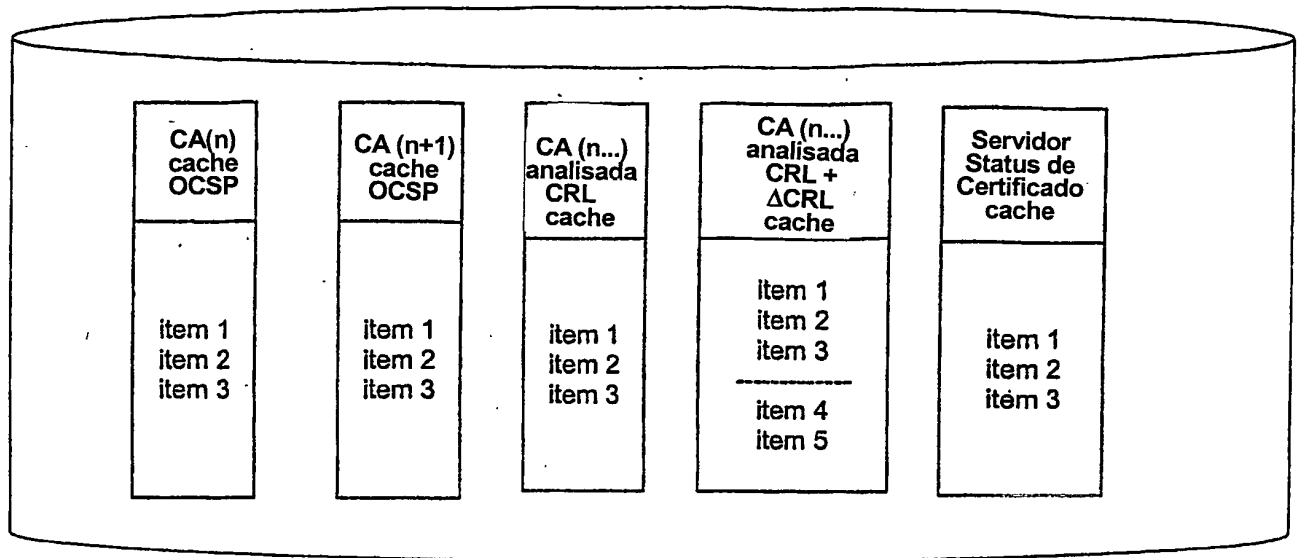


FIGURA 4

Exemplo de sintaxe de bloco de assinatura

Exemplo de forma livre de elementos de dados constituindo uma assinatura digital, onde a assinatura é aplicada a múltiplos fragmentos de mensagem e uma marca de data/hora. Este exemplo não tem a intenção de ser considerado literalmente, mas de ser ilustrativo do tipo de sintaxe que pode ser usado:

```
<Signature>
  <SignedInfo>
    <Signature Method
      Algorithm = RSA (1024bit)/>
    <ReferenceContent>
      <ReferencetoFragment1>
        <HashAlgorithm = SHA-1>
        <HashValue>A62E...</HashValue>
      </Reference>
      <ReferencetoFragment2>
        <HashAlgorithm = SHA-1>
        <HashValue>F0BC...</HashValue>
      </Reference>
      <Authenticated Data>
        <Date>...</Date>
        <Time>...</Time>
      </Authenticated Data>
      <HashAlgorithm = SHA-1>
      <CumulativeHashValue>6E31...</CumulativeHashValue>
    </ReferenceContent>
  </SignedInfo>
  <SignatureValue>602C...</SignatureValue>
  <Unauthenticated Data>
    <
  </Unauthenticated Data>
  <KeyInfo>
    <X509ParsedData>
      <Sequence of X.509 Data Elements>
        <X509Serial #
        <X509Issuer name
        <..
        <X509Subject name
        <..
      </
    </X509ParsedData>
    <X509Certificate>MIIE...</X509 Certificate>
  </KeyInfo>
</Signature>
```

O <CumulativeHashValor> é o aplicado a um ou mais fragmentos de HashValores ou ao conteúdo total e qualquer dado Autenticado

FIGURA 5

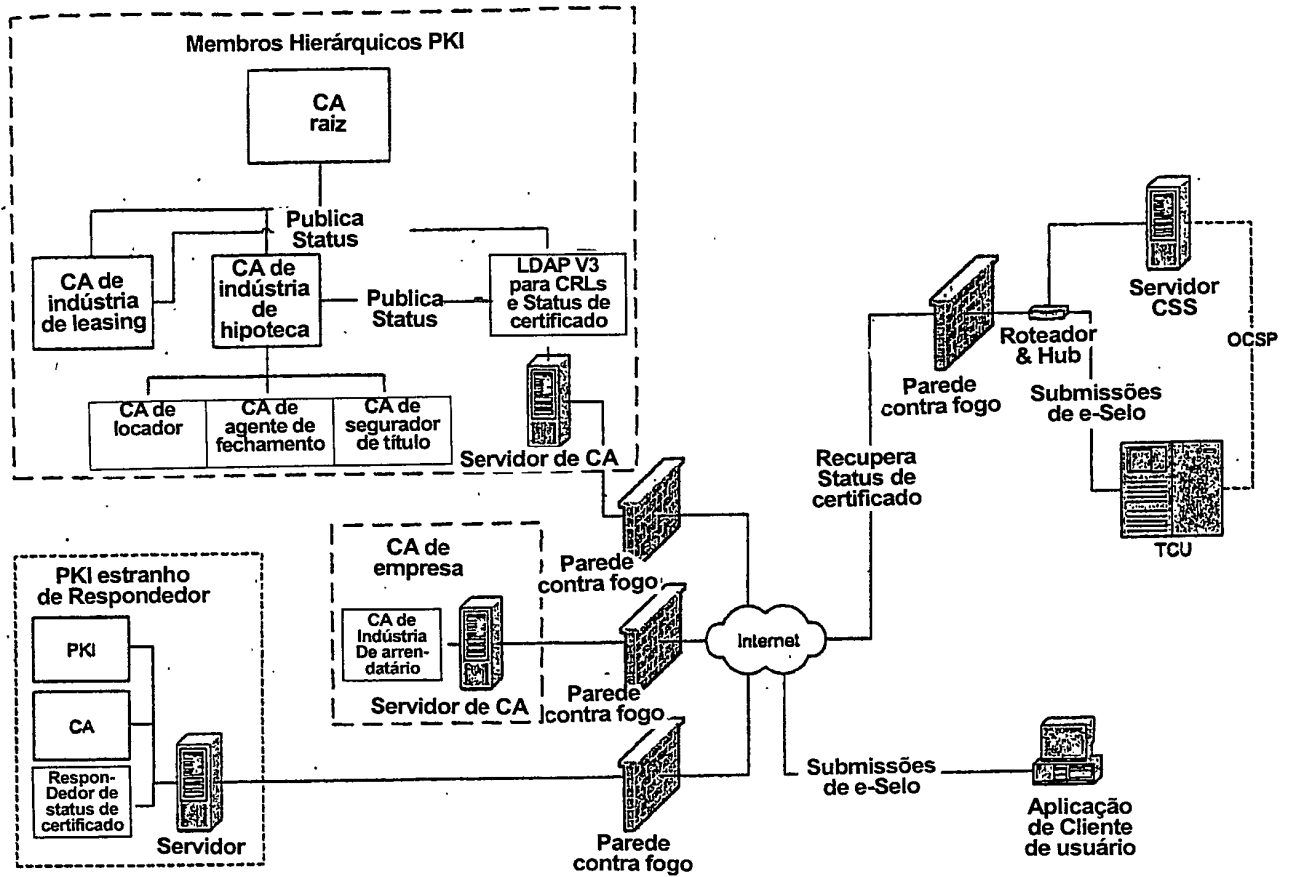


FIGURA 6

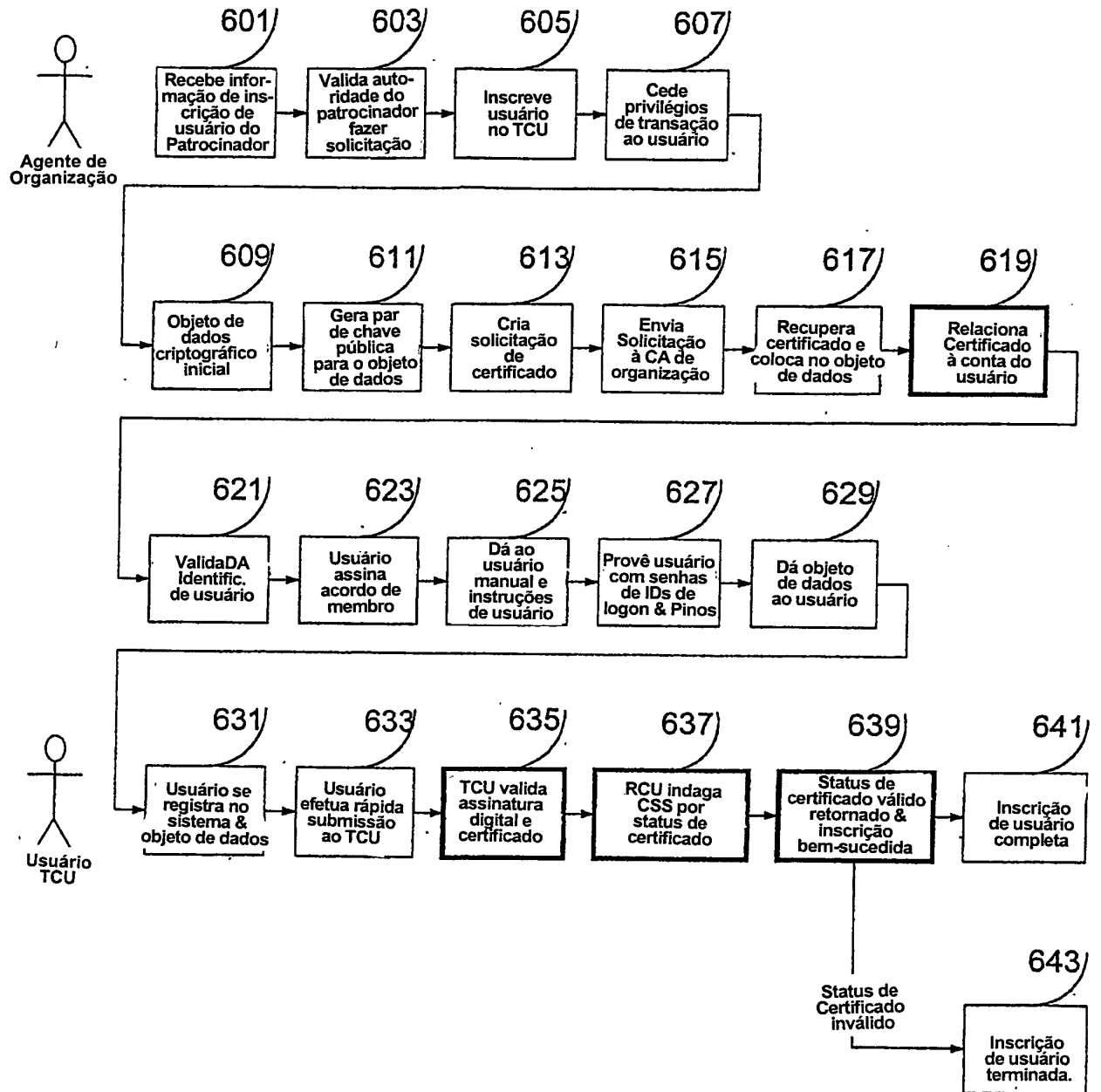


FIGURA 7

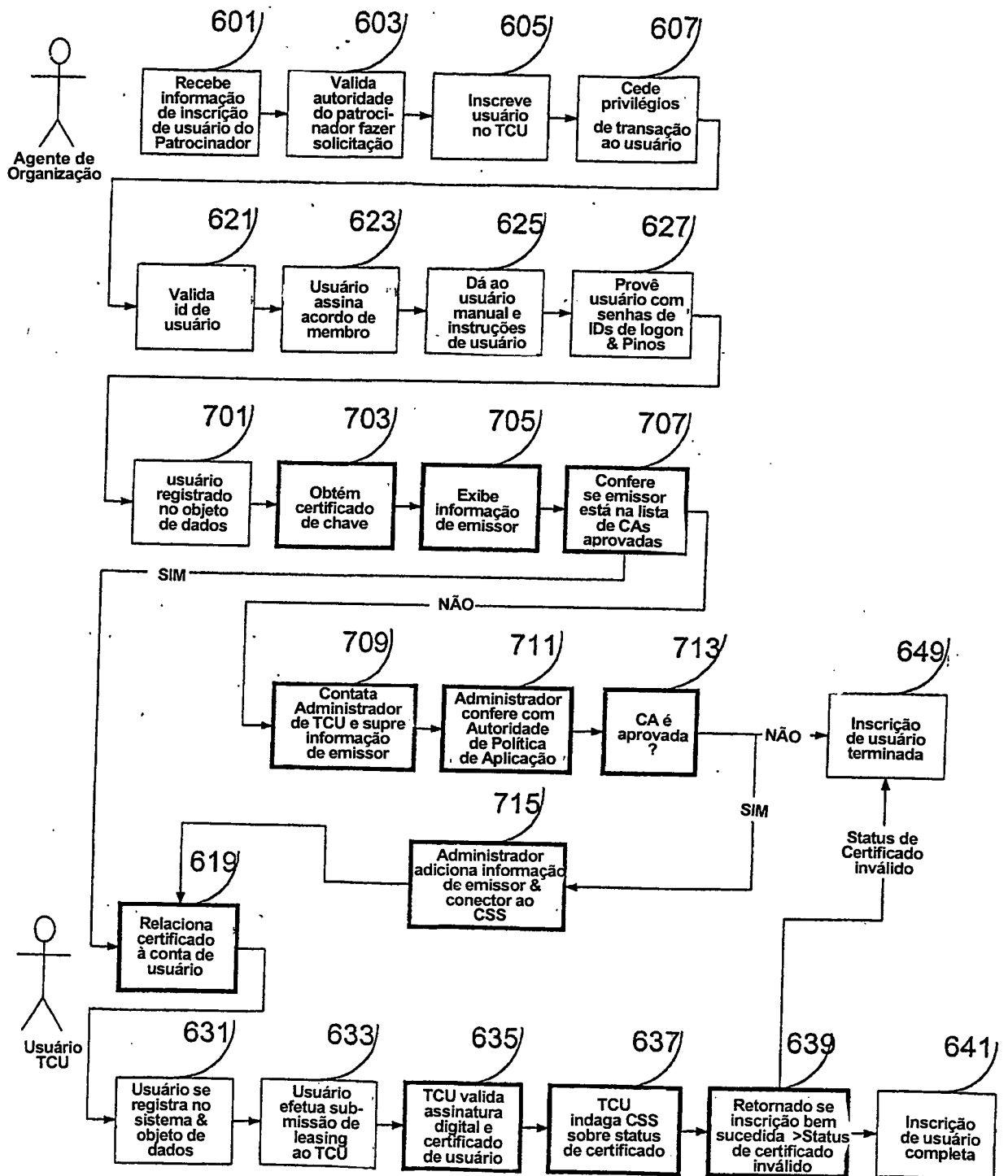


FIGURA 8

