



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

(21) PI 1006951-8 A2



* B R P I 1 0 0 6 9 5 1 A 2 *

(22) Data de Depósito: 25/11/2010

(43) Data da Publicação: 21/05/2013
(RPI 2211)

(51) Int.Cl.:

G06K 19/00

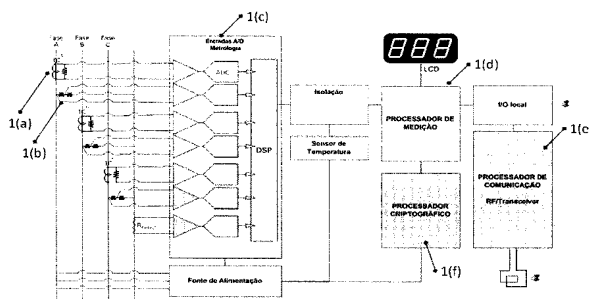
H02H 9/00

(54) Título: MEDIDOR ELETRÔNICO DE ENERGIA ELÉTRICA COM MECANISMO INTEGRADO DE CERTIFICAÇÃO DIGITAL PARA COMUNICAÇÃO SEGURA

(73) Titular(es): Cas Tecnologia S/A, Fundação CPQD - Centro de Pesquisa e Desenvolvimento em Telecomunicações, Instituto de Tecnologia para o Desenvolvimento - LACTEC, Light Serviços de Eletricidade S/A.

(72) Inventor(es): Celso Pinto Saraiva, Fabio de Oliveira Toledo, Rodrigo Jardim Riella, Welson Régis Jacometti

(57) Resumo: MEDIDOR ELETRÔNICO DE ENERGIA ELÉTRICA COM MECANISMO INTEGRADO DE CERTIFICAÇÃO DIGITAL PARA COMUNICAÇÃO SEGURA. Medidor eletrônico de energia elétrica com mecanismo integrado de certificação digital para comunicação segura, compreendendo sensores de corrente 1(a), sensores de tensão (b), circuito eletrônico (c) para acondicionar os sinais de corrente e tensão nos níveis elétricos exigidos pela unidade de processamento (d), unidade de processamento (d) realiza o cálculo de energia ativa e reativa passantes e determina os valores de energia a contabilizar e uma unidade de comunicação (e), associada à unidade de processamento (d), que mediante um protocolo digital de dados e uma interface física relaciona-se com o mundo exterior ao medidor, e unidade de processamento de funções de certificação digital (f) que se interpõe entre a unidade de processamento (d) e a unidade de comunicação (e), em que a unidade de processamento de funções de verificação digital (UPFCD) tem por função realizar a criptografia e a assinatura de todos os dados que são disponibilizados, através do protocolo de dados da unidade de comunicação (e) ao mundo externo, de forma que o relacionamento eletrônico com o medidor no tocante à comunicação de dados passa a ser regido pelo uso da técnica da certificação digital de forma nativa e não dissociável.



MEDIDOR ELETRÔNICO DE ENERGIA ELÉTRICA COM MECANISMO INTEGRADO DE CERTIFICAÇÃO DIGITAL PARA COMUNICAÇÃO SEGURA

CAMPO DE APLICAÇÃO

A presente patente de invenção se refere em geral a medidores de energia elétrica digitais e, em particular, a medidores de energia elétrica digitais tendo um dispositivo que proporciona certificação digital para os dados medidos e transmitidos pelo medidor.

FUNDAMENTOS DA INVENÇÃO

Medidores eletrônicos com leitura automatizada já são conhecidos no estado da técnica.

O documento PI 0503956-8, depositado em 08/09/2005, publicado em 22/05/2007, intitulado “Dispositivo eletrônico de leitura aplicável num medidor digital de energia elétrica dotado de interface para leitura automatizada”, revela um dispositivo eletrônico com a finalidade de realizar a leitura automatizada do valor de consumo de energia acumulado por um medidor de energia digital. Dito sistema leitor é dotado de um cartão de memória flash ou similar para registrar os dados captados através de uma interface de comunicação com ou sem fio; o leitor possui um microcontrolador que é responsável por fazer a comunicação com o medidor de consumo, a integração de dados e gravação na memória de armazenamento; depois de coletados os dados e gravados na memória basta retirar o cartão, coloca-lo num equipamento leitor acoplado a um computador e trabalhar esses dados no sentido de permitir a emissão dos boletos de cobrança aos consumidores da rede. Trata de um cartão de memória para registrar dados do medidor que ao ser inserido em um leitor acoplado a um computador gera boletos de cobrança. Este documento não trata nem menciona um dispositivo eletrônico com certificado digital para proporcionar transmissão segura de dados de um medidor eletrônico a um centro de controle, por exemplo.

O documento PI 0516274-2, depositado em 30/09/2005, data de publicação internacional 20/04/2006, intitulado “Método de prepagamento de energia elétrica, método para controlar automaticamente o fornecimento de energia elétrica, método para obter informação sobre o uso de um medidor eletrônico de prepagamento, método de prepagamento e controle de fornecimento de energia elétrica e sistema de prepagamento e controle de fornecimento de energia elétrica”, revela o uso de um medidor completamente integrado numa única peça, totalmente coberto e sem contato com o exterior que incorpora um sistema de prepagamento e um método mais eficiente para controlar o fornecimento de energia elétrica e obter informação relevante sobre o medidor através de cartões inteligentes sem contato. Portanto, o cartão inteligente do referido documento não antecipa a presente invenção.

OBJETO DA INVENÇÃO

O objeto da presente invenção consiste em medidor de energia elétrica digital tendo inserido no mesmo um chip com certificação digital para proporcionar assinatura eletrônica aos dados da medição de consumo a serem transmitidos a um centro de controle.

BREVE DESCRIÇÃO DAS FIGURAS

A Figura 1 é um diagrama esquemático de um medidor de energia elétrica mostrando os seus componentes principais.

5 A Figura 2 é uma representação do medidor eletrônico concebido em diferentes modelos.

A Figura 3 é um diagrama de utilização de um medidor com seu respectivo certificado digital.

10 A Figura 4 apresenta (a) as técnicas de criptografia (cifra e decifra) e (b) assinatura digital de um pacote de dados.

DESCRIÇÃO DETALHADA DA INVENÇÃO

A presente patente de invenção se refere a medidores de energia elétrica digitais tendo um dispositivo que proporciona certificação digital para os dados medidos e transmitidos pelo medidor. Dessa forma, o medidor da presente invenção proporciona
15 recursos de segurança e rastreamento de dados que permitem tanto às concessionárias distribuidoras de energia elétrica quanto aos consumidores verificar a veracidade dos dados disponibilizados pelos medidores que são utilizados no processo de faturamento de consumo e demanda de energia elétrica.

A presente invenção trata, basicamente, de um medidor eletrônico de energia
20 elétrica que incorpora software e componentes eletrônicos para armazenar um certificado digital e, através destes, disponibiliza dados eletronicamente assinados através de suas portas de comunicação de dados. Dessa forma, estes dados podem ser transportados até a concessionária distribuidora de energia elétrica com a garantia de não poderem ser alterados e, além disso, permitindo que sua origem seja verificada digitalmente, o que
25 garante dois aspectos fundamentais do processo de faturamento de consumo e demanda de energia elétrica, que interessam tanto à distribuidora de energia elétrica quanto aos consumidores, que são a garantia de que o dado pertence realmente ao medidor associado ao consumidor e a garantia que o dado não foi indevidamente alterado, modificado ou incorretamente anotado durante o processo de leitura. Com isso, é dada uma garantia real
30 tanto à distribuidora de energia elétrica quanto ao consumidor sobre a validade do dado que resultará na fatura de consumo e demanda de energia elétrica.

O uso de energia elétrica por residências, comércios e indústrias é uma característica da sociedade contemporânea cuja prática iniciou-se há mais de uma centena de anos. A medição de energia elétrica através de medidores é uma prática que começou
35 quase ao mesmo tempo. As primeiras patentes de invenção associadas a medidores eletromecânicos de energia elétrica foram solicitadas por Gardiner (1872) e Fuller (1878)

e, desde então, tem sido comum em todos os países do mundo a construção de redes de distribuição de energia elétrica onde, para cada consumidor, é instalado um medidor de energia elétrica na entrada da residência ou estabelecimento comercial ou industrial, destinado a registrar quanta energia elétrica foi utilizada pelo consumidor com a finalidade de possibilitar processos de cobrança. Desde sua invenção, os medidores de energia elétrica apresentam em seu painel frontal informações que permitem que o consumo em um dado período, por exemplo, 1 mês, seja aferido por processos de anotação manual e, mediante a contabilização cíclica, o valor adequado seja cobrado de cada consumidor.

Mais recentemente, com o advento da eletrônica, os medidores de energia elétrica passaram a ser eletrônicos, evitando o uso de engrenagens e mostradores analógicos em prol do uso de circuitos eletrônicos e mostradores digitais para apresentar os dados relativos ao consumo e a demanda de energia elétrica.

Nos medidores eletrônicos, além da leitura manual (verificação dos valores presentes nos mostradores digitais e sua anotação em papel ou dispositivos computacionais portáteis), tornou-se possível a aquisição de dados através de portas de comunicação presentes nos medidores e que, mediante processos eletrônicos (interfaces e protocolos digitais de dados), tornaram possível dispensar a escrita manual das informações. Tal recurso proporciona não apenas maior rapidez na leitura dos dados como também tende a eliminar o erro humano possível no processo de anotação manual.

Os processos eletrônicos presentes nos instrumentos de medição eletrônica geram, portanto, através de portas de comunicação eletrônicas e protocolos digitais dados que, em última instância, criam registros de dados que irão posteriormente ser inseridos em grandes bases de dados, dando origem ao faturamento de energia elétrica.

Embora a evolução desde os primeiros medidores eletromecânicos até os medidores eletrônicos de energia elétrica seja notável, e a redução – tanto nos erros metrológicos (o que é denotado basicamente pelo aumento da precisão dos medidores ao longo dos anos) quanto nos erros humanos de leitura manual dos valores medidos no processo de faturamento, a modernidade da medição eletrônica introduziu, no contexto de leitura para faturamento, novos problemas no cenário de leitura, faturamento e cobrança que envolvem as distribuidoras de energia elétrica e os consumidores.

Em primeiro lugar, o processo eletrônico de medição de energia elétrica – ao agregar a possibilidade de leitura dos dados de medição através de portas de comunicação, seja através de um coletor eletrônico portátil, seja através de qualquer dispositivo de coleta remota de informações (como por exemplo, modems digitais) para leitura à distância, operam através do conceito de protocolos digitais de dados. Estes protocolos permitem obter as informações guardadas internamente aos medidores mediante sequências de

comandos e respostas, no domínio da comunicação de dados, e – de maneira invariante, os dados transportados são levados desde o medidor até um ou mais computadores até que venha a ser introduzido no sistema de faturamento que fará o processamento de fatura do consumidor. Aí reside o primeiro problema do estado da técnica atual que precisa ser
5 solucionado: há inúmeras formas de *alterar*, proposital ou acidentalmente, os dados obtidos originalmente do medidor. Estas alterações, independentemente da motivação, irão ocasionar uma discrepância entre o dado original, entregue pelo medidor, e o dado efetivamente processado, gerando possíveis erros de faturamento que irão interferir negativamente no processo de distribuição de energia elétrica assim como no correto
10 atendimento ao consumidor.

Em primeiro lugar é sabido que erros de software, erros de operação, erros de transmissão de dados, assim como manipulações fraudulentas dos dados podem ocorrer e, a despeito da modernidade e precisão dos medidores eletrônicos, o processo de faturamento, tal como ocorria nos erros de leitura e escrita manual dos registradores dos
15 medidores eletromecânicos, torna-se comprometido. (A)

Em segundo lugar, os protocolos digitais de comunicação disponíveis nos medidores de energia elétrica foram concebidos para coordenar, mediante seqüências binárias de comunicação de perguntas e respostas, a troca de informação entre o medidor e um dispositivo de leitura, local ou remoto. Dentre os dados comunicados encontram-se, em
20 geral, as informações a respeito do medidor em si (número de série, parâmetros de operação, configurações, modelo, marca e fabricante, dentre outros) assim como as informações de medição (valor dos registradores de energia ativa e reativa, valores relativos à tensão, corrente, demandas máximas, dentre outras). Embora estas informações, à priori, pareçam ser suficientes para um processo de faturamento seguro, elas ignoram–
25 otimistamente, o primeiro problema já demonstrado, só que desta vez no caso das informações do medidor propriamente dito. Em outras palavras, tão possível quanto manipular, por erro ou intencionalmente, os dados de medição (leituras) é alterar a identificação do medidor em si. Isso torna possível uma grande nova gama de erros e fraudes de medição, uma vez que – com o conhecimento de como gerar as informações de
30 um medidor, pode-se criar as informações de medição, falsas, a partir – por exemplo, de um microcomputador. Isso equivaleria, no processo manual, a uma leitura fictícia gerada por um processo de falsificação de documentos, porém levado ao nível da eletrônica, muito mais complexo de ser percebido e administrado e que, potencialmente, poderia levar o caos completo à indústria de distribuição de energia elétrica – e consequentemente aos
35 consumidores.

Com os dados de um medidor de energia elétrica, pode-se rastrear – pelo número de

série, o medidor que gerou as informações originalmente. Porém, conforme exposto acima, o próprio número de série pode ser alterado nos arquivos de dados, fazendo com que este rastreamento seja frágil e não sirva ao propósito de aumentar a segurança do processo de maneira significativa. (B)

5 Em terceiro lugar, existe uma questão de natureza regulatória que é presente em praticamente todos os países do mundo, que diz respeito à segurança metrológica dos medidores de energia elétrica, representada através da verificação de cada modelo, tipo e fabricante de medidores de energia elétrica por um conjunto de regras regulatórias por uma Autoridade Metrológica. No Brasil, o INMETRO – Instituto Nacional de Metrologia
10 cumpre esta função e, de acordo com as regras vigentes, todo medidor de energia elétrica utilizado no processo de faturamento de consumidores deve ser submetido ao INMETRO para a realização de ensaios de aferição metrológica. Todo novo modelo, marca e tipo de medidor, assim como o próprio fabricante, são verificados pelo INMETRO para verificar se, de acordo com as especificações e exigências metrológicas, cumprem com as
15 exigências definidas por um documento conhecido como *RTM – Regulamento Técnico-Metrológico*, que define o mínimo a ser seguido em termos de metrologia, para corretamente atender ao mercado de aplicação dos medidores, concessionárias distribuidoras de energia elétrica e medidores.

Além de verificar o correto atendimento às regras de um medidor *novo*, o
20 INMETRO e possivelmente outras agências e instituições de regulação definem também procedimentos a serem seguidos em, no mínimo, três outras situações: quando da reclamação de um consumidor a respeito de um valor medido (são definidos procedimentos a serem seguidos pela distribuidora e pelo consumidor para a aferição do correto funcionamento do medidor), quando da retirada de um medidor de sua instalação
25 em campo para manutenção (são definidos regulamentos a serem seguidos pela distribuidora e por empresas prestadoras de serviço de manutenção e fabricantes de medidores para certificar o correto funcionamento do medidor após uma manutenção) e, finalmente, de acordo com cada tipo de aplicação do medidor, quando ele deve sofrer novas aferições para verificar que seu desempenho não sofreu degradação com o passar do
30 tempo.

No estado da técnica atual, os procedimentos metrológicos são realizados mediante uma série de documentações, verificações e processos de auditoria. O consumidor é informado da correta execução de todos os procedimentos legais e regulatórios mediante um *selo* identificando o medidor perante a Autoridade Metrológica que é, em geral,
35 impresso ou colado ao medidor.

É desnecessário argumentar que, muito embora os fabricantes de medidores, os

consumidores, as distribuidoras de energia elétrica e a própria Autoridade Metrológica sejam todas instituições ou pessoas físicas de reconhecida idoneidade – formando o que chamamos *Sociedade*, os processos manuais, procedimentos administrativos e *selos* adesivos ou impressos aos medidores conferem pouca segurança ao complexo ciclo de vida de um medidor de energia elétrica.

É comum o fato de existirem medidores de energia elétrica instalados em um grande número de residências e estabelecimentos comerciais e industriais com mais de 30 anos de uso sem sofrer qualquer verificação metrológica. Isto se deve ao fato, inclusive, de existir uma dificuldade natural em instalar e manter um grande número de medidores em campo e, por consequência, dar a estes medidores o tratamento regulatório devido. Este fato agrava-se, uma vez que *selos*, impressos ou colados aos medidores são passíveis de adulteração, o que pode ser realizado com o propósito fraudulento de introduzir propositalmente erros de medição, causando – novamente, erros no processo de faturamento. Existem centenas de milhões de medidores de energia elétrica instalados no mundo e é improvável que todos eles estejam em total concordância com as regras metrológicas existentes em cada um dos países onde estão instalados. O mais provável é que exista uma parcela significativa de medidores em discordância com as regras metrológicas prejudicando consumidores e concessionárias distribuidoras de energia elétrica por todo o mundo, gerando perdas comerciais que são – em praticamente todos os países do mundo, rateadas para todos os consumidores. (C)

Certificação Digital é o nome dado para um conjunto de técnicas computacionais, em geral realizadas de maneira segregada em um circuito integrado (*chip*) – tal como os usados nos cartões bancários do tipo *smart-card*, associadas à tecnologia de chaves públicas. Estas técnicas e tecnologia permitem: a) estabelecer um par de chaves (valores numéricos) para um determinado *chip*, sendo uma chave pública (que virá a ser dado o conhecimento a qualquer interessado) e uma chave privada (que reside exclusivamente no *chip* ou *smart-card*). Este par de chaves, através de um conjunto de algoritmos e funções computacionais, num padrão conhecido como X.509 ou ICP – *Infraestrutura de Chaves Públicas*, proporcionam funções de Assinatura (geração de um código matemático que sintetiza de maneira unívoca um conjunto de dados) e Criptografia (cifra de um conjunto de dados por algoritmos de criptografia diversos). Estas funções, juntas, estabelecem um contexto de segurança que proporciona dois recursos importantes para as transações eletrônicas: sigilo e não-repúdio. Sigilo, estabelecido pela cifra de dados a partir de um remetente (A) para um destinatário (B) utilizando, por parte de (A) a chave pública de (B) de tal sorte que apenas (B), de posse de sua chave privada, pode decifrar os dados. Não-repúdio, estabelecido por uma assinatura digital de dados a partir de um remetente (A)

utilizando sua chave privada para cifrar um resumo (*hash*) do conteúdo enviado para um destinatário (B) de tal sorte que (B) possa, decifrando a assinatura digital (obtendo o *hash* gerado pelo remetente) e, gerando ele próprio um *hash* pelo mesmo algoritmo, comparar ambos os valores e, em caso de coincidência, obter confirmação de que o dado enviado por (A) não sofreu alteração até chegar em (B).

A Certificação Digital tem sido utilizada, com sucesso, por instituições financeiras, pela rede de computadores mundial (Internet) e instituições públicas e privadas no mundo todo para conferir segurança às transações eletrônicas.

Por sua estrutura hierárquica de emissão de “Certificados Digitais”, que são documentos eletrônicos gerados por uma “Autoridade Certificadora”, a Certificação Digital é especialmente adequada para substituição dos processos documentais e foi adotada em diversos países, incluindo o Brasil, como base tecnológica para garantia de transações eletrônicas realizadas na rede mundial de computadores (Internet). No Brasil, especialmente, o ITI – Instituto Nacional de Tecnologia da Informação, ligado diretamente à Presidência da República, instituiu o ICP-Brasil (Infraestrutura de Chaves Públicas do Brasil) para regular a emissão de certificados digitais, instituir as autoridades certificadoras brasileiras e, mediante legislação específica, atribuir equivalência às transações eletrônicas realizadas sob a égide da Certificação Digital àquelas realizadas em papel. Assim é que, desde o ano de 2002, a certificação digital tem servido de base para – por exemplo, o Sistema de Pagamentos Brasileiros (SPB), que trata da interconexão do sistema bancário ao Banco Central do Brasil, com isso reduzindo os riscos financeiros associados ao giro econômico brasileiro e trazendo inúmeros benefícios para o país.

A Certificação Digital foi concebida para tratar da segurança das transações eletrônicas entre pessoas e instituições públicas ou privadas utilizando redes de computadores.

A presente invenção foi concebida, por um lado, para estabelecer padrões mais seguros para concessionárias distribuidoras e consumidores no que diz respeito à coleta da informação de medidores eletrônicos de energia elétrica e, por outro lado, para colaborar com a Autoridade Metrológica e Entidades Reguladoras do processo de distribuição de energia elétrica com mecanismos mais eficazes para a qualificação e o controle dos instrumentos de medição por elas certificados e homologados.

De acordo com estes objetivos, a invenção é apresentada a seguir com descrição detalhada de cada componente fazendo-se referência às folhas de desenhos anexas.

A presente invenção não se trata nem de um medidor eletrônico de energia elétrica nem do uso de certificação digital para comunicação de dados, mas de ambos utilizados em conjunto, de forma a concretizar os objetivos acima expostos em sua totalidade e de forma

absolutamente inovadora.

A Figura 1 apresenta o diagrama esquemático de um medidor de energia elétrica tendo como seus componentes principais: a presença de sensores de corrente 1(a), a presença de sensores de tensão (b), a existência de um circuito eletrônico (c) para
 5 acondicionar os sinais de corrente e tensão nos níveis elétricos exigidos pela unidade de processamento (d), uma unidade de processamento (d) capaz de realizar amostragem contínua dos sinais de corrente e tensão proporcionados pelo circuito (c) e que refletem, mediante uma relação conhecida, o valor real da corrente e tensão entregues nos terminais de conexão do medidor. A unidade de processamento (d) realiza o cálculo de energia ativa
 10 e reativa passantes e determina os valores de energia a contabilizar. Uma unidade de comunicação (e), associada à unidade de processamento (d) e que, mediante um protocolo digital de dados e uma interface física relaciona-se com o mundo exterior ao medidor (usuários e dispositivos de comunicação remotos). Uma unidade de processamento de funções de certificação digital (f) que se interpõe entre a unidade de processamento (d) e a
 15 unidade de comunicação (e). Esta Unidade de Processamento de Funções de Certificação Digital (UPFCD) tem por função realizar a criptografia e a assinatura de todos os dados que são disponibilizados, através do protocolo de dados da unidade de comunicação (e) ao mundo externo, de forma que o relacionamento eletrônico com o medidor no tocante à comunicação de dados passa a ser regido pelo uso da técnica da Certificação Digital de
 20 forma nativa e não dissociável.

A Figura 2 apresenta o medidor eletrônico, uma vez concebido em diferentes modelos (para medição de diferentes tipos de consumidores, desde o porte residencial até o porte industrial) em um fluxo que demonstra seu ciclo de vida do ponto de vista de (a) projeto, (b) produção das unidades de referência, (c) apresentação do medidor à Autoridade
 25 Metrológica para *Apreciação e Aprovação Técnica de Modelo* (reconhecimento e homologação da Autoridade Metrológica quanto à aplicabilidade do instrumento em processos oficiais de medição para faturamento), (d) solicitação de compra, proveniente de um comprador (em geral uma distribuidora de energia elétrica, mas essencialmente, qualquer empresa ou cidadão autorizado a utilizar o instrumento para medição com
 30 finalidade de faturamento), (e) a emissão de certificados digitais a partir de solicitação do comprador à Autoridade Metrológica para medidores que já tenham sido homologados, (f) a carga dos certificados digitais nos medidores comprados pelo comprador, (g) a utilização de medidores eletrônicos com seus respectivos certificados digitais nos processos reais de medição para faturamento.

35 Neste ponto, faz-se necessário descrever detalhadamente o fluxo da Figura 2. A fase apresentada na Figura 2(a) relacionada ao projeto do instrumento não é específica, e

pressupõe apenas que o medidor concebido é tal que respeita o diagrama esquemático apresentado na Figura 1, ou seja, utiliza componentes eletrônicos capazes de suportar as funções de certificação digital (armazenar um certificado digital, chaves públicas e privadas associadas ao certificado, cifrar, decifrar e assinar dados eletronicamente).

5 A fase apresentada na Figura 2(b) relaciona-se ao período de tempo em que o medidor – já concebido e com seu processo de fabricação definido e exercitado (até o ponto que for de interesse do fabricante) ainda não possui – na terminologia da Autoridade Metrológica brasileira (INMETRO), uma *Aprovação de Técnica de Modelo*. Tomando-se por base a terminologia adotada no Brasil e válida no contexto da OIML (Organização
10 Internacional de Metrologia Legal), todo instrumento de medição, medida materializada ou parte destes, objeto de regulamentação metrológica – seja fabricado no Brasil ou importado, deve obter a aprovação de seu modelo, de acordo com o regulamento técnico metrológico pertinente, antes de ser posto no mercado para comercialização ou uso.

Ainda de acordo com o INMETRO, a aprovação de modelo é uma decisão de
15 caráter legal baseada no relatório de apreciação técnica de modelo (ATM) reconhecendo que o modelo de um instrumento de medição satisfaz às exigências regulamentares e pode ser utilizado no campo regulado fornecendo resultados confiáveis, durante um período de tempo definido.

Assim, a fase apresentada na Figura 2(c) representa o conjunto de ações através das
20 quais um fabricante ou equivalente apresenta ao INMETRO um modelo para ser objeto de uma ATM. Nesta invenção, como parte integrante, está a consideração de que – de fato, a Autoridade Metrológica e a Autoridade Certificadora são, na verdade, complementares e que, o certificado digital emitido para um instrumento de medição requer antecipadamente que o instrumento tenha sido previamente recebido sua Aprovação Técnica de Modelo para
25 efeito cadastral. Como consequência, em uma futura emissão de certificado digital, este será emitido apenas para instrumentos que previamente tiverem recebido ATM, dentro de um padrão de certificado que contenha – no certificado digital, os dados que são do interesse da Autoridade Metrológica tal como nome do modelo, nome do fabricante, identificação da concessionária distribuidora de energia elétrica solicitante e prazo de
30 validade da certificação, todos de acordo com a definição raiz do próprio processo de Aprovação Técnica de Modelo. Como consequência, pode-se dizer que o certificado digital confere ao instrumento um *selo* – não apenas impresso ou colado ao seu exterior, mas *inserido* de forma a estar presente em todas as comunicações referentes ao instrumento em sua utilização em campo.

35 Os certificados digitais só existem após terem sido solicitados por um comprador para uso em um conjunto (quantidade e modelo) definido de instrumento de medição. Por

este motivo, a Figura 2(d) apresenta uma solicitação de compra a um fabricante de medidores. Considerando as exigências legais estabelecidas pela Autoridade Metrológica, a ordem de compra de medidores cuja finalidade de utilização é regulamentada deverá ser também acompanhada de uma solicitação à própria Autoridade Metrológica para emissão dos certificados competentes (quantidade e modelo).

A Figura 2(e) apresenta a fase em que a Autoridade Metrológica, tendo verificado a validade da solicitação de emissão de certificados digitais realiza sua emissão, entregando os certificados digitais ao solicitante que, por sua vez concretizará sua carga nos medidores, conforme a fase apresentada na Figura 2(f).

A Figura 2(g), apresenta a utilização do medidor em campo, de tal sorte que todas as suas comunicações serão cifradas e assinadas conforme a técnica da certificação digital. Dadas as dificuldades anteriormente apresentadas com o estado atual da técnica, a Figura 2(g) tem como grande avanço e conteúdo inovador o fato de que o prazo de validade do certificado digital atribuído ao instrumento emitido conforme a norma específica da Aprovação Técnica de Modelo definida pela Autoridade Metrológica, poderá ser verificado em toda e qualquer comunicação de dados com o medidor. Como consequência, todo instrumento de medição com um certificado digital terá – de forma indelével, irretratável e inegável característica de prazo de validade atribuído, em sua raiz, pela Autoridade Metrológica, resolvendo de maneira cabal um dos problemas anteriormente descrito (C).

A Figura 3 apresenta um diagrama de utilização de um medidor com seu respectivo certificado digital, onde: (a) apresenta uma solicitação proveniente de coletor de dados ou dispositivos de comunicação remota para dados de medição, (b) apresenta a composição dos dados (pacote) que serão respondidos pela unidade de processamento interna ao medidor, (c) apresenta o tratamento do pacote de dados pela unidade UPFCD – o que confere ao pacote a criptografia e a assinatura digital (pacote cifrado e assinado), (d) apresenta a entrega do pacote cifrado e assinado à unidade de comunicação (porta de comunicação) que o entrega ao mundo exterior ao medidor.

A Figura 4 apresenta (a) as técnicas de criptografia (cifra e decifra) e (b) assinatura digital de um pacote de dados.

De acordo com a técnica ICP (*Infraestrutura de Chaves Públicas*), os dados cifrados e assinados eletronicamente são garantidos a respeito de sua origem. Isto significa que o destinatário dos dados (em última instância, a concessionária distribuidora de energia elétrica) tem condições de verificar a assinatura existente no pacote de dados recebidos e, mediante sua validação, confiar em sua origem. Desta forma, a presente invenção confere aos dados uma característica de rastreamento de dados até a sua origem (o medidor) à

concessionária distribuidora de energia elétrica (o destinatário da informação) que, no estado da técnica atual simplesmente não existe, resolvendo de maneira cabal outro dos problemas anteriormente descritos (B).

Finalmente, e ainda de acordo com a técnica ICP (*Infraestrutura de Chaves Públicas*), os dados cifrados e assinados são garantidos a respeito de seu conteúdo. Isto significa que o destinatário dos dados tem condições de verificar a assinatura existente no pacote de dados recebidos e avaliar se o conteúdo transmitido condiz com o originalmente postado pelo remetente (o medidor) ou se sofreu alteração no trajeto. Uma vez assegurado, mediante validação o conteúdo da comunicação, a concessionária distribuidora de energia elétrica (o destinatário da informação) tem a segurança necessária para aceitar a informação como válida e – portanto, proceder ao faturamento do consumidor para o qual o dado destina-se. Esta característica resolve de maneira cabal outro dos problemas anteriormente descrito (A).

De maneira absolutamente inovadora, a presente invenção resolve ainda uma série de problemas colaterais associados ao processo de faturamento de energia elétrica. Qualquer consumidor pode exigir - além do já atualmente disponível processo de aferição de um medidor de energia, a comprovação digital de que seu faturamento baseia-se em um dado assinado eletronicamente por seu medidor. Assim, o consumidor poderá, de forma equivalente à distribuidora de energia elétrica, ter a segurança inequívoca de que seu faturamento foi originado pelo medidor que se encontra instalado em sua residência ou estabelecimento comercial ou industrial.

Igualmente, toda contenda judicial relacionada ao processo de medição poderá, em seu processo de perícia, basear-se estritamente nos aspectos metrológicos da medição, uma vez que para as questões de adequação da medição e correção do processo de comunicação dos dados até seu processamento, a certificação digital oferecerá as ferramentas necessárias para validação do procedimento.

A Autoridade Metrológica poderá, mediante Aprovação Técnica de Modelo, estabelecer o padrão de certificado digital (conteúdo e prazo de validade a partir da emissão) a ser usado em cada instrumento instalado em campo, com isso gerando – de maneira objetiva e verificável, a correta aplicação da regulamentação associada ao medidor. Isso inclui não apenas o prazo de validade, mas vários outros aspectos que podem afetar um instrumento de medição posto à venda no mercado, inclusive o descredenciamento de modelos ou fabricantes. Um instrumento de medição previamente aprovado (ATM) cujo fabricante, posteriormente, deixe de cumprir as exigências legais, pode não apenas ter a emissão de novos certificados digitais negada, como certificados emitidos podem – dentro da técnica ICP, ser revogados, de forma que sua aplicação em

campo seja – automática e centralizadamente (sob o controle da Autoridade Metrológica) invalidada, garantindo para os consumidores que apenas instrumentos que estejam em conformidade com a regulamentação sejam efetivamente utilizados e conferindo segurança ao processo comercial de distribuição de energia elétrica.

REIVINDICAÇÕES

1. Medidor eletrônico de energia elétrica com mecanismo integrado de certificação digital para comunicação segura, caracterizado por compreender:

sensores de corrente 1(a),

sensores de tensão (b),

circuito eletrônico (c) para acondicionar os sinais de corrente e tensão nos níveis elétricos exigidos pela unidade de processamento (d),

unidade de processamento (d) capaz de realizar amostragem contínua dos sinais de corrente e tensão proporcionados pelo circuito (c) e que refletem, mediante uma relação conhecida, o valor real da corrente e tensão entregues nos terminais de conexão do medidor, a unidade de processamento (d) realiza o cálculo de energia ativa e reativa passantes e determina os valores de energia a contabilizar e uma unidade de comunicação (e), associada à unidade de processamento (d), que mediante um protocolo digital de dados e uma interface física relaciona-se com o mundo exterior ao medidor, e

unidade de processamento de funções de certificação digital (f) que se interpõe entre a unidade de processamento (d) e a unidade de comunicação (e), em que a unidade de processamento de funções de verificação digital (UPFCD) tem por função realizar a criptografia e a assinatura de todos os dados que são disponibilizados, através do protocolo de dados da unidade de comunicação (e) ao mundo externo, de forma que o relacionamento eletrônico com o medidor no tocante à comunicação de dados passa a ser regido pelo uso da técnica da certificação digital de forma nativa e não dissociável.

2. Medidor, de acordo com a reivindicação 1, caracterizado por a unidade de processamento de funções de verificação digital (UPFCD) realizar funções de criptografia e assinatura digital conforme tecnologia da Infraestrutura de Chaves Públicas.

3. Medidor, de acordo com a reivindicação 1, caracterizado por os certificados digitais conterem informações sobre fabricante, modelo, usuário, nome da concessionária distribuidora de energia elétrica solicitante e prazo de validade relacionado à Aprovação Técnica de Modelo relacionado ao medidor para posterior rastreamento no processo, garantindo a validade do instrumento de medição no momento em que ocorre seu uso para a finalidade de faturamento.

4. Medidor, de acordo com a reivindicação 1, caracterizado por permitir a validação dos dados recebidos pela concessionária em qualquer processo de comunicação de dados originados nas portas de comunicação do medidor.

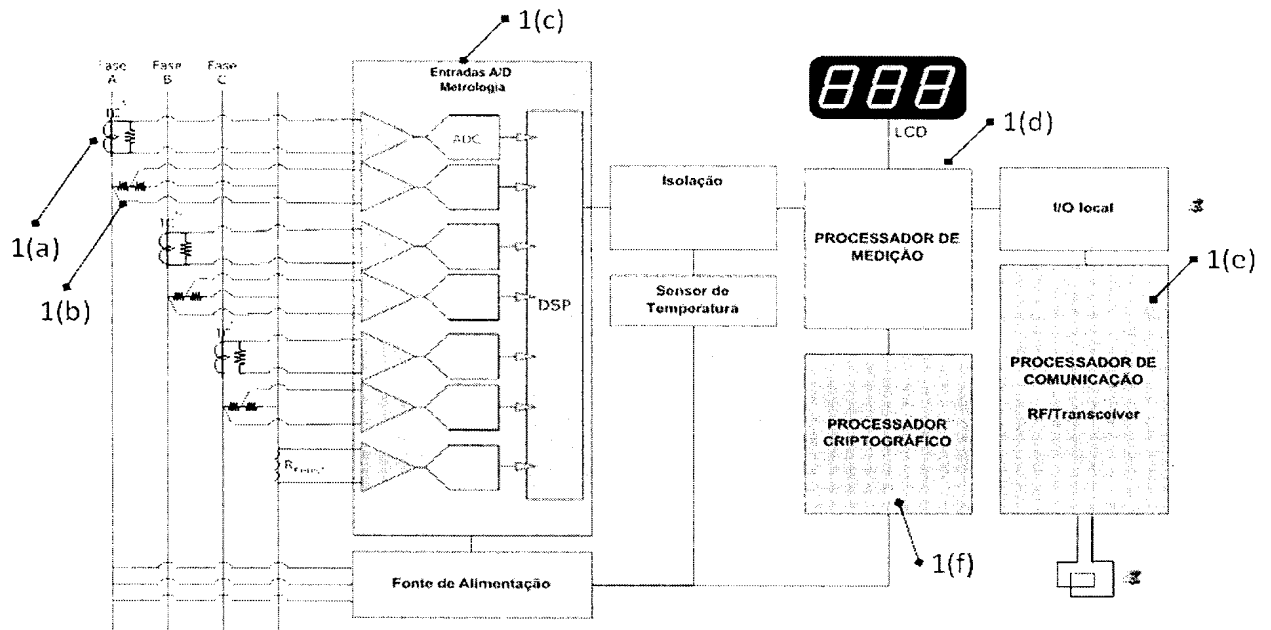


FIGURA 1

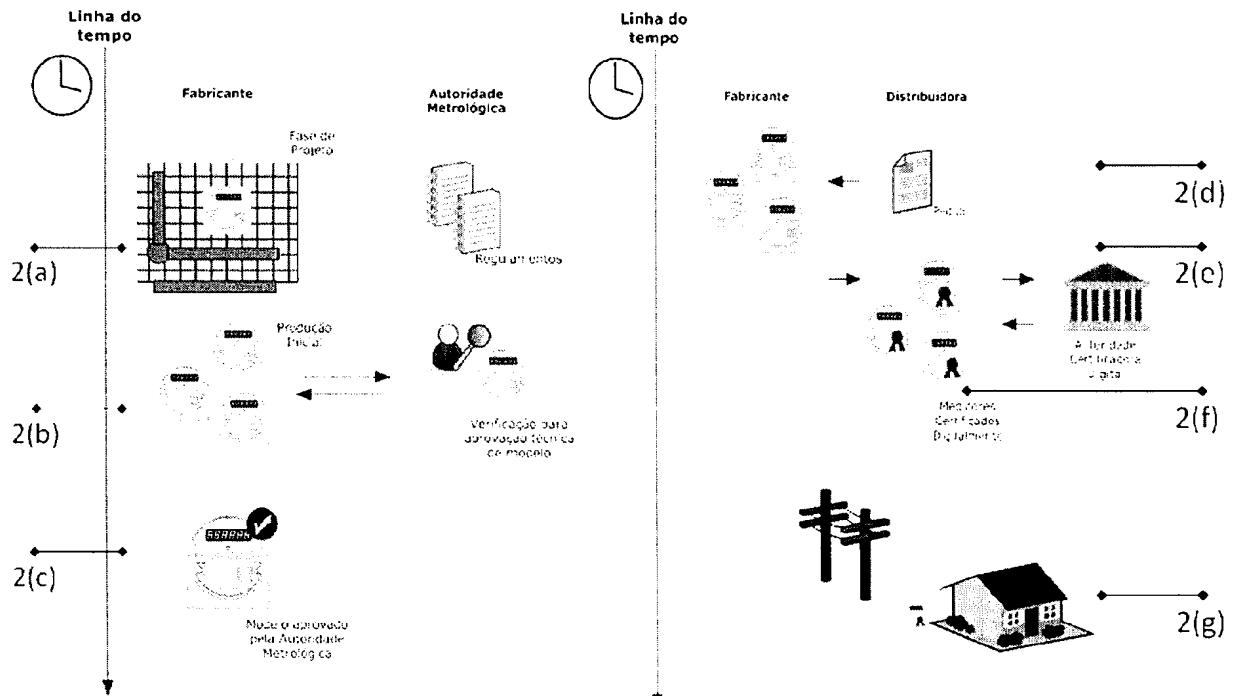


FIGURA 2

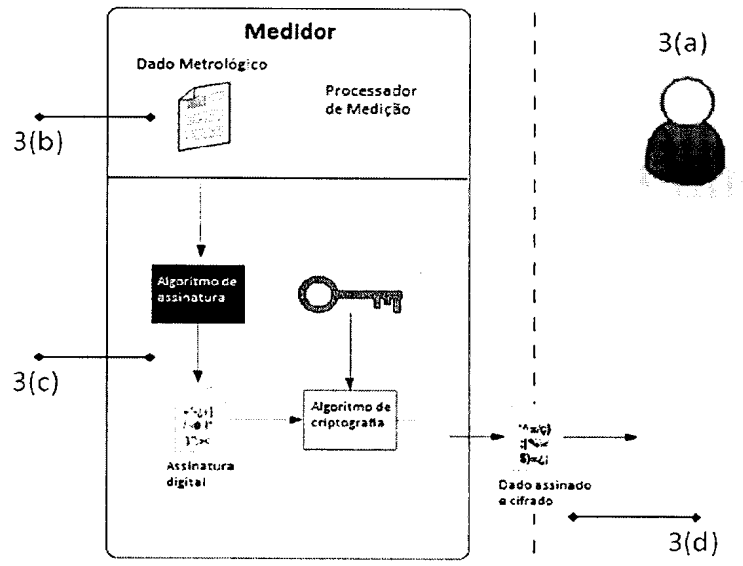


FIGURA 3

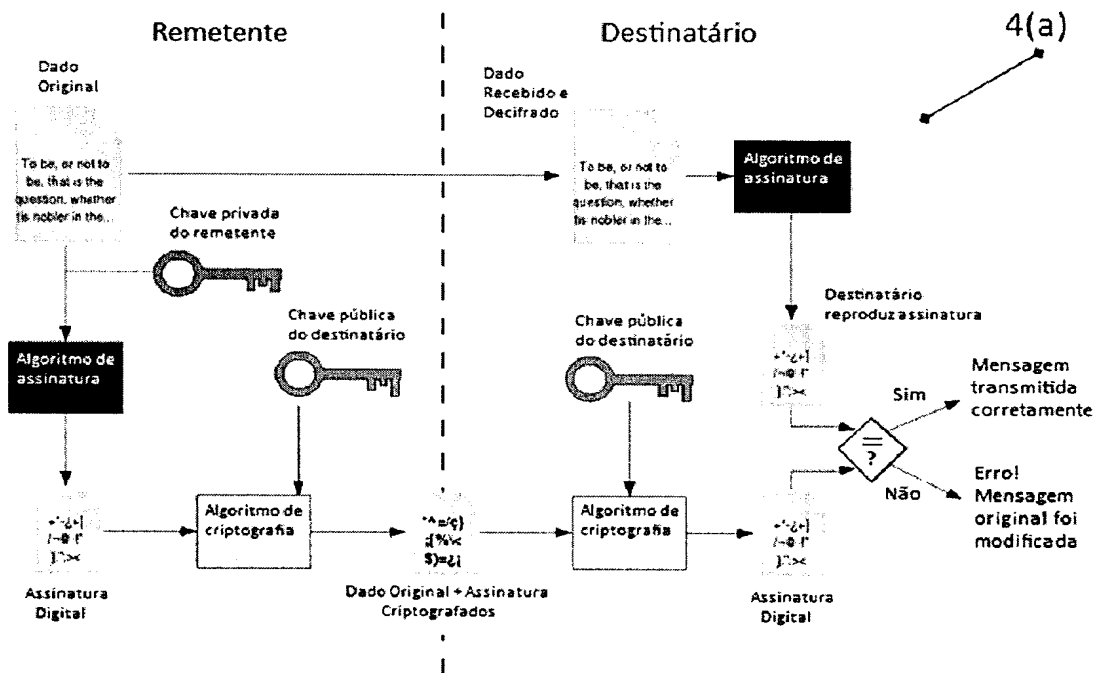


FIGURA 4

RESUMO**MEDIDOR ELETRÔNICO DE ENERGIA ELÉTRICA COM MECANISMO INTEGRADO DE CERTIFICAÇÃO DIGITAL PARA COMUNICAÇÃO SEGURA**

Medidor eletrônico de energia elétrica com mecanismo integrado de certificação digital para comunicação segura, compreendendo sensores de corrente 1(a), sensores de tensão (b), circuito eletrônico (c) para acondicionar os sinais de corrente e tensão nos níveis elétricos exigidos pela unidade de processamento (d), unidade de processamento (d) capaz de realizar amostragem contínua dos sinais de corrente e tensão proporcionados pelo circuito (c) e que refletem, mediante uma relação conhecida, o valor real da corrente e tensão entregues nos terminais de conexão do medidor, a unidade de processamento (d) realiza o cálculo de energia ativa e reativa passantes e determina os valores de energia a contabilizar e uma unidade de comunicação (e), associada à unidade de processamento (d), que mediante um protocolo digital de dados e uma interface física relaciona-se com o mundo exterior ao medidor, e unidade de processamento de funções de certificação digital (f) que se interpõe entre a unidade de processamento (d) e a unidade de comunicação (e), em que a unidade de processamento de funções de verificação digital (UPFCD) tem por função realizar a criptografia e a assinatura de todos os dados que são disponibilizados, através do protocolo de dados da unidade de comunicação (e) ao mundo externo, de forma que o relacionamento eletrônico com o medidor no tocante à comunicação de dados passa a ser regido pelo uso da técnica da certificação digital de forma nativa e não dissociável.