Certificação Digital como Ferramenta de Segurança para Medidores Inteligentes

Wilson Melo, Raphael Machado,
Bruno Abreu e Luiz Rust Carmo
Instituto Nacional de Metrologia, Qualidade e Tecnologia
Rio de janeiro - RJ
Email: {wsjunior,rcmachado,beabreu,lfrust}@inmetro.gov.br

Ruy Ramos
Instituto de Tecnologia da Informação
Brasília - DF
Email: ruy@iti.gov.br

***Resumo*—In this paper, we present a digital certificate-based solution for smart meters. Our propose meets the identification requirements found in several scenarios related to Legal Metrology. Also, it extends previous models of smart meters authentication. This proposal results in a new class of digital certificate called "Metrologic Objects Digital Certificate."The ICP-Brasil Management Committee recently approved the use of these certificates. Fuel dispensers are the first implementation case. The objective is to reduce tampering on these instruments, so increasing their reliability.**

I. Introdução

Certificação digital é a associação, realizada por uma parte confiável, entre uma chave pública de uma entidade e a identificação daquela entidade [1]. Na prática, a certificação digital permite que se tenha confiança nas assinaturas digitais geradas por uma entidade, funcionando como um mecanismo de apoio a protocolos de identificação e autenticação.

Embora o uso de certificados digitais esteja tradicionalmente associado a uma pessoas física ou jurídica, os requisitos de autenticação e identificação estão presentes em diversos cenários envolvendo o uso de dispositivos inteligentes. Uma área em que os requisitos de autenticação e identificação são particularmente interessantes é a área de Metrologia Legal [2]. Medidores inteligentes são dispositivos que operam, na maior parte do tempo, de forma autônoma, muitas vezes, em ambientes hostis, e gerando informações de interesse financeiro e legal. Dessa forma, tais medidores são, frequentemente, objetos de ataques de segurança objetivando adulterar os dados por eles gerados [3], [4]. A capacidade de proteger a integridade de tais dados, portanto, é de importância central para o equilíbrio das relações baseadas em tais medidores.

Historicamente, observa-se diferentes abordagens para a implementação de protocolos de identificação e autenticação de medidores inteligentes [5]. Tais iniciativas, no entanto, apresentam limitações relacionadas ao uso de modelos simplificados de gerenciamento de chaves. No presente trabalho, é descrito como o uso de assinaturas e certificados digitais contribui para a proteção das medições realizados por um medidor inteligente. Inicialmente, são introduzidos os principais conceitos relacionados à segurança cibernética de medidores inteligentes, no âmbito da Metrologia Legal. Em seguida, discute-se a adoção de certificados digitais específicos para dispositivos de medição, e como os mesmos agregam confiabilidade ao processo de medição, tornando-se uma ferramenta de apoio às atividades da metrologia legal. Por fim, apresentamos um modelo baseado no uso de Infraestruturas de Chaves Públicas (ICP), inclusive com a proposta de um novo tipo de certificado digital que passou a integrar a lista de certificados digitais oficiais da ICP-Brasil. A proposta está sendo implementado na construção de novos modelos de *medidores de combustível*, com o objetivo de dificultar ataques de segurança e reduzir riscos de fraude.

II. Preliminares

A. Metrologia legal e segurança de medidores inteligentes

A Metrologia Legal é responsável por prover a confiança nas medições de grandezas físicas em relações que envolvem o consumo de determinado bem mensurável, segurança e a proteção à vida e integridade das pessoas [4], [6]. Tal confiança está fortemente baseada em atividades que visam garantir a confiabilidade dos instrumentos de medição utilizados em diferentes aplicações. As atividades relacionadas à Metrologia Legal visam a realização ensaios de *apreciação de modelos* de instrumentos, bem como a inspeção e verificação desses instrumentos *a posteriori*, seja em chão de fábrica ou em campo, em um conjunto de práticas denominado *supervisão metrológica*.

No mundo todo, a execução das atividades associadas à Metrologia Legal tem se tornado um desafio crescente, especialmente em relação aos *instrumentos de medição controlados por software*. Devido à inserção de novas tecnologias da informação, tais instrumentos apresentam maior complexidade e introduzem importantes questões relacionadas à segurança cibernética [5], [4]. A garantia de integridade de dados e programas, a proteção de informações sensíveis, a privacidade, e a disponibilidade de instrumentos de medição conectados à Internet, são algumas das preocupações que se tornaram latentes nos últimos anos. Especialmente nos países em desenvolvimento, tal desafio torna-se ainda mais complexo em função da rápida inserção desses instrumentos em diferentes cenários de uso, bem como devido ao elevado número de fraudes associadas a esses instrumentos. Estudos apontam que, apenas no Brasil, o prejuízo causado à sociedade em função de fraudes em medições é da ordem de US$ 300

milhões por ano [6]. Essas fraudes geralmente ocorrem quando uma entidade maliciosa tenta adulterar as respostas fornecidas por um instrumento de medição, obtendo assim vantagens indevidas na comercialização de um determinado bem.

O Brasil tem um histórico de mais de 10 anos na apreciação de modelo e supervisão metrológica de instrumentos de medição controlados por software. Dentro do arcabouço brasileiro de metrologia legal, instrumentos de medição são regulamentados a partir de Regulamentos Técnicos Metrológicos (RTMs)[1] que definem requisitos que devem ser verificados durante a apreciação de modelo, bem como diretivas a serem observadas em atividades de supervisão metrológica. Desde 2007, o Inmetro publica RTMs que incluem requisitos específicos para a proteção do software embarcado em instrumentos de medição. Os primeiros RTMs abordando esse escopo foram direcionados a Sistemas Centralizados de Medição (SMCs) [5] de energia. Posteriormente, novos RTMs foram propostos para instrumentos com arquiteturas especiais. Estes RTMs são fortemente baseados nos guias WELMEC 7.2 [7], usado como base para diretivas de regulamentação pela União Europeia; e no OIML D 31 [8], que constitui um dos principais documentos orientativos sobre requisitos gerais para instrumentos de medição controlados por software. Ambos os documentos apresentam requisitos e diretivas de avaliação do *software legalmente relevante*, definido como as partes do software que determinam ou manipulam informações metrológicas (i.e., medições) ou legais (i.e., dados que complementam as medições).

A elaboração de um RTM sempre considera aspectos críticos na garantia de funcionalidade de um determinado instrumento. Na prática, a definição de quais requisitos devem ser exigidos por regulamentação envolve uma análise de risco [4]. Questões de segurança cibernética são endereçadas de modo a se obter um equilíbrio entre o nível de segurança desejado, os riscos e ataques associados ao instrumento, e também a nível de desenvolvimento da indústria para absorver um maior ou menor grau de complexidade no desenvolvimento e utilização de cada instrumento de medição. Em geral, os reguladores buscam pelas melhores práticas, que propiciem o máximo de benefícios com o menor impacto. Deste modo, requisitos de segurança cibernética são inseridos de acordo com necessidades claras relacionadas à proteção do software embarcado no instrumento, dos dados e processos manipulados por este software, e do vetor de ataques assumido como realístico na utilização do instrumento.

B. Assinatura digital, certificados digitais e a ICP-Brasil

A assinatura digital constitui uma das principais aplicações da criptografia de chave pública, ou criptografia assimétrica [1]. Ela se caracteriza por garantir a autenticidade, integridade e irrefutabilidade (não repúdio) de uma dada informação. A autenticidade deriva imediatamente do uso do par de chaves assimétricas. Isso porque qualquer informação verificável por meio de uma chave pública tem sua origem intrinsecamente ligada à entidade que possui a respectiva chave privada, permitindo assim a identificação e autenticação desta entidade. A integridade, por sua vez, vem da encriptação de um resumo criptográfico da informação. Por fim, a irrefutabilidade depende do uso de um certificado digital, que nada mais é do que a atestação por uma terceira parte confiável de que determinada chave pública pertence à respectiva entidade.

Autenticidade e integridade estão diretamente ligadas ao simples uso de um algoritmo de criptografia de chave pública e um algoritmo de *hash*. A irrefutabilidade, por sua vez, depende de uma infraestrutura de gestão de certificados digitais, também conhecida como Infraestrutura de Chaves Públicas (ICP). No contexto de uma ICP, três papéis são de fundamental importância para se garantir o devido funcionamento de sistemas baseados em assinaturas digitais:

- Autoridade Certificadora (AC): é a autoridade responsável pela emissão, distribuição, renovação, revogação e gerenciamento dos certificados digitais. Na prática, a AC é responsável por assinar os certificados digitais com sua própria chave privada, atestando assim a correspondência destes às suas respectivas entidades.
- Autoridade de Registro (AR): é a autoridade responsável pela interface entre a AC e entidade interessada em ter um certificado digital (usuário). A AR tem a função de receber, validar e encaminhar solicitações de um usuário para a AC.
- Autoridade Certificadora Raiz (AC-Raiz): é a primeira autoridade da cadeia de certificação, responsável por fiscalizar e auditar outras ACs e ARs. Sendo ela mesma uma AC, é também responsável pela emissão, distribuição, renovação, revogação e gerenciamento dos certificados digitais das demais ACs.

A ICP-Brasil implementa a ICP oficial brasileira, constituindo uma cadeia de confiança hierárquica para a emissão de certificados digitais e identificação virtual de pessoas físicas e jurídicas. Dentro do modelo ICP-Brasil, a função de AC-Raiz cabe ao Instituto de Tecnologia da Informação (ITI)[2], que também é o responsável por credenciar e descredenciar as demais entidades participantes da cadeia (i.e., ACs e ARs).

C. Assinatura digital em instrumentos de medição

Embora o uso de assinatura digital, bem como de certificados digitais, seja um tema amplamente consolidado no contexto de segurança da informação, o mesmo constitui uma prática relativamente recente em aplicações envolvendo instrumentos de medição.

Trabalhos correlatos são encontrados em aplicações diversas envolvendo sensores e dispositivos IoT (Internet of Things) [9], [10].O uso de criptografia de chave pública e também de certificados digitais é amplamente difundido em soluções de segurança para tais aplicações. Tal abordagem é justificada pelo simples fato de se aplicar um modelo extremamente consolidado em outros cenários envolvendo redes e sistemas

[1] http://www.oconsumidor.gov.br/metlegal/legislacao-metrologica-em-vigor.asp

[2] https://www.iti.gov.br

computacionais. Todavia, existem também aspectos negativos a serem considerados. A complexidade inerente à manutenção de uma ICP, bem como o custo computacional associado ao uso de algoritmos criptográficos, justifica o reaproveitamento de infraestruturas já existentes [9] ou ainda a implementação de soluções de certificação digital simplificadas [10], visando a redução do custo computacional em dispositivos que apresentam restrições nesse quesito.

Por sua vez, o uso de certificados digitais em instrumentos de medição ainda é pouco comum. O WELMEC 7.2 o OIML D 31 fazem menção ao conceito de *assinatura de chave pública*, argumentando que chaves assimétricas podem ser usadas para prover autenticidade e integridade dos registros legalmente relevantes de um instrumento. Todavia, esses guias não fazem qualquer referência ao uso de certificados digitais, que seriam necessários para se garantir a irrefutabilidade de uma assinatura de chave pública. Entre os exemplos de uso da assinatura de chave pública em instrumentos de medição é possível citar Jager et al. [11], que emprega essa tecnologia para proteger informações legalmente relevantes geradas por radares de velocidade de veículos, e o trabalho de Boccardo et al. [12] que descreve esse tipo de assinatura como um mecanismo viável para proteção de medições realizadas por esfigmomanômetros. No Brasil, os RTMs associados a radares de velocidade, bem como a regulamentação de REPs, estabelecem o uso de assinaturas de chave pública como requisitos obrigatórios para essas classes de instrumentos.

III. Modelo Proposto

Neste trabalho, apresentamos um modelo de regulamentação que introduz requisitos associados ao uso de certificados digitais ICP-Brasil em instrumentos de medição controlados por software. Tais requisitos constituem um mecanismo para se prover integridade, autenticidade e irrefutabilidade dos dados e processos gerenciados por um instrumento, dentro de uma cadeia de confiança hierárquica legalmente instituída no Brasil. Alguns aspectos relevantes na concepção deste modelo são discutidos a seguir.

A. A assinatura digital e a cadeia legalmente relevante

O conceito de *cadeia legalmente relevante* remete à transferência do controle de execução de um software entre módulos legalmente relevantes (LR) e não legalmente relevantes (NLR). Tal conceito é fundamental na construção de um instrumento de medição controlado por software, pois permite implementar a *separação de software*, o que agrega em maior confiabilidade no produto e também simplifica a complexidade dos processos de aprovação de modelo [13].

A assinatura digital é um mecanismo eficiente para se obter separação de software e definir de forma clara a fronteira entre o software LR e NLR [12]. Se o acesso à chave privada associada a uma assinatura digital é restrito a um módulo de software X, então qualquer informação digitalmente assinada e transmitida por X a um outro módulo Y terá sua integridade e autenticidade preservada, uma vez que Y não pode forjar uma nova assinatura sem a respectiva chave privada. De igual modo, a assinatura digital de um registro de medição por um módulo de software LR encerra a cadeia LR, desde que:

- Somente o módulo LR tem acesso à respectiva chave privada usada na assinatura;
- Todos os subsequentes módulos NLR são obrigados a apresentar a assinatura digital correspondente à informação recebida, quando solicitado; e
- Existem mecanismos disponíveis para se verificar tal assinatura, por meio de um certificado digital.

B. A assinatura digital no momento mais próximo da concretização da medição

Como discutido na seção anterior, a assinatura digital encerra a cadeia legalmente relevante, e determina de forma clara a fronteira entre módulos LR e NLR. Deste modo, é evidente que, quanto mais cedo a assinatura digital for realizada no processo de medição, menor será a cadeia legalmente relevante e também menor será o tamanho do software LR [12].

O tamanho do software LR tem uma implicação tremenda sobre a complexidade do processo de apreciação de modelo. Instrumentos de medição cujo software LR é menor são mais simples de ser avaliados, em virtude da redução de acoplamento entre módulos e também por não exigir do avaliador um domínio sobre funcionalidades implementadas pelo software NLR. Além disso, pode-se afirmar que tais produtos são significativamente mais seguros contra ataques cibernéticos e menos susceptíveis a defeitos de software remanescentes, dada a relação conhecida entre o tamanho do software e a quantidade de defeitos contida em seu código [14].

C. Requisitos de um certificado digital para instrumentos de medição

Um certificado digital para utilização em instrumentos de medição deve satisfazer requisitos essenciais de segurança. Ao mesmo tempo, é necessário considerar aspectos associados à aplicação do instrumento de medição. Diferentes instrumentos são utilizados em aplicações diversas, todavia é possível identificar requisitos que são comuns a diferentes casos de uso:

1) Os certificados digitais devem ter sua segurança assegurada pelo uso de módulos criptográficos baseados em hardware. Deste modo, é possível prover mecanismos para geração e proteção das chaves criptográficas associadas ao certificado digital, bem como implementar diretivas criptográficas à parte dos módulos que gerenciam o software LR;
2) Os algoritmos criptográficos adotados devem ser passíveis de implementação pelos fabricantes do instrumento de medição associado. O custo computacional do algoritmo também deve ser adequado aos recursos de hardware disponíveis, de modo a não onerar a fabricação do instrumento de medição;
3) A validade do certificado digital deve ser adequada ao ciclo de vida do instrumento de medição. Muitos instrumentos são projetados para uso por longos

períodos de tempo, operando sob condições que dificultam intervenções técnicas para substituição dos certificados.

Com base nos requisitos propostos, o Comitê Gestor da Infraestrutura de Chave Pública Brasileira criou, por meio da Resolução[3] 139/2018, o certificado digital do tipo *Objeto Metrológico (OM-BR)*. O certificado OM-BR é exclusivo para instrumentos de medição regulados pelo Inmetro e são implementados para atender aos requisitos propostos. Isso permite que fabricantes de medidores os incorporem aos seus produtos, agregando maior segurança com um mínimo impacto.

IV. Estudo de Caso: Uso de Certificação Digital em Medidores de Combustível

A. Descrição do problema

Medidores de combustível, também conhecidos como *bombas de combustível*, são talvez os instrumentos mais visados em termos de fraudes e adulteração de medidas. A literatura relata problemas relacionados a estes instrumentos em diferentes países, tais como Brasil [3], [15], México [16] e Nigéria [17]. A fraude associada à medição de combustível pode ser extremamente lucrativa, e ao mesmo tempo difícil de ser exposta [3], [15]. Isso motiva especialmente a ação de vendedores de combustível maliciosos, que deliberadamente adulteram o medidor de combustível em uma categoria de fraude conhecida como ”bomba baixa”[15]. Por mais que as autoridades de verificação metrológica intensifiquem esforços na fiscalização dos medidores de combustível, tal tarefa é complexa em virtude do elevado número de equipamentos e da capilaridade de distribuição destes pelo país. Tais características tornam a fiscalização extremamente custosa e mesmo ineficiente contra mecanismos de fraude que podem ser furtivos e facilmente desabilitados pelo atacante na iminência de uma inspeção [3].

Em face dessas dificuldades, muitos esforços tem sido feitos no sentido de tornar o medidor de combustível um instrumento mais robusto contra eventuais ataques. Recentemente, o Inmetro propôs uma revisão do RTM de medidores de combustível (Portaria[4] 294/2018) incluindo entre os requisitos já existentes dois requisitos essenciais para se garantir a integridade, autenticidade e não repúdio de uma medição:

- O uso de assinatura digital do registro legalmente relevante do instrumento, no momento mais próximo possível da concretização de uma medição, e;
- O uso de certificados digitais padrão ICP-Brasil.

B. Funcionamento de um medidor de combustível

Um medidor de combustível basicamente bombeia o combustível de um tanque subterrâneo, passando por um transdutor de medição responsável pela medição. O combustível segue então por um duto ou mangueira, sob o controle de uma válvula solenóide, sendo por fim injetado por meio de um bico no tanque do carro. O transdutor é tipicamente representado por um eixo mecânico integrado a um pulsador. O movimento do eixo é convertido em pulsos eletrônicos, de modo que o número de pulsos é proporcional ao volume medido. Em função disso, o conjunto mecânico que inclui o transdutor é denominado *pulser*.

C. Principais ataques em medidores de combustível

Ataques contra medidores de combustível geralmente se concentram na adulteração das medições, sendo que o principal alvo são os dados gerados pelo *pulser*. O Inmetro detalha por meio da NIT-Sinst-002[5] 18 diferentes métodos de ataques contra bombas de combustível, detectados e catalogados por agentes metrológicos no período de 2013 a 2016. Em nosso estudo, consideramos duas principais categorias de ataques, a saber:

1) Fraudes associadas ao pulser: São os casos onde componentes eletrônicos associados à placa de contagem de pulsos são modificados (ou inseridos) de modo a incrementar o número de pulsos, resultando assim em uma medição fraudulenta. Diferentes componentes podem ser comprometidos, incluindo placas de circuitos de interfaceamente, placas controladoras do *pulser*, cabos de interconexão dos componentes, CPUs, ou ainda o próprio sensor transdutor do *pulser*. Basicamente, esses casos de ataque ocorrem antes da entrega dos dados computados pelo *pulser*.

2) Fraudes usando sistemas de gerenciamento: Essa categoria de fraude caracteriza-se pelo uso de um mecanismo de ataque baseado na ideia de *man-in-the-middle*. Para tanto ele se vale do sistema de gerenciamento do medidor de combustível. Esse sistema é externo ao medidor e tem a função de obter informações e enviar comandos específicos. Quando fraudado, o sistema de gerenciamento é programado para interceptar a informação de medição dada pelo *pulser*, modificá-la acrescentando um valor maior e retornar esse valor adulterado ao medidor de combustível, para que o mesmo seja exibido no *display* disponibilizado ao consumidor. Estes ataques se caracterizam por adulterar as medições após a entrega das mesmas pelo *pulser*.

D. Assinatura digital como contramedida de segurança

A assinatura digital das medições realizadas por um medidor de combustível, feita no ponto mais próximo à realização desta medida, constitui um mecanismo eficaz de garantia da integridade da medição, e da identificação e autenticação do medidor. Uma vez que os ataques mencionados se concentram essencialmente na adulteração dos dados providos pelo *pulser*, este precisa se tornar um elemento inviolável e capaz de realizar a assinatura digital sem depender de qualquer outro módulo do sistema.

A inviolabilidade do *pulser* pode ser obtida modificando suas características construtivas de modo que todos os componentes eletrônicos associados ao mesmo sejam protegidos por um invólucro físico, cuja violação inutiliza o dispositivo como um todo. Este invólucro passa a incorporar inclusive os componentes computacionais que contêm as diretivas criptográficas

[3]https://www.iti.gov.br/legislacao/61-legislacao/501-resolucoes

[4]http://www.inmetro.gov.br/legislacao/rtac/pdf/RTAC002514.pdf

[5]http://www.inmetro.gov.br/metlegal/docdisponiveis.asp

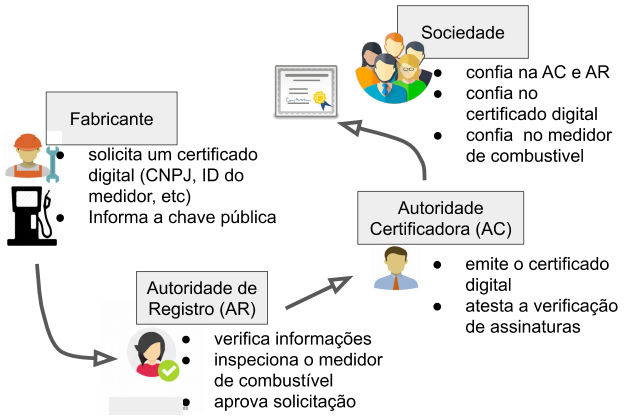

Figura 1. Diagrama descrevendo papéis de AR e AC.

para se fazer a assinatura digital (e.g., um *chip* criptográfico capaz de gerar um par de chaves e armazenar um certificado digital).

Por sua vez, todos os dados de medição providos pelo *pulser* são disponibilizados em conjunto com sua respectiva assinatura digital, que passa a ser exigida pelos demais módulos do sistema, e acompanha permanentemente o registro de medição de combustível, desde uma simples exibição da medida em um *display* na bomba de combustível, até a impressão da medida em um recibo concedido ao cliente em um reabastecimento.

E. Procedimento para gerenciamento dos certificados digitais

Um certificado digital está associado a um ciclo de vida. No caso do OM-BR, o certificado é atrelado ao *pulser*, mas seu uso passa por diferentes estágios durante o ciclo de vida de um medidor de combustível, tal como ilustra a Figura 1. A gestão desse ciclo requer um procedimento a ser seguido pelas entidades envolvidas, ou seja: fabricantes, usuários (i.e., proprietários de postos de combustível que adquirem os instrumentos), autoridades de regulamentação, e também ACs e ARs. Este procedimento é descrito nas próximas subseções.

1) Fabricação do pulser: Neste novo modelo de medidor de combustível, o *pulser* é concebido como um dispositivo único e selado. Isso implica que todos os subcomponentes responsáveis por suas funcionalidades são encapsulados em um invólucro de segurança. Em caso de defeito em qualquer dos seus subcomponentes, o *pulser* deve ser substituído como um todo. Não existe a possibilidade de reparos funcionais envolvendo a substituição ou reparação de subcomponentes do *pulser*. Além dos subcomponentes diretamente associados à eletrônica responsável pela medição de combustível, o *pulser* inclui também um módulo criptográfico OM-BR. Deste modo, cada *pulser* possui seu próprio par de chaves assimétricas, atribuídas de forma única. O módulo criptográfico permite a divulgação da chave pública do *pulser*, ao passo que a chave privada é permanentemente protegida pelo módulo criptográfica, sem ser jamais revelada pelo mesmo. Uma vez que o próprio *pulser* isola seus subcomponentes por meio do invólucro de segurança, o mesmo protege o módulo criptográfico inclusive contra ataques *side channel*.

Cada *pulser* é associado a um identificador único, correspondente a seu número de série. A chave pública do *pulser* também pode constituir um identificador, dado seu caráter único. Deste modo, pode-se dizer que existem dois identificadores, um forte e um fraco, sendo esses respectivamente a chave pública do *pulser* e seu número de série.

2) Fabricação do medidor de combustível: A fabricação do medidor de combustível envolve a integração do *pulser* aos demais componentes de constituição mecânica, hidráulica, elétrica e eletrônica que o constituem. É importante observar, todavia, que o *pulser* passa a incorporar todas as funcionalidades legalmente relevantes do medidor. Ainda que outros componentes sejam usados para exibição de informação legalmente relevante (e.g., *display* informando o volume abastecido em litros), tal informação é rastreável à assinatura digital da medição feita pelo *pulser*, o que encerra a cadeia legalmente relevante. O medidor possui também um número de série, atribuído pelo fabricante como um mecanismo de controle de produção. Quando o *pulser* é instalado no medidor de combustível, o fabricante associa o identificador do *pulser* ao respectivo número de série do medidor. É importante observar que essa associação existe enquanto o *pulser* se encontra funcional dentro deste medidor. Se em algum momento a substituição do *pulser* se faz necessária, essa associação é atualizada, de modo a se manter o controle de qual *pulser* se encontra funcional dentro de cada medidor de combustível.

3) Verificação inicial: A verificação inicial é feita por um organismo de inspeção delegado pela autoridade regulamentadora em cada novo medidor de combustível. A mesma ocorre ainda em fábrica, constituindo um pré-requisito para a comercialização do mesmo. Nessa verificação, o organismo de inspeção verifica se o instrumento apresenta as características de projeto correspondentes à sua aprovação de modelo, bem como executa testes metrológicos para se certificar de que a incerteza de medição apresentada pelo instrumento se encontra dentro dos limites aceitáveis. Em seguida, o organismo de inspeção exerce também a atividade de Autoridade de Registro, verificando a existência da chave pública do medidor (e sua correspondente chave privada), bem como coletando as informações de cunho legal que comporão o certificado digital OM-BR deste medidor. Consequentemente, o organismo de inspeção torna-se também o responsável pela emissão das informações à respectiva Autoridade Certificadora.

4) Emissão do certificado digital: De posse das informações verificadas pela AR, a AC emite certificado OM-BR a ser embarcado no medidor de combustível. Como já discutido anteriormente, o certificado digital associa de forma única e irrefutável um medidor de combustível e sua respectiva chave pública. Desta forma, as medições obtidas a partir deste instrumento têm sua rastreabilidade assegurada, sendo impossível a negação de que determinada medição não foi gerada pelo respectivo *pulser*.

Uma vez gerado o certificado digital, o mesmo é remetido ao fabricante, para que este proceda com a gravação do mesmo no respectivo instrumento. A possibilidade de que o fabricante não proceda com a gravação do certificado, ou ainda que a

gravação do certificado seja feita em um medidor de combustível distinto, são irrelevantes. Isso porque, na incidência de qualquer uma das situações, o medidor será incapaz de realizar suas funções de forma apropriada. Deste modo, tais situações são detectadas de imediato na operação do instrumento.

5) Instalação em campo: Uma vez concluídas as etapas anteriores, o medidor de combustível pode ser comercializado e instalado em campo normalmente. As oficinas autorizadas responsáveis por essa tarefa ficam também responsáveis por informar ao organismo de inspeção o identificador do medidor, identificador do seu respectivo *pulser* no momento da instalação, bem como o local de instalação do mesmo e as informações relevantes do detentor do instrumento (e.g., CNPJ e razão social do posto de combustível).

Periodicamente, o organismo de inspeção realiza a verificação do medidor em seu respectivo local de operação. Nessas circunstâncias, além de proceder com a verificação das funcionalidades metrológica e legalmente relevantes, o organismo de inspeção confirma também se a respectiva associação entre o identificador do medidor, o identificador do *pulser* e as informações complementares do detentor do instrumento permanecem consistentes. Tal procedimento garante que não ocorreram substituições indevidas do *pulser*, ou ainda a realocação do medidor de combustível como um todo.

6) Substituição de pulser e realocações de medidores de combustível: Em caso de necessidade de substituição de um *pulser*, seja por defeito ou violação do mesmo, ou ainda de realocação do medidor de combustível como um todo para um novo ponto de instalação, a oficina autorizada responsável deve comunicar o evento ao organismo de inspeção, procedendo conforme definido na subseção anterior.

V. Considerações Finais

Este trabalho apresentou os estudos e esforços associados à criação e implementação de uma classe específica de certificados digitais para uso em medidores inteligentes. Tal resultado é especialmente relevante para a área de Metrologia Legal. Até onde é de nosso conhecimento, o Brasil se torna pioneiro na implementação de um mecanismo de certificação digital atrelado à Autoridade Raiz, que garante a integridade, autenticidade e não repúdio de informações de cunho legal gerada por medidores inteligentes.

Vale ressaltar que os resultados aqui apresentados são emblemáticos, em especial quando se considera o estudo de caso associado aos medidores de combustível. O problema de fraudes nesta classe de medidor constitui um desafio de proporções gigantescas no campo da segurança da informação, e afeta a sociedade como um todo. Assim, a implantação do sistema descrito para uso dos certificados digitais nesta classe de medidores constitui um passo importante no combate às fraudes mencionadas, o que provê maior confiança à sociedade em suas relações de consumo.

Os próximos passos incluem a aplicação dessa mesma solução a outros grupos de medidores inteligentes. É importante enfatizar que tal solução não se restringe a medidores, e pode ser estendida também a outras classes de dispositivos inteligentes. Uma demanda latente é o uso de certificados digitais em dispositivos IoT, dado o crescimento vertiginoso dessa tecnologia e a necessidade crescente de garantir a segurança e confiabilidade das informações geradas por eles.

Agradecimentos

Trabalho apoiado por CNPq e FAPERJ.

Referências

[1] W. Stallings and L. Brown, *Computer Security: Principles and Practice*, 4th ed. Pearson, 2018.

[2] B. A. Rodrigues Filho and R. F. Gonçalves, "Legal metrology, the economy and society: A systematic literature review," *Measurement*, vol. 69, pp. 155–163, 2015.

[3] F. O. Leitão, M. T. Vasconcellos, and P. C. R. Brandão, "Hardware and Software Countermeasures on High Technology Fraud at Fuel Dispensers under the Scope of Legal Metrology," in *IX Simposio Internacional 'Metrologia 2014'*, Havana, 2014, pp. 1–10.

[4] M. Esche and F. Thiel, "Software Risk Assessment for Measuring Instruments in Legal Metrology," in *Proceedings of the Federated Conference on Computer Science and Information Systems*, vol. 5, 2015, pp. 1113–1123. [Online]. Available: https://fedcsis.org/proceedings/2015/drp/127.html

[5] D. R. Boccardo, L. C. G. Dos Santos, L. F. Carmo, M. H. Dezan, R. C. S. Machado, and S. D. A. Portugal, "Software evaluation of smart meters within a legal metrology perspective: A Brazilian case," in *IEEE PES Innovative Smart Grid Technologies Conference Europe, ISGT Europe*, 2010, pp. 1–7.

[6] B. A. Rodrigues Filho and R. F. Gonçalves, "Measuring the economic impact of metrological frauds in trade metrology using an Input-Output Model," *IFIP Advances in Information and Communication Technology*, vol. 488, 2016.

[7] European Cooperation in Legal Metrology (WELMEC), "WELMEC 7.2, 2015: Software Guide," pp. 1–114, 2015.

[8] International Organization of Legal Metrology (OIML), "OIML D 31, Editon 2008: General requirements for software controlled measuring instruments," p. 53, 2008.

[9] A. Ray, J. Akerberg, M. Bjorkman, R. Blom, and M. Gidlund, "Applicability of LTE Public Key Infrastructure Based Device Authentication in Industrial Plants," *Proceedings - International Computer Software and Applications Conference*, vol. 2, pp. 510–515, 2015.

[10] S. Al Salami, J. Baek, K. Salah, and E. Damiani, "Lightweight encryption for smart home," *Proceedings - 2016 11th International Conference on Availability, Reliability and Security, ARES 2016*, pp. 382–388, 2016.

[11] F. Jäger, U. Grottker, H. Schrepf, and W. Guse, "Protection of image and measurement data in an open network for traffic enforcement," *Computer Standards & Interfaces*, vol. 28, no. 3, pp. 327–335, 2006.

[12] D. R. Boccardo, R. C. S. Machado, S. Camara, C. B. Prado, W. S. Melo Jr., L. C. Ribeiro, and L. F. Carmo, "Software validation of medical instruments," *2014 IEEE International Symposium on Medical Measurements and Applications (MeMeA)*, no. October 2015, pp. 1–4, 2014. [Online]. Available: http://ieeexplore.ieee.org/document/6860090/

[13] D. Peters, F. Thiel, M. Peter, and J.-P. Seifert, "A secure software framework for Measuring Instruments in legal metrology," *2015 IEEE International Instrumentation and Measurement Technology Conference (I2MTC) Proceedings*, pp. 1596–1601, 2015. [Online]. Available: http://ieeexplore.ieee.org/document/7151517/

[14] O. H. Alhazmi, Y. K. Malaiya, and I. Ray, "Measuring, analyzing and predicting security vulnerabilities in software systems," *Computers and Security*, vol. 26, no. 3, pp. 219–228, 2007.

[15] A. Beteto, V. Melo, and E. Dias, "Fuel Reselling: Electronic Documents and Tax Surveillance," *International Journal of Economics and Management Systems*, vol. 1, pp. 163–168, 2016.

[16] H. Luchsinger, C. Cajica, M. Maldonado, and I. Castelazo, "Are Gas Pumps Measuring Up? The Mexican Experience," *NCSLI Measure*, vol. 3, no. 2, pp. 62–68, 2008.

[17] O. Rasheed, A. Adetunji, and A. Ige, "Control Systems, Fraud Minimization and Organisational Compliance in the Downstream Sector of Nigerian Oil and Gas Industry 1," *Imperial Journal of Interdisciplinary Research (IJIR)*, vol. 3, no. 10, pp. 226–233, 2017.