IMPACTO DO USO DE ASSINATURA DIGITAL NA SEGURANÇA DA INFORMAÇÃO E NO PROCESSO DE AVALIAÇÃO DA SEGURANÇA EM SISTEMAS DE MEDIÇÃO

F. P. Moraes[1], D. R. Boccardo[2], C. B. Prado[3], L. F. Rust[4]

[1] *Inmetro, Rio de Janeiro, Brasil, fpmoraes@inmetro.gov.br*
[2] *Inmetro, Rio de Janeiro, Brasil, drboccardo@inmetro.gov.br*
[3] *Inmetro, Rio de Janeiro, Brasil, cbprado@inmetro.gov.br*
[4] *Inmetro, Rio de Janeiro, Brasil, lfrust@inmetro.gov.br*

Resumo: Este trabalho propõe o uso da assinatura digital em sistemas de medição com software embarcado como ferramenta adequada para reduzir ou eliminar possíveis falhas/fraudes no processo de apreciação técnica de modelo pelo Inmetro, bem como para viabilizar a construção de um processo de validação de software com maior celeridade e confiabilidade.

Palavras chave: assinatura digital, sistema de medição, software embarcado, validação de software.

1. Introdução

Compete ao Inmetro, por meio da Diretoria de Metrologia Legal, executar o processo de apreciação técnica de modelo dos instrumentos de medição que estão sujeitos aos regulamentos elaborados pelas Comissões Técnicas de Regulamentação Metrológica. Até pouco tempo atrás, esse processo consistia apenas no exame feito através de estudo da documentação, inspeção visual, e ensaios em um ou mais exemplares do modelo, conforme definido nos Regulamentos Técnicos Metrológicos.

No entanto, após o advento de sistemas de medição – conjunto de um ou mais instrumentos de medição – com software embarcado e partes distribuídas, novos desafios à área metrológica passaram a demandar maior reflexão sobre os riscos introduzidos para a segurança da informação [1].

Frente a essa demanda, novas formas de validação do sistema de medição e metodologias para proteção do software e das comunicações de dados têm sido propostas a fim de assegurar o atendimento aos requisitos de segurança tendo em vista o aumento da complexidade dos sistemas de medição modernos.

Atualmente, o trabalho despendido na avaliação de software é complexo. Exige uma análise completa do código-fonte do sistema de medição para cercar as possibilidades de fraude ou reduzir o seu impacto, garantir a continuidade do funcionamento do sistema de medição após uma falha e assegurar a adequação de mecanismos que permitam uma análise *a posteriori* do seu funcionamento. Sem essa análise, não é possível garantir que o valor da grandeza de medição observada pelo usuário é resultado de uma consideração adequada dos valores capturados pelos sensores.

Além de demandar muito tempo e recurso, essa análise ainda sofre crítica por parte dos fabricantes dos sistemas de medição, que veem o seu segredo industrial revelado e o consideram suscetível de vazamento.

Diante desse cenário, este trabalho propõe um estudo de impacto do uso da assinatura digital [2-3] em sistemas de medição como meio para garantir a segurança da informação nos processos de auditoria, operação, manutenção e apreciação técnica de modelo, sem a necessidade de uma análise prévia completa de todo o código-fonte, e também aponta os aspectos dessa nova abordagem que contribuem para alterar o processo de avaliação de software realizado atualmente.

O restante do artigo está estruturado da seguinte forma. Seção 2 define sucintamente um sistema de medição e seus possíveis subsistemas. Seção 3 apresenta o método de análise de software atual e os seus pontos fracos. Seção 4 descreve o método proposto baseado no uso de assinatura digital para incremento da segurança e aperfeiçoamento do processo de avaliação da segurança em sistemas de medição. Por fim, Seção 5 contém as conclusões pertinentes.

2. Sistema de medição

Um sistema de medição é um conjunto de um ou mais instrumentos de medição e frequentemente outros dispositivos, compreendendo, se necessário, reagentes e insumos, montado e adaptado para fornecer informações destinadas à obtenção dos valores medidos, dentro de intervalos específicos para grandezas específicas [4].

Sob o ponto de vista de um processo de medição, a atuação desse sistema se realiza em três etapas: a captura de dados de medição, o processamento, e a publicação do resultado final da medição. Essas etapas compõem uma cadeia – dita legalmente relevante –, através da qual os dados de medição obtidos durante a etapa de captura determinam o resultado final de medição publicado. Nessa cadeia, antes da publicação e após a captura, encontram-se os componentes do sistema que abrigam as funções de medição envolvidas na etapa de processamento dos dados de medição. Todos os componentes de tecnologia da informação (hardware e software), localizados na cadeia legalmente relevante ou que possa interferir nessa cadeia estão sujeitos a controle pelo Inmetro.

A função de medição é a função que calcula valores de grandezas de entrada a partir de valores de grandezas de saída em um modelo de medição. Este, por sua vez, é a relação matemática entre todas as grandezas as quais, sabidamente, estão envolvidas numa medição [4]. Neste trabalho, doravante, valores de grandeza de entrada e valores de grandeza de saída são referenciados, genericamente, como dados de medição.

As funções de medição podem ser distribuídas em dois tipos de subsistemas de medição: subsistema do tipo P e subsistema do tipo U, conforme o guia da WELMEC [5].

Um subsistema de medição do tipo P é construído com o propósito específico de medição, de acordo com as seguintes considerações:

a) Todo o software aplicativo foi desenvolvido para suporte à medição, incluindo as funções sujeitas ao controle metrológico legal, assim como as restantes;
b) A interface do usuário é dedicada à aplicação de medição;
c) Se existir, um sistema operacional não pode compartilhar recursos computacionais com outros usuários.

Um subsistema de medição do tipo U faz uso de um sistema de computador de propósito geral, de acordo com as seguintes considerações:

a) O sistema de computador pode funcionar isoladamente, participar de uma rede fechada (exemplos: Ethernet, *token-ring*) ou participar de uma rede aberta (exemplo: Internet);
b) Uma vez que o subsistema é de propósito geral, o sensor seria normalmente externo à unidade de computador e seria normalmente conectado a este por meio de um enlace de comunicação fechado. O enlace de comunicação também poderia ser, no entanto, aberto (exemplo: rede à qual vários sensores poderiam estar ligados);
c) A interface de usuário pode ser alternada de um modo de operação, o qual não está sob o controle legal, para outro, e vice-versa;
d) O armazenamento pode ser fixo (exemplo: disco rígido), ou removível (exemplo: CD-RW);
e) Qualquer sistema operacional pode ser usado. Em adição ao aplicativo do instrumento de medição, outros aplicativos de software podem também residir no sistema concomitantemente. Partes do software (exemplo: aplicação do instrumento de medição) estão sujeitas ao controle legal e não podem ser modificadas após aprovação. Partes não sujeitas ao controle legal podem ser modificadas;
f) O sistema operacional e *drivers* de baixo nível (exemplo: *driver* de impressora) não são legalmente relevantes a menos que eles sejam programados especificamente para uma tarefa de medição.

A Figura 1 mostra um modelo de sistema de medição com destaque para as funções de medição distribuídas entre os subsistemas do tipo P e U. Nessa figura, três valores de grandeza de entrada são obtidos na etapa de captura, no escopo do subsistema do tipo P. Durante a etapa de processamento, esses valores são considerados pelas funções de medição, que geram os valores de grandezas de saída a serem usados como valores de grandezas de entrada para o subsistema do tipo U. Estes últimos são considerados pelas funções de medição, que geram o valor de grandeza de saída – o resultado final de medição –, apresentado na etapa de publicação da cadeia legalmente relevante.

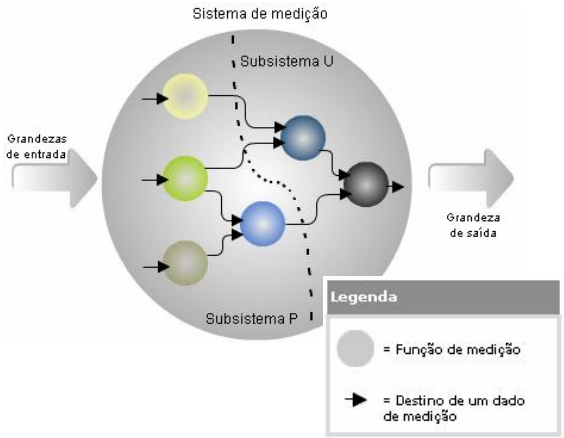

Figura 1: Modelo de sistema de medição composto de um subsistema do tipo P e de um subsistema do tipo U.

3. Processo de avaliação de software dos sistemas de medição

O processo atual de avaliação de software dos sistemas de medição envolve uma análise de todos os componentes de tecnologia de informação localizados na cadeia legalmente relevante. O objetivo é garantir que os requisitos de software desses sistemas – constantes nos regulamentos elaborados pelas Comissões Técnicas de Regulamentação Metrológica – sejam atendidos.

A necessidade de uma análise tão abrangente está associada à solução de segurança presente nos sistemas de medição atuais: uso de um segredo compartilhado entre os componentes do sistema para dar suporte ao mecanismo de autenticidade e de integridade na comunicação de dados (criptografia simétrica).

Com essa solução, torna-se necessário garantir, nas etapas de captura, processamento e publicação, que as propriedades de segurança dos dados de medição sejam preservadas a fim de garantir a legitimidade do resultado final para o usuário.

Em decorrência dessa necessidade, a avaliação de software dos sistemas de medição envolve, dentre outras atividades, percorrer e entender os diversos caminhos de função de medição, mostrados na Figura 1, desde a captura de dados de medição até a publicação do resultado final de medição. Para tanto, torna-se imperativa a abertura do código-fonte dos componentes do sistema de medição ao longo de toda a cadeia legalmente relevante.

Esse cenário motiva a elaboração de uma nova metodologia para facilitar o processo de avaliação de software, bem como para resguardar a proteção intelectual por parte do fabricante.

3.1 Implicações do uso de sistema operacional diante do processo de avaliação

A partir do início do uso de software embarcado em sistemas de medição não tardou a aparecer um sistema operacional, com o propósito de gerenciar os recursos do sistema de medição, tais como processador, memória, dispositivos de E/S e comunicação de dados. Em função de tantas atribuições e funcionalidades, o sistema operacional é geralmente composto por muitos módulos complexos de software. Esses módulos trocam informações entre si, armazenam dados, compartilham recursos computacionais e modificam a memória primária e secundária em tempo de execução, sem qualquer restrição. Essa permissividade contribui para dificultar a análise do comportamento de um sistema operacional, que, além de ter um código-fonte muito extenso, geralmente faz uso de estruturas de dados otimizadas para maximizar a eficiência do uso dos recursos computacionais disponíveis [6].

Diante desse cenário, a análise de código-fonte torna-se ainda mais falível, no que concerne a segurança da informação. Além de desfavorecer a investigação por fraudes, dificulta a busca de falhas, que surgirão inevitavelmente.

Além do sistema operacional, existem alguns módulos de software, chamados *drivers*, que são executados com a mesma permissividade que o sistema operacional por atuarem como ponte entre este e o hardware.

Os *drivers* são extensões do sistema operacional, porém desenvolvidos separadamente para permitir que novas funcionalidades sejam incorporadas ao sistema sem que o sistema operacional seja modificado, recompilado e redistribuído. Por isso, os *drivers* abrem espaço para novas oportunidades de fraude já que atuam como um software que executa com privilégios e podem ser programados para executarem de forma oculta, sem o conhecimento do administrador, ao subverter bibliotecas de sistema e ignorar mecanismos de autenticação e autorização.

4. Proposta

A proposta deste trabalho tem por objetivo principal influenciar dois aspectos do processo de apreciação técnica de modelos no que concerne os sistemas de medição com software embarcado: o processo de análise de software e a validação da solução técnica empregada frente aos requisitos de segurança da informação. Para

esse fim, propõe-se o uso de assinatura digital pelo sistema de medição.

Além de seu uso conferir maior celeridade ao processo, sem comprometer a sua confiabilidade, a assinatura digital diminui o potencial de falha na avaliação do software ao reduzir a abrangência da análise, sem, no entanto, reduzir o seu escopo, conforme será visto adiante.

Todas essas vantagens são obtidas por meio de uma propriedade da assinatura digital: associar de forma unívoca a informação à sua fonte. Após assinado digitalmente, o valor de medição não pode ser modificado (acidentalmente ou intencionalmente), sem ser percebido, ao longo da cadeia legalmente relevante.

Com essa nova abordagem, a segurança da informação passa a ser baseada na rastreabilidade do resultado final da medição. Essa característica repercute no processo de análise de software, que deixa de focar a proteção dos dados de medição, ao longo de toda a cadeia legalmente relevante, para garantir a sua proteção, por meio de assinatura digital, nas etapas de captura ou de processamento.

Um dos benefícios alcançados com essa abordagem é que a análise do código-fonte pode ser restringida. Dependendo das características físicas e lógicas do sistema, o momento de aplicação da assinatura digital, dentro da cadeia legalmente relevante, estabelece um marco a partir do qual a análise de software torna-se desnecessária. A determinação desse momento traz, então, conseqüência: quanto mais tardia for a aplicação da assinatura digital, maior será o esforço para análise de software do sistema de medição.

Características físicas e lógicas do sistema de medição são determinantes para o julgamento da assinatura digital como solução adequada para segurança da informação. Uma característica física desejável é uma arquitetura bem estruturada, de fácil entendimento, na qual seja constatada a necessidade de cada elemento da infraestrutura, sem portas de comunicação redundantes e com protocolos simples. Uma característica lógica desejável é a estruturação modular do código-fonte, com o uso de estruturas de dados adequadas. Sem essas características desejáveis, que devem ser comprovadas principalmente pela documentação, torna-se comprometido o julgamento da solução técnica adotada.

A Figura 2 mostra a abrangência da avaliação de software para um determinado sistema de medição considerando-se a aplicação de assinatura digital aos dados de medição logo após a etapa de captura dentro da cadeia legalmente relevante. Nesse caso, as atividades de análise de código-fonte poderão ser concentradas nos sensores, o que representa apenas parte do total de atividades de análise detalhada de software que seria necessária, caso a assinatura digital não tivesse sido aplicada – conforme destacado no preenchimento parcial do retângulo de abrangência da avaliação detalhada de software.

No entanto, a Figura 2 pode não retratar fielmente a distribuição do volume de atividades de análise de software entre as etapas de captura, processamento e publicação. Normalmente, a maior parte das atividades se concentra nessas duas últimas etapas. Se os dados de medição forem todos assinados na etapa de captura, como é o caso ilustrado, então o esforço despendido para apreciação técnica de modelo pode ser bastante reduzido. Por esse motivo, esta abordagem encoraja a aplicação antecipada da assinatura digital dentro da cadeia legalmente relevante.

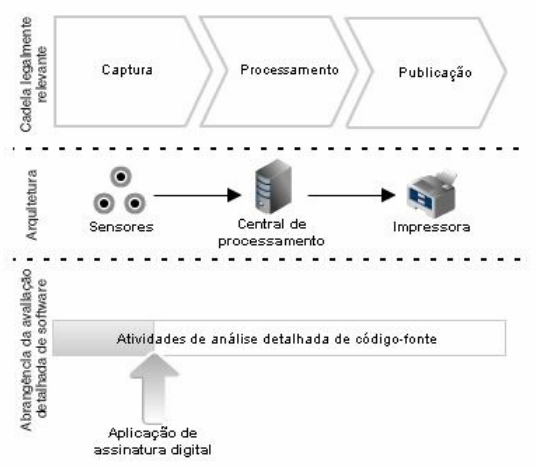

Figura 2: Impacto do uso da assinatura digital na análise de software.

Em sistemas de medição com sistema operacional de propósito geral (subsistema do tipo U), uma restrição acerca da aplicação da assinatura digital faz-se necessária: todos os valores de grandezas de entrada para funções de medição dentro do subsistema do tipo U devem estar assinadas digitalmente.

Diante da inviabilidade de atestar a segurança do mecanismo que aplica a assinatura digital dentro do subsistema do tipo U, a rastreabilidade do resultado de medição deve ser garantida por meio da aplicação de assinatura digital no subsistema do tipo P. Isso garante que o sistema operacional e os *drivers* não sejam capazes de modificar intencionalmente ou corrompa os dados de medição gerados a partir do subsistema do tipo P.

4.1 Publicação do resultado final de medição

Como consequência da adoção desta proposta, a etapa de publicação deve fornecer todas as informações que permitem reconstituir o resultado final da medição, que deve incluir as assinaturas digitais dos dados de medição originários das etapas de captura e de processamento.

Além disso, a regra usada para alcançar o resultado final de medição e as constantes consideradas nas etapas de captura e de processamento devem ser conhecidas. Ou seja, as funções de medição, os dados de medição assinados digitalmente e as constantes de ajuste do sistema de medição, tais como constantes de calibração e de adaptação para instalação, devem ser revelados para permitir a rastreabilidade do resultado final da medição.

A Figura 3 mostra um conjunto de funções de medição que compõem um sistema de medição. Essas funções são encadeadas de acordo com a arquitetura do sistema e convergem para o resultado final de medição na etapa de publicação. Na figura, não existe um caminho de funções para o qual dados de medição não assinados influenciem o resultado final da medição. No caso da Figura 2, todas as três assinaturas digitais necessárias para rastrear o resultado de medição devem ser publicadas.

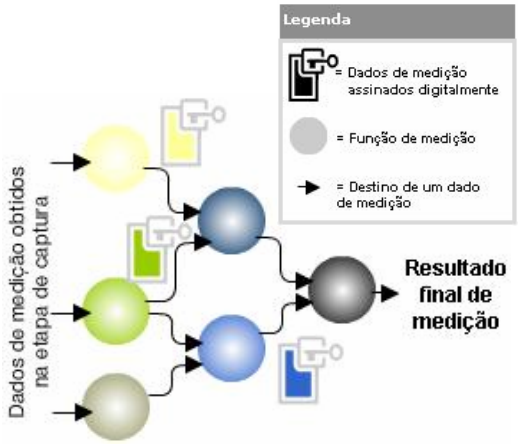

Figura 3: Encadeamento de funções de medição que geram um resultado de medição rastreável.

Por outro lado, a Figura 4 mostra um exemplo de conjunto de funções de medição que convergem para um resultado final de medição não rastreável, pois existe pelo menos um caminho de funções, mostrado com uma linha tracejada, que considera dados de medição não assinados.

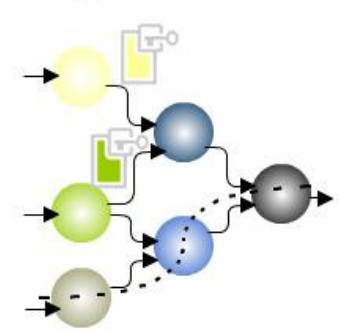

Figura 4: Encadeamento de funções de medição que geram um resultado de medição não rastreável.

4.2 Considerações finais

Na esteira do aumento das funcionalidades dos sistemas de medição, preocupações tradicionais sobre a segurança da informação voltam à tona no processo de análise de software, a despeito do uso da assinatura digital.

Novas funcionalidades aumentam a vulnerabilidade do sistema, seja pelo maior risco de ocorrerem falhas durante operação, seja pela maior dificuldade de detectar fraudes e preveni-las durante análise de código-fonte.

Se por um lado a aplicação da assinatura digital em sistemas de medição, na abordagem deste trabalho, é uma condição necessária para garantia da rastreabilidade do resultado final de medição, por outro lado ela traz a possibilidade de redução da abrangência da avaliação de software, podendo dispensar, do processo de análise do software, estudo detalhado das etapas de processamento e de publicação, conforme mostrado no exemplo da Figura 2.

Essa abordagem pode suscitar desconfiança quanto à influência de novas funcionalidades sobre a cadeia legalmente relevante e operação do sistema, mesmo que de fato não estejam envolvidas diretamente com o processo de medição.

Via de regra, a simples possibilidade de existirem funcionalidades não envolvidas diretamente com a medição impõe uma condição para o uso da assinatura digital em sistemas de medição: exigência de investigação individual de cada fluxo externo de entrada de dados, o qual pode representar uma seqüência de comandos que alteram o comportamento do sistema de medição.

Na presença de um subsistema do tipo U, devido ao uso de um sistema operacional de propósito geral, essa exigência deve ser acompanhada de outras medidas para dificultar ao máximo qualquer tentativa de ocultar funcionalidades não previstas na documentação

e de subverter as soluções de segurança empregadas no sistema de medição.

Essas medidas, não necessariamente aplicáveis na sua totalidade, podem envolver: investigação cuidadosa da arquitetura do subsistema para descobrir as portas de entradas de dados e os discos rígidos presentes; análise dos discos rígidos para detectar partições lógicas desnecessárias ou informações/dados em espaços não formatados; verificação da integridade do software de medição, dos *drivers*, do sistema operacional e do sistema de arquivos associado; estabelecimento de controle de acesso nas comunicações com redes para resguardar o subsistema de ataques; habilitação apenas da operação de leitura nos discos rígidos para evitar a instalação de softwares não autorizados após a aprovação de modelo; lacre do gabinete que guarda os componentes internos do subsistema.

Embora essas atividades aumentem o esforço de análise no processo de apreciação técnica de modelo, sem o uso da assinatura digital seria necessário um estudo da segurança do software de medição – juntamente com bibliotecas e outros subsistemas envolvidos –, que executa sobre um sistema operacional, o que demandaria um esforço muito maior do que aquele despendido na análise de um subsistema do tipo P.

Felizmente, existem ferramentas que verificam a integridade do sistema operacional e que varrem as partições lógicas dos discos rígidos de forma automática, tornando mais ágeis algumas atividades do processo de análise do subsistema do tipo U.

4.3 Relacionamento temporal e espacial dos valores de medição

Uma conseqüência do uso de assinatura digital em etapas anteriores do processo de medição é que valores desconexos de medição assinados digitalmente em subsistemas de medição diferentes propagam-se por toda a cadeia legalmente relevante até chegarem ao resultado final de medição na etapa de publicação.

Assim, os valores que compõem o resultado da medição são considerados isoladamente quando usados como entrada para uma função de medição. No entanto, a assinatura digital confere uma vinculação temporal entre as grandezas de entrada e entre as grandezas de saída. Essa vinculação é importante porque os dados de medição tão somente compõem um conjunto autêntico se cada um dos valores de medição for autêntico. Por exemplo, a repetição de um dos valores de medição pelo sistema pode comprometer o resultado final de uma medição.

Uma assinatura digital possui uma informação temporal inerentemente associada, fazendo com que os valores de grandeza assinados pelo sistema de medição tornem-se relacionados pelo tempo, se houver uma única fonte de informação temporal ou se todas as fontes estiverem sincronizadas entre si. Mesmo que a informação temporal não seja exatamente a mesma em todas as assinaturas geradas pelo sistema, deve existir uma correlação temporal constante entre elas.

Enquanto a vinculação temporal apresentada é necessária para garantir a rastreabilidade do resultado de medição, ela não é suficiente. Uma medição deve estar relacionada ao local/instrumento de medição. Nesse sentido, o vínculo espacial entre as grandezas de entrada e entre as grandezas de saída é garantido, também, pela assinatura digital, que identifica a origem dos dados de medição. Somente o instrumento de medição do sistema é capaz de gerar dados de medição autenticados pelas chaves públicas divulgadas, que se tornam conhecidas pelo Inmetro durante o processo de apreciação técnica de modelo.

5. Conclusão

Este trabalho abordou o uso da assinatura digital em sistemas de medição e o seu impacto no processo de apreciação técnica de modelo. Ficou evidenciado que o uso da assinatura digital traz consequências importantes tanto para a segurança da informação quanto para o processo de avaliação de software dos sistemas de medição.

Quanto mais tardia for a aplicação de assinatura digital dentro da cadeia legalmente relevante, maior poderá ser o esforço para a avaliação da eficácia da solução técnica empregada para garantir a segurança da informação, já que um maior volume de código-fonte do sistema de medição terá que ser investigado.

Antecipada ou postergada, a aplicação da assinatura digital, a fim de alcançar a rastreabilidade do resultado final de medição, implica a necessidade de exibição de dados de medição – com as respectivas assinaturas – obtidos na etapa de captura e gerados na etapa de processamento na etapa de publicação.

A aplicação antecipada da assinatura digital não considera possíveis falhas ao longo da cadeia legalmente relevante que venham a comprometer a disponibilidade do resultado final da medição, uma vez que o escopo da análise do código-fonte pode ficar restrito ao

software anterior à assinatura digital, que foca apenas a autenticidade/rastreabilidade dos dados de medição. Mas, para suprir tal deficiência desta nova abordagem, a disponibilidade da informação pode ser garantida por meio da execução de testes sistêmicos, o que já é um caminho seguido pelo Inmetro durante o processo de avaliação de software.

Por outro lado, a aplicação antecipada da assinatura digital também contribui para aumentar a celeridade do processo de análise do software e diminuir o risco de fraude do resultado final de medição porque a assinatura digital, nesse caso, garante a inviolabilidade dos dados de medição já em etapas iniciais do processo de medição.

Por causa dessa vantagem, a exigência do uso de assinatura digital deve orientar a elaboração de futuros Regulamentos Técnicos Metrológicos do Inmetro com requisitos de software para sistemas de medição.

6. Referências bibliográficas

[1] Inmetro, *Portaria Inmetro nº 011 de 13 de janeiro de 2009*, In Proceedings of the Third USENIX Conference (Anaheim, CA, Jan.), USENIX Assoc., Berkeley, CA, 519–529, 1993.

[2] W. Stallings, *Cryptography and network security*, Second Edition, Prentice Hall, 1999.

[3] ETSI. *Signature Policies Report*. ETSI TR 102 041 (200202);European Telecomunications Standards Institute, 2002.

[4] *Vocabulário internacional de metrologia, Conceitos fundamentais e gerais e termos associados*, Primeira edição brasileira do VIM 2008.

[5] *European Cooperation in Legal Metrology*. WELMEC 7.2 – Guia de software, quarta edição. *Measuring instruments directive 2004/22/EC.*

[6] *Physikalisch-Technische Bundesanstalt (PTB). Workshop "Operating Systems in Measuring Instruments and other software problems in Legal Metrology" 2010. Berlin.*