UM MODELO PARA AS NORMAS SOBRE CERTIFICAÇÃO DIGITAL NO BRASIL

Viviane Bertol, Rafael Timóteo de Sousa Jr., Laerte Peotta de Melo
Departamento de Engenharia Elétrica – Universidade de Brasília (UnB)
Campus Universitário Darcy Ribeiro – Asa Norte – 70910-900 – Brasília, DF – Brasil

***Resumo*—Neste artigo apresenta-se a seguinte questão: com a atual regulamentação da ICP-Brasil, os documentos assinados digitalmente reúnem as condições técnicas necessárias e suficientes para serem úteis como evidência legal? Estão garantidas a confiabilidade e a longevidade desses documentos? Para respondê-la, foram analisados em detalhes os regulamentos da ICP-Brasil e foram relacionadas as características esperadas de uma ICP que emite certificados para uso em assinaturas digitais com validade jurídica. São apresentadas as lacunas mais importantes na regulamentação brasileira. Propõe-se um conjunto de medidas que possa solucionar ou pelo menos minimizar os principais problemas levantados.**

***Index Terms*—Infraestrutura de chaves públicas, Assinatura Digital, Preservação de longo Prazo, Documento Eletrônico**

I. Introdução

A Certificação digital no Brasil tomou impulso a partir de 2001, quando da criação, pelo Governo Federal, da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), que teve um grande crescimento, desde então. Estima-se que tenham sido emitidos mais de um milhão de certificados digitais ICP-Brasil para pessoas físicas e jurídicas. Esses certificados estão sendo utilizados em variadas aplicações, como: automatização da prestação de informações fiscais à Receita Federal do Brasil, nota fiscal eletrônica, informatização do Poder Judiciário, informatização de serviços cartoriais, informatização de processos para abertura de empresas, informatização de prontuários médico-odontológicos, compras governamentais por meio de pregão eletrônico.

Essa situação coloca o Brasil na dianteira em relação a muitos países, nos quais a certificação e a assinatura digital ainda são utilizadas de forma bastante restrita. Por outro lado, caso não sejam adotados os cuidados necessários, a utilização dessa tecnologia pode acarretar graves consequências, como a instalação de um "caos jurídico"em torno da validade de uma assinatura digital.

As questões propostas neste artigo são: com a atual regulamentação, os documentos assinados digitalmente no âmbito da ICP-Brasil reúnem as condições técnicas necessárias e suficientes para serem úteis como evidência legal, mesmo no longo prazo? Estão garantidas a confiabilidade e a longevidade desses documentos?

Para responder a essas questões foram analisados os regulamentos da ICP-Brasil considerando as características esperadas de uma ICP que emite certificados para uso em assinaturas digitais com validade legal. Esses regulamentos foram também comparados aos emanados por outros países e aos padrões internacionais criados por organismos de normalização reconhecidos. Ficou evidenciada a existência de lacunas importantes, para as quais foram recomendadas medidas corretivas, que vão desde a criação de novas entidades e serviços na ICP-Brasil, até a alteração dos formatos e tipos de certificados utilizados no País.

II. A ICP-Brasil

A. Entidades Integrantes

As principais entidades integrantes da ICP-Brasil estão representadas na estrutura hierárquica apresentada na Figura 1.

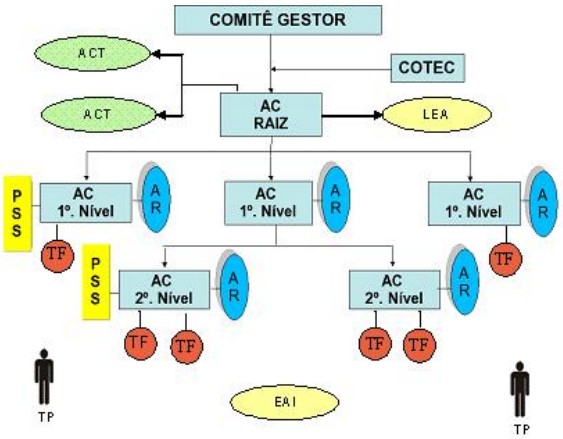

Figura 1. Organograma da ICP-BRASIL

1) Comitê Gestor: Composto por membros do Governo e da sociedade civil, tem por principal atribuição coordenar a implantação e o funcionamento da ICP-Brasil, além de estabelecer a política, os critérios e as normas para credenciamento das ACs, ARs e demais entidades que fazem parte da estrutura.

2) Comissão Técnica (COTEC): Presta suporte técnico e assistência ao Comitê Gestor, sendo responsável por manifestar-se previamente sobre as matérias apreciadas e decididas pelo comitê Gestor. É convocada sempre que necessário, sendo que cada um de seus representantes é indicado por um dos membros do Comitê Gestor.

3) AC-Raiz: Primeira autoridade da cadeia de certificação, a AC-Raiz executa as políticas de certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor. Emite seus próprios certificados; emite, expede, distribui, revoga e

gerencia os certificados das ACs de nível imediatamente subsequente ao seu; gerencia sua lista de certificados revogados.

4) Autoridades Certificadoras (AC): As autoridades certificadoras (ACs) são credenciadas para emitir certificados digitais vinculando pares de chaves criptográficas ao respectivo titular. Emitem, expedem, distribuem, revogam e gerenciam os certificados, bem como colocam à disposição dos usuários listas de certificados revogados e outras informações pertinentes e mantêm o registro de suas operações.

5) Autoridades de Registro (AR): As autoridades de registro (ARs) são entidades operacionalmente vinculadas a determinada AC. Compete-lhes identificar e cadastrar usuários na presença destes, encaminhar solicitações de certificados às ACs e manter registros de suas operações.

6) Prestadores de Serviços de Suporte (PSS): Os Prestadores de Serviços de Suporte (PSSs) são empresas contratadas por uma AC ou AR para realizar atividades de disponibilização de infraestrutura física e lógica e disponibilização de recursos humanos especializados.

7) Empresas de Auditoria Independente (EAI): As empresas de auditoria independentes (EAIs) são entidades que, uma vez cadastradas junto à AC-Raiz, podem ser contratadas pelas autoridades certificadoras para realizar auditorias operacionais nas próprias ACs e nas entidades a elas subordinadas.

8) Laboratórios de Ensaio e Auditoria (LEA): Os laboratórios de ensaios e auditoria (LEAs) são entidades formalmente vinculadas à AC Raiz, aptas a realizar os ensaios exigidos nas avaliações de conformidade e a emitir os correspondentes laudos de conformidade que embasarão a tomada de decisão, por parte da AC Raiz, quanto à homologação ou não de um dado sistema ou equipamento avaliado pelos LEAs.

9) Autoridades de Carimbo do Tempo (ACT): As autoridades de carimbo do tempo (ACTs) são entidades responsáveis pela operação dos equipamentos que, conectados à Rede de Carimbo do Tempo da ICP-Brasil, geram carimbos e os assinam em nome da ACT.

10) Titulares Finais (TF): Os titulares finais (TFs) são as entidades, pessoa física ou jurídica, para as quais são emitidos certificados digitais. O titular do certificado é responsável pela chave privada correspondente à chave pública contida no certificado e pode utilizar tanto uma quanto a outra.

11) Terceiras Partes (TP): As terceiras partes (TPs) são quaisquer pessoas físicas ou jurídicas que confiam no teor, validade e aplicabilidade dos certificados digitais, dos carimbos do tempo e demais documentos assinados digitalmente no âmbito da ICP-Brasil.

B. Regulamentos

Os regulamentos sobre os quais se alicerça a ICP-Brasil são: Medida Provisória 2.200-2 [5]; decretos; resoluções do Comitê Gestor da ICP-Brasil; instruções normativas da AC Raiz; documentos complementares. 2.2.1 MP 2.200-2

A Medida Provisória 2.200-2 [5] é o principal marco legal da ICP-Brasil. Publicada em 24.08.2001 tem força de lei, mesmo não tendo sido analisada no Congresso Nacional, haja vista que o mecanismo de "caducidade"das MPs não analisadas somente foi instituído pela Emenda Constitucional 32, de 11.09.2001.

1) Decretos: Vários decretos presidenciais tratam da regulamentação da ICP-Brasil, sendo os principais:

- DECRETO Nº 3.872 [6], que dispõe sobre o Comitê Gestor da InfraEstrutura de Chaves Públicas Brasileira - CG ICP-Brasil, sua Secretaria-Executiva, sua Comissão Técnica Executiva e dá outras providências;
- DECRETO Nº 3.996 [4] e DECRETO Nº 4.414 [7], que dispõem sobre a prestação de serviços de certificação digital no âmbito da Administração Pública Federal;
- DECRETO Nº 4.689 [8], que aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão do Instituto Nacional de Tecnologia da Informação - ITI, e dá outras providências;
- DECRETO Nº 6.605 [13], que dispõe sobre o Comitê Gestor da InfraEstrutura de Chaves Públicas Brasileira - CG ICP-Brasil, sua Secretaria-Executiva e sua Comissão Técnica Executiva - COTEC.

2) Resoluções do Comitê Gestor da ICP-Brasil: O Comitê Gestor estabelece diretrizes e normas técnicas para a formulação de políticas de certificados e regras operacionais das ACs e das ARs e define níveis da cadeia de certificação. Também atualiza, ajusta e revisa os procedimentos e as práticas estabelecidas para a ICP-Brasil, garante sua compatibilidade e promove a atualização tecnológica do sistema e a sua conformidade com as políticas de segurança. Para emanar essas diretrizes e normas, utiliza-se de Resoluções, que são analisadas pelos membros da COTEC e do Comitê Gestor e aprovadas por esses últimos em reuniões específicas.

3) Documentos ICP-Brasil: As resoluções são sucintas, limitando-se a aprovar documentos em anexo, esses sim contendo as diretrizes técnicas a serem observadas. Tais documentos são conhecidos por DOC-ICP-nn. Possuem controle de versão e qualquer alteração deve sempre ser aprovada pelo Comitê Gestor da ICP-Brasil, por meio de uma nova resolução. Para cada alteração em um DOC-ICP-nn deve ser adotado um novo número de versão. Uma nova versão consiste num documento completo, contendo todo o texto da versão anterior mais as modificações aprovadas. A Tabela I relaciona esses documentos agrupados de acordo com o assunto principal.

Tabela I
DOCUMENTOS ICP-BRASIL AGRUPADOS POR ASSUNTO

Assunto	**DOC-ICP**
Credenciamento e funcionamento das entidades	01, 02, 03, 05, 06, 07
Formato dos certificados digitais e das LCR	04
Fiscalização e auditoria das entidades credenciadas	08,09
Processo de homologação de dispositivos criptográficos	10
Carimbo do tempo	11,12,13 e 14
Formato das Assinaturas Digitais	15

III. ASSINATURAS DIGITAIS E SUA UTILIZAÇÃO COMO EVIDÊNCIA LEGAL

A. O Processo De Assinatura Digital

Assinar um documento eletrônico com uma assinatura digital é um processo de dois passos: o arquivo de computador que

contém o documento eletrônico é primeiramente submetido a um algoritmo de embaralhamento com perda, o que produz um valor conhecido por hash ou resumo criptográfico. Na segunda etapa, esse hash é então cifrado com a chave privada do signatário. O resultado dessa operação é a assinatura digital, que se constitui em um objeto digital separado do documento eletrônico em si, mas que fica associado a ele, para futura validação.

O documento eletrônico, juntamente com a assinatura digital, é apresentado para a terceira parte, que confirma sua validade ao decifrar a assinatura digital com a chave pública do signatário, obtida no certificado digital. O resultado da decifração é o valor hash do documento eletrônico, conforme gerado pelo signatário. A seguir, a terceira parte realiza, ela própria, um novo cálculo do valor hash do documento e o compara com o valor hash que recebeu junto com o documento. Se forem iguais, significa que o documento eletrônico está íntegro e que é possível identificar o signatário por meio do certificado digital. Caso contrário, a assinatura digital é inválida.

O certificado digital contém a chave pública e informações sobre a identidade do titular do certificado (proprietário da chave), o período de validade, o algoritmo de assinatura, o número de série do certificado e o nome da autoridade certificadora, entre outras informações. Os certificados digitais têm um prazo de validade limitado, mas também podem ser revogados antes do término desse período. O titular do certificado pode pedir a revogação do certificado em diversas situações, como roubo ou perda da chave privada, alteração nas informações contidas no certificado etc.

Documentos assinados digitalmente têm, muitas vezes, uma vida muito maior do que as chaves criptográficas e as tecnologias empregadas na geração da assinatura digital. Isso ocorre porque a validade das chaves é intencionalmente curta, uma vez que elas podem ser comprometidas ou podem, futuramente, ser descobertos métodos de criptoanálise que permitam descobrir com facilidade a chave privada, a partir da chave pública correspondente [29]. Como verificar, daqui a uma dezena de anos, se o certificado digital correspondente à chave privada que assinou o documento não estava expirado ou revogado, no momento da assinatura? Ou ainda, como precisar o momento em que foi realizada a assinatura?

Para tentar solucionar essa questão, podem ser utilizados carimbos do tempo, que registram data e hora no resumo criptográfico (hash) do documento digital e/ou da assinatura digital. Essa medida, todavia, remete de volta à questão inicial, uma vez que o carimbo do tempo é, ele mesmo, um conjunto de dados assinado digitalmente. Como provar, daqui a dezenas de anos, que a chave privada da Autoridade de Carimbo do Tempo não foi comprometida, ou que o carimbo não foi forjado, de alguma maneira, dada a evolução tecnológica dos computadores e o avanço na solução de problemas matemáticos hoje insolúveis?

B. Características Esperadas Das ICPs E Das Assinaturas Digitais

Uma ICP, ao fornecer certificados que podem ser utilizados para assinar digitalmente documentos eletrônicos com validade jurídica, deve prover confiabilidade e segurança em todos os processos, tanto os que envolvem o ciclo de vida do certificado digital como os que dizem respeito ao ciclo de vida da assinatura digital. Deve também prover rastreabilidade e auditoria dos processos executados, de forma a possibilitar a realização de perícias técnicas, em caso de eventuais disputas judiciais.

Essas características são fundamentais para que as assinaturas sejam usadas como evidência legal e implicam a adoção de um grande número de cuidados pelos executores das diversas atividades que compõem aqueles processos. As etapas que dizem respeito ao ciclo de vida dos certificados digitais na ICP-Brasil estão previstas e regulamentadas no DOC-ICP-05 [12], são:

- Solicitação - processo no qual é acessado o sistema da AC e preenchido formulário específico de solicitação de certificado digital;
- Validação - processo no qual o solicitante do certificado comparece a uma instalação técnica de AR e apresenta seus documentos de identidade;
- Emissão - processo no qual o solicitante, utilizando uma senha especial, recebida na AR, comanda a emissão do seu certificado;
- Revogação - processo no qual um certificado já emitido é revogado pelo próprio titular ou pela AR.

Já as etapas do ciclo de vida de uma assinatura digital, conforme DOC-ICP-15 [15], são:

- Criação - processo de criação de um resumo criptográfico;
- Verificação Inicial - processo de verificação quanto à validade de uma ou mais assinaturas digitais;
- Armazenamento - processo que trata da guarda da assinatura digital.
- Revalidação - processo que estende a validade do documento assinado.

IV. Principais Desafios Na ICP-Brasil

Neste capítulo relacionam-se questões sobre assinatura digital de documentos eletrônicos que, na visão dos autores, ainda não estão tratadas de forma adequada na ICP-Brasil e que podem comprometer a utilização desses documentos como evidência legal competente.

Todas as questões discutidas neste artigo baseiam-se na legislação publicada até 20.06.2009. Foram desconsiderados, portanto, eventuais estudos internos que possam estar em andamento na AC-Raiz e que não tenham sido aprovados pelo Comitê Gestor da ICP-Brasil e publicados no Diário Oficial da União e no sítio www.iti.gov.br [26].

A. Propostas De Adequação Na ICP-Brasil

1) Revogação de Certificados: Para verificar a situação do certificado digital quanto à revogação são utilizados dois mecanismos: as Listas de Certificados Revogados (LCRs) [23] e as consultas usando o Online Certificate Status Protocol (OCSP).

As LCRs funcionam pela publicação, em algum repositório, de uma relação de certificados que não estão mais válidos

e devem ser rejeitados pela pessoa ou aplicação que estiver realizando a validação. Essa relação pode ter tamanho variável, chegando muitas vezes a vários megabytes. Já as consultas OCSP baseiam-se no envio de uma consulta ao servidor, na qual são informados dados do certificado cuja validade se deseja verificar. O servidor emite uma resposta assinada com sua chave privada, informando a situação do certificado.

Na ICP-Brasil, embora algumas ACs disponibilizem serviço OCSP, a principal forma de validação de status de certificados é através de LCRs. O DOC-ICP-05 [12] define que cada AC deve gerar uma nova versão de LCR a cada 6 horas e publicá-la em repositório com disponibilidade de 99,5% (noventa e nove vírgula cinco por cento) do mês, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana).

Ocorre que, para evitar que as LCRs fiquem muito longas, as ACs da ICP-Brasil excluem delas os certificados revogados, após sua expiração. Esse procedimento, previsto na seção 5 da RFC 5280 [24], permite diminuir o tamanho da LCR, o que confere maior agilidade na sua importação para um sistema local. Todavia, fragiliza a automação dos processos de validação do status de certificados, pois para validar uma assinatura digital, cujo certificado correspondente já tenha expirado, será preciso consultar a LCR emitida logo depois do momento provável da assinatura.

O DOC-ICP-05 [12] no item 6.1.3, define que as ACs da ICP-Brasil devem guardar, permanentemente, todas as LCRs emitidas ao longo de sua existência, para verificações futuras, mas não faz referência alguma à disponibilização dessas LCRs. Com isso, caso as informações sobre o status dos certificados que compõem a cadeia de certificação não tenham sido capturadas no momento da geração da assinatura digital, ou pelo menos antes da expiração do certificado do titular, validar uma assinatura digital na ICP-Brasil será uma tarefa bastante difícil. Além disso, como para validar um certificado é preciso fazê-lo igualmente para os demais certificados da cadeia de certificação, essa complexidade aumenta ainda mais.

2) Preservação de Documentos Assinados Digitalmente: Um dos principais desafios com que se depara ao lidar com documentos assinados digitalmente diz respeito à sua preservação por longo prazo. Essa preocupação extrapola o âmbito da certificação digital, visto que se aplica a todos os documentos eletrônicos, sejam eles assinados digitalmente ou não.

No âmbito da ICP-Brasil, ainda não existem diretrizes sobre o caminho a adotar para manter a validade das assinaturas a longo prazo, embora já existam milhões de documentos assinados digitalmente. Somente em dezembro de 2008 foram aprovados regulamentos sobre assinaturas digitais no âmbito da ICP-Brasil [15]. Uma importante lacuna nesses regulamentos é que não definem o tratamento a ser dado aos milhões de documentos assinados antes da sua publicação e que provavelmente se encontram fora do padrão ali definido.

Finalmente, não se observa em nenhum documento da ICP-Brasil orientação sobre como armazenar os documentos assinados digitalmente, tarefa essa bastante complexa. Envolve não apenas as questões relacionadas com o arquivamento de documentos eletrônicos (migração de dados e metadados para novas mídias, sistemas operacionais e sistemas aplicativos; migração de representações e formatos de arquivos) [30].

Além de oferecer resposta todas essas questões, os responsáveis pelo armazenamento dos documentos eletrônicos assinados digitalmente devem preocupar-se em registrar todos os procedimentos realizados, de forma que seja possível provar a integridade do documento ao longo do tempo, para que ele mantenha sua capacidade de servir como evidência legal.

Muitas das pessoas ou entidades brasileiras que hoje estão de posse de documentos eletrônicos assinados digitalmente desconhecem a maneira correta de armazená-los e não há, na ICP-Brasil, definição de processos e estruturas visando à preservação adequada desses documentos no longo prazo.

Outra questão relevante é que, para verificar assinaturas digitais será necessário reconstruir de forma correta o caminho de certificação e obter informações adicionais [2] [27]; é necessário, portanto, dispor de LCRs, certificados digitais da AC, da ACT e respectivas PC, DPC, PCT, DPCT etc. Hoje a maior parte desses arquivos encontra-se na guarda das entidades que os geraram, o que pode dificultar sua recuperação a médio e longo prazo, caso não sejam realizados os procedimentos de arquivamento adequados.

Algumas ACs podem ter dificuldade de manter disponíveis até mesmo os dados mais básicos, como os certificados digitais e LCRs emitidos, por utilizarem sistemas de certificação com restrições operacionais e deficiências diversas.

Todas essas questões podem dificultar a verificação se certificado digital era válido em determinado momento do passado, o que é especialmente danoso para os casos de certificados usados em carimbos do tempo, que são utilizados, muitas vezes, como forma de garantir a validade das assinaturas digitais [25].

3) Sistemas para Geração e Verificação das Assinaturas Digitais: Para que documentos assinados digitalmente apresentem as condições técnicas necessárias e suficientes para serem úteis como evidência legal, é preciso que todos os processos relacionados com sua criação e verificação sejam realizados de forma segura. Esses processos envolvem, em maior ou menor grau, a utilização de sistemas e equipamentos criptográficos, que devem ter seu funcionamento avaliado e, de preferência, certificado por um organismo confiável, para garantir aos usuários a segurança de suas chaves privadas.

Uma solução para garantir que os sistemas estejam seguros e adequados à regulamentação brasileira seria submetê-los ao processo de homologação ICP-Brasil, criado em outubro de 2004, com a publicação do DOC-ICP-10 [9], que estabelece as regras e os procedimentos gerais que devem ser observados nos processos de homologação de sistemas e equipamentos para uso na ICP-Brasil. A especificação dos requisitos técnicos que esses sistemas e equipamentos devem atender é realizada pela AC-Raiz e publicada nos Manuais de Condutas Técnicas (MCTs).

Para equipamentos, esse modelo tem obtido relativo sucesso, na medida em que já existem dispositivos homologados e que, obrigatoriamente, a partir de 31.12.2010, todos os equipamentos criptográficos para uso na ICP-Brasil deverão ter sido previamente homologados, conforme DOC-ICP-01.01 [14].

A situação é diferente, porém no que tange aos sistemas

utilizados para geração e verificação de assinaturas digitais. Percebe-se que muitas aplicações que utilizam certificação digital não estão aptas a lidar de forma adequada com os certificados e as informações de revogação. Mesmo softwares de grandes fabricantes tratam de forma errada os bits configurados nos certificados. É comum, por exemplo, que certificados de sigilo sejam usados para realizar assinaturas.

A interpretação e o tratamento das extensões críticas ou não críticas varia de um software para outro. Muitos aplicativos não estão configurados para trabalhar corretamente com campos importantes dos certificados, como aqueles que tratam das restrições de uso aplicáveis.

Na ICP-Brasil vivenciam-se esses problemas não apenas nos sistemas operacionais, navegadores e outros programas de grandes fabricantes, mas também naqueles desenvolvidos especificamente para a realidade brasileira, como softwares de assinatura e outros aplicativos específicos, como os que tratam de nota fiscal eletrônica, por exemplo. Em todos eles, a não-implementação adequada de rotinas para tratamento da certificação digital pode comprometer a segurança e confiabilidade dos processos executados.

O documento que traz as especificações dos sistemas para geração e verificação de assinaturas digitais é o Manual de Condutas Técnicas 4 (MCT-4) [10], cuja versão mais atual foi publicada em 2007, antes, portanto, da publicação do DOC-ICP-15 [15], que regulamenta as assinaturas digitais no âmbito da ICP-Brasil.

Além de não estar ajustado à regulamentação atual sobre assinatura digital na ICP-Brasil, o MCT-4 mostra outras deficiências, se comparado, por exemplo, com o padrão utilizado na Comunidade Europeia, constante dos documentos CWA 14170 Security requirements for signature creation applications [16] e CWA 14171 General guidelines for electronic signature verification [17]. Entre elas podem ser citadas a inexistência de requisitos para autenticação biométrica do titular para acesso à sua chave privada, a não previsão de assinatura digital em ambientes distribuídos etc.

Entende-se o receio das autoridades da ICP-Brasil em exigir que todos os sistemas e aplicativos sejam homologados, haja vista que o processo pode ser demorado e caro, impactando de forma indesejada o preço e consequente utilização de dispositivos homologados. Além disso, uma vez homologado o dispositivo, é difícil que se mantenham estáticos seus componentes, o que pode gerar a necessidade de constante reavaliação pelos laboratórios, com mais custos e delongas.

Isso é mais verdadeiro ainda para os softwares, haja vista a dinâmica natural dos sistemas informatizados. Por outro lado, deixando-se a situação como está, expõe-se os usuários a riscos significativos e compromete-se a credibilidade das assinaturas geradas.

4) Tipo e Aplicabilidade dos Certificados Digitais: Na ICP-Brasil conforme DOC-ICP-04 [11] estão regulamentados apenas dois tipos de certificados para titular final: certificados de sigilo e de assinatura. Esses últimos são usados tanto para assinatura digital, propriamente dita, como para processos de autenticação do titular em servidores e aplicativos. Ocorre que esses servidores podem estar instalados em ambientes que não são controlados pelo titular. Exemplo disso se observa nas organizações que exigem que o funcionário se autentique com certificado digital para acessar suas áreas de trabalho, em computadores controlados por terceiros, como os administradores de sistemas e de redes. Com isso, gera-se um risco ao titular do certificado, pois a mesma chave privada usada para autenticação pode ser usada para assinar documentos de cunho legal e financeiro.

As chaves privadas associadas aos certificados do tipo A1 e A2 são geradas e/ou armazenadas em software e as do tipo A3 e A4 são geradas e armazenadas em hardware criptográfico. Mesmo oferecendo níveis de segurança bastante distintos, qualquer desses certificados pode, em tese, ser utilizado para assinar qualquer tipo de documento, ficando essa definição na dependência apenas do gestor do aplicativo. Com isso, os titulares de certificados do tipo A1 e A2 ficam ainda mais expostos ao risco de captura de sua chave privada para utilização em transações as mais diversas.

Outro fator que traz insegurança aos titulares de certificados ICP-Brasil é que a regulamentação atual não lhes permite estabelecer limite de valores para as transações, documentos e contratos a serem assinados com a chave privada associada ao certificado. Na Comunidade Europeia, ao contrário, essa possibilidade está prevista na própria diretiva 93/1999 [20].

Para as pessoas jurídicas, os certificados ICP-Brasil apresentam ainda deficiências importantes, que dificultam sua utilização nos processos de negócios. Uma empresa pode ter vários certificados de assinatura, cada um deles indicando uma pessoa física responsável pela guarda e uso da chave privada correspondente, conforme DOC-ICP-05 [12].

Ocorre que não é possível estabelecer, no certificado digital, segregação de funções e limitação de poderes para os responsáveis. Assim, cada um deles pode assinar, em nome da empresa, documentos de qualquer tipo e valor. Além dos problemas de segurança, isso dificulta a automação dos processos de negócios, em que existem fluxos pré-definidos de atividades, com segregação das partes executantes e nos quais os sistemas devem analisar as assinaturas digitais e sua relação com o documento, ou seja, identificar se o documento admite uma assinatura digital de uma pessoa e qual o papel dela no processo.

Vê-se, assim, que os tipos e aplicabilidade dos certificados ICP-Brasil não atendem às atuais necessidades da sociedade e podem ensejar, no futuro, alegações de que algum documento foi assinado sem a expressa vontade e consentimento do titular do certificado ou do responsável legal pela chave privada.

V. Adequações Propostas Para A ICP-Brasil

Neste capítulo propõe-se um conjunto de medidas que buscam auxiliar a equacionar os desafios, medidas essas que se aplicam especificamente à ICP-Brasil e que visam solucionar apenas questões técnicas relacionadas com documentos eletrônicos assinados digitalmente e sua utilização como evidência legal.

A. Revogação de certificados

1) Implantação Obrigatória de Serviço de Validação Online do Status dos Certificados: Para eliminar a situação que se

vivencia hoje na ICP-Brasil, com a defasagem das informações de revogação, todas as ACs (exceto a Raiz) devem oferecer obrigatoriamente, um serviço online de validação de status de certificados, que pesquise a base de dados de certificados emitidos e forneça uma resposta binária, ou seja:

- o certificado é válido: consta da lista de certificados emitidos pela AC e não está revogado; ou
- o certificado não é válido: não consta da lista de certificados emitidos pela AC ou está revogado.

Esse modelo de serviço de verificação online é diferente do que está proposto na RFC 2560, mas equipara-se ao que vem sendo usado em países da Comunidade Europeia, como a Alemanha, conforme Menke [28]. Essa medida tem vários pontos positivos:

- elimina os inconvenientes apresentados pelas LCRs e serviço OCSP tradicional, de fornecer informação defasada e/ou incompleta;
- permite que a certificação digital seja usada de forma mais intensa para processos críticos, como transações financeiras;
- diminui a carga na rede, por evitar a baixa de LCRs.

Na regulamentação desse novo serviço devem ser igualmente tratados pontos importantes a ele relacionados, como a inclusão, nos certificados de titulares finais, da extensão AuthorityInfoAccess, que indica como acessar informações e serviços da AC emitente do certificado, entre eles o serviço OCSP.

B. Preservação de Documentos Assinados Digitalmente

1) Regulamentação do serviço de arquivamento de documentos assinados: Uma medida prioritária para a ICP-Brasil é a regulamentação dos procedimentos a serem adotados para arquivamento de documentos assinados digitalmente, assunto que não é tratado em nenhum dos documentos da ICP-Brasil. Para a criação desses novos regulamentos é importante o envolvimento do Arquivo Nacional, que poderá contribuir na definição das políticas e práticas arquivísticas a serem observadas, considerando ainda as necessidades dos usuários dessas informações no futuro [18].

Entre essas práticas, tem-se:

- carimbos do tempo emitidos por Autoridades de Carimbo do Tempo confiáveis;
- concatenação de valores de hashes criptográficos;
- apresentação de evidências para grupos de documentos digitais;
- cadeias de carimbos do tempo de arquivamento.

Nessa regulamentação, deve ser prevista a criação de uma nova categoria de entidade: o Prestador de Serviços de Arquivamento (PSA), responsável pela guarda de forma confiável de documentos assinados digitalmente no longo prazo. Os objetivos primários de um PSA são dar suporte ao não-repúdio da existência de dados, integridade e origem [3].

Esse tipo de entidade já existe na Comunidade Europeia, que, premida pela necessidade de arquivar os documentos relativos a faturas eletrônicas assinadas digitalmente, criou em 2007 o padrão ETSI TS 102573 Policy requirements for trust service providers signing and/or storing data for digital accounting [19].

2) Criação de Repositório Seguro de Informações Críticas: Foi destacada a importância em guardar informações complementares para validar assinaturas digitais no futuro, como LCRs, certificados digitais de AC e diferentes versões de PC, DPC, PCT, DPCT etc. Hoje essas informações estão armazenadas nas diferentes ACs e ACTs, o que pode dificultar sua recuperação, no futuro.

A proposta é que a AC-Raiz brasileira crie um repositório seguro com essas informações (ou designe um Prestador de Serviços para isso), de forma a garantir sua preservação e disponibilidade adequada.

3) Criação de manuais orientando os usuários sobre o tratamento do legado: Conforme Resolução 62 do CG da ICP-Brasil, de 09.01.2009 [15], a definição dos critérios para validação dos documentos assinados digitalmente usando certificados ICP-Brasil em formatos não padronizados foi deixada a cargo das partes interessadas. Como essa definição pode ser complicada, especialmente para usuários leigos que não disponham de estrutura organizacional para apoiá-los, cabe à AC-Raiz criar um Guia, orientando-os sobre as formas como pode ser realizada a validação e sobre os consequentes procedimentos a que os documentos assinados devem ser submetidos, em cada caso.

4) Inclusão de orientações sobre arquivamento a longo prazo de documentos assinados digitalmente nos termos de titularidade: No momento em que recebe o certificado digital, o titular assina e recebe uma cópia do Termo de Titularidade, documento no qual constam seus dados de identificação e uma relação resumida de seus deveres como titular de um certificado ICP-Brasil. A minuta desse termo está estabelecida em adendo do DOC-ICP-05 [12] e deve ser adotada por todas as ACs credenciadas. Propõe-se que sejam incluídas nesse documento orientações sobre os procedimentos que o titular deve adotar em relação aos documentos assinados digitalmente, com vistas a manter as características adequadas para utilização como evidência legal, no futuro.

C. Sistemas para Geração e Verificação das Assinaturas Digitais

1) Regulamentação do Processo de Validação de Certificados e Assinaturas Digitais: A regulamentação do processo de validação de certificados e assinaturas digitais é necessária para evitar a implementação incorreta desse processo nas aplicações, o que pode gerar consequências indesejadas, como a aceitação de certificados inválidos ou revogados ou a validação de assinaturas sem as características esperadas.

Nenhum dos documentos da ICP-Brasil trata do assunto, motivo pelo qual deverá ser criado novo conjunto de documentos, incorporando essa proposta.

2) Regulamentação do Serviço de Validação de Certificados e Assinaturas Digitais: Mesmo com a regulamentação do processo de validação de certificados e assinaturas digitais, usuários e desenvolvedores podem preferir delegar essa atividade a entidades especializadas. Propõe-se, por isso, a criação de Prestadores de Serviço de Verificação (PSV), entidades

credenciadas na ICP-Brasil para realizar os processos de criação de caminhos de certificação e validação do status de certificados. Esses prestadores também poderiam validar até mesmo as assinaturas digitais como um todo, e não apenas o caminho de certificação, simplificando essa atividade para usuários finais e aliviando as aplicações para que possam se concentrar nas atividades-fim a que se destinam.

Essa solução se assemelha à proposta na RFC5055 [21], que define um protocolo que permite a um cliente delegar a um servidor a criação do caminho de certificação e a validação dos certificados.

3) Implantação de Declaração de Conformidade para Sistemas: Viu-se a importância de oferecer aos usuários sistemas para geração e verificação de assinaturas seguros e alinhados com os regulamentos da ICP-Brasil. A garantia de que esses dispositivos atendem a tais características poderia ser obtida pela homologação junto a laboratórios especializados, mas essa alternativa encareceria os produtos e inibiria o lançamento de novas versões.

Para solucionar essa questão, propõe-se estratégia semelhante à adotada na Alemanha [1], em que os fabricantes de produtos para assinaturas digitais devem fornecer declaração pública de que seus produtos estão em conformidade com os requisitos de segurança estabelecidos nos regulamentos da ICP-Brasil. Uma cópia escrita deve ser depositada na AC-Raiz, que publicaria no seu sítio a lista desses dispositivos "declarados confiáveis", para conhecimento dos titulares de certificados e terceiras partes.

D. Tipos e Aplicabilidade dos Certificados Digitais

1) Criação de Infraestrutura para Emissão de Certificados de Atributos: Um certificado de atributo é uma estrutura de dados contendo um conjunto de atributos para uma entidade final e alguma outra informação. Essa estrutura é assinada digitalmente por uma entidade confiável. O certificado de atributo não possui chave pública: é utilizado em conjunto com um certificado de chave pública, adicionando atributos ao detentor desse certificado. Assim os atributos constantes no certificado de atributo podem ser alterados ou mesmo revogados sem que isso implique a revogação do certificado de chave pública. Os certificados de atributos podem ser usados para diversas finalidades, como:

- identificação de profissionais que pertencem a determinada categoria;
- identificação e definição de cargos/hierarquias de funcionários e servidores de empresas ou órgãos públicos;
- identificação de pessoas que fazem jus a determinado direito (ex.: bolsa-família;)
- restrição de acesso de determinados usuários à aplicações;
- delegação de poderes (procuração).

Os padrões internacionais que tratam dessa matéria são a RFC 3281 An Internet Attribute Certificate [23] e o documento ETSI TR 102 044 Electronic Signatures and Infrastructures (ESI); Requirements and role for attribute certificates [19]. Neles está prevista a criação de dois tipos de entidades: a Autoridade Designadora de Atributos e a Autoridade Emissora de Atributos. A primeira possui autoridade sobre determinado atributo, podendo designar quem poderá obter um certificado com aquele atributo (por exemplo, um conselho de classe pode designar quais são os profissionais habilitados a exercer a profissão). Já a autoridade emissora realiza a emissão do certificado de atributo, em condições semelhantes às utilizadas para emissão de certificados digitais: ambientes com requisitos elevados para segurança física, lógica e de pessoal etc.

Para a ICP-Brasil, além de definir as entidades que irão compor essa nova infraesturutura, é preciso detalhar suas funções, regras de acreditação e funcionamento, tipos de dispositivos a utilizar, procedimentos a serem observados pelos agentes de registro para validação dos atributos, forma e condições de revogação de atributos etc.

2) Alteração nos certificados ICP-Brasil: Viu-se que os tipos de certificados atualmente disponíveis na ICP-Brasil não atendem adequadamente às necessidades dos titulares, trazendo mesmo riscos de segurança aos seus usuários.

Propõe-se, assim, a criação de um novo tipo de certificado: o certificado de autenticação, que se destina apenas a permitir ao titular acesso a sistemas diversos, não podendo ser utilizado para assinatura digital de documentos. As chaves criptográficas desse tipo de certificado podem estar armazenadas em software ou em hardware criptográfico, visto que seu uso restrito não ensejará graves prejuízos, em caso de captura por terceiros.

Esse tipo de certificado é usado em países como Portugal e Bélgica, que incorporam em seus documentos de identidade certificados digitais de assinatura e de autenticação, armazenados em áreas distintas dos cartões inteligentes. Isso permite que o certificado de autenticação seja utilizado em variados ambientes, como serviços médicos e escolas (o que propicia às autoridades a obtenção de dados para programas sociais), preservando a segurança da chave privada de assinatura.

VI. Conclusões e Trabalhos Futuros

O objetivo deste artigo foi estudar a situação atual dos regulamentos da ICP-Brasil para verificar se contemplam os aspectos relevantes para conferir aos documentos assinados digitalmente as características técnicas necessárias e suficientes para serem úteis, efetivamente, como evidência legal, mesmo por longo prazo.

Para tanto, analisaram-se os regulamentos da ICP-Brasil, confrontando-os com os padrões internacionais que tratam do assunto e a legislação de outros países e blocos econômicos. Isso permitiu apontar lacunas na legislação brasileira que necessitam ser sanadas. A principal delas diz respeito ao armazenamento de documentos assinados digitalmente, que exige a adoção de uma série de procedimentos periódicos, como a revalidação das assinaturas, para preservar a eficácia dos documentos. Esse assunto não é regulamentado em nosso País e muitos usuários desconhecem a necessidade de executar tais procedimentos. Também foram detectadas lacunas na regulamentação que trata da revogação de certificados, dos sistemas para geração e verificação das assinaturas digitais, e dos tipos e aplicabilidade dos certificados digitais.

Recomendou-se, para cada lacuna, medidas que podem contribuir para saná-las. Entre tais medidas estão a criação

de novas entidades e de novos serviços na ICP-Brasil, a modificação de serviços já existentes, a alteração dos tipos de certificados utilizados na ICP-Brasil, a criação de manuais e documentos para orientar os usuários e a definição de novo processo para a homologação de sistemas.

Trabalhos futuros na área podem compreender:

- detalhamento dos assuntos cuja regulamentação está sendo proposta, com vistas a subsidiar a elaboração dos regulamentos brasileiros;
- análise de lacunas na regulamentação brasileira com relação a outros pontos relevantes, como proteção de dados pessoais;
- utilização da certificação digital em carteira de identificação.

REFERÊNCIAS

[1] ALEMANHA (2001). German Bundestag. Ordinance on Electronic Signatures (Signatures Ordinance - SigV). Novembro 2001.

[2] ALEMNEH, D.; HASTINGS, S.; HARTMAN, C. (2002). A metadata approach to preservation of digital resources: The University of North Texas Libraries' experience, First Monday Journal, v. 7, n. 8. Agosto 2002.

[3] BLAZIC, A.; KLOBUCAR, T.; JERMAN, B. (2007). Long-term trusted preservation service using service interaction protocol and evidence records. Computer Standards and Interfaces, v. 29, e. 3, p. 398-412. Março 2007.

[4] BRASIL. Poder Executivo. Decreto n. 3.996, de 31 de outubro de 2001. Dispõe sobre a prestação de serviços de certificação digital no âmbito da Administração Pública Federal. Brasília, DF.

[5] BRASIL. Poder Executivo. Medida Provisória nº 2.200-2, de 24 de agosto de 2001. Brasília, DF.

[6] BRASIL. Poder Executivo. Decreto N. 3.872, de 18 DE julho de 2001. Dispõe sobre o Comitê Gestor da Infra-Estrutura de Chaves Públicas Brasileira. Brasília. DF. DOU DE 19/7/2001.

[7] BRASIL. Poder Executivo. Decreto N. 4.414, de 31 de outubro de 2001. Altera o Decreto no 3.996. Brasília. DF.

[8] BRASIL. Decreto nº 4.689, de 07 de maio de 2003. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão do Instituto Nacional de Tecnologia da Informação - ITI, e dá outras providências. Poder Executivo, Brasília, DF.

[9] BRASIL. Comitê Gestor da ICP-Brasil. Resolução N° 33, de 21 de outubro de 2004 - Delega à AC Raiz da ICP-Brasil atribuição para suplementar as normas do Comitê Gestor e dá outras providências. Infraestrutura de Chaves Públicas Brasileira.

[10] BRASIL. Instituto Nacional de Tecnologia da Informação. Manual de Condutas Técnicas 4 - Volume I - Requisitos, Materiais e Documentos Técnicos para Homologação de Softwares de Assinatura Digital no Âmbito da ICP-Brasil. versão 2.0. São Paulo, 22 de novembro de 2007.

[11] BRASIL. Comitê Gestor da ICP-Brasil. Resolução N° 53, de 28 de Novembro de 2008 - Altera os Requisitos Mínimos para as Políticas de Certificado na ICP-Brasil (DOC-ICP-04). Infraestrutura de Chaves Públicas Brasileira.

[12] BRASIL. Comitê Gestor da ICP-Brasil. Resolução N° 54, de 28 de Novembro de 2008 - Altera os Requisitos Mínimos para as Declarações de Práticas de Certificação das Autoridades Certificadoras da ICP-Brasil (DOC-ICP-05). Infraestrutura de Chaves Públicas Brasileira.

[13] BRASIL. Poder Executivo. Decreto Nº 6.605, de 14 de outubro de 2008. Dispõe sobre o Comitê Gestor da Infra-Estrutura de Chaves Públicas Brasileira -CG ICP-Brasil, sua Secretaria-Executiva e sua Comissão Técnica Executiva - COTEC. Brasília, DF.

[14] BRASIL. Comitê Gestor da ICP-Brasil. Padrões e Algoritmos Criptográficos da Infra-Estrutura de Chaves Públicas Brasileira (DOC ICP-01.01). Versão 2.0. Brasília. ICP-BRASIL.

[15] BRASIL. Comitê Gestor da ICP-Brasil. Resolução N° 62 de 09 de janeiro de 2009. Aprova a versão 1.0 do documento Visão Geral sobre Assinaturas Digitais na ICP-Brasil (DOC-ICP-15). Infraestrutura de Chaves Públicas Brasileira.

[16] CEN. European Committee for Standardization. CWA 14170 Security requirements for signature creation applications. Maio 2004.

[17] CEN. European Committee for Standardization. CWA 14171 General guidelines for electronic signature verification. Maio 2004.

[18] DOYLE, J.; VIKTOR, H.; PAQUET, E. (2007). Long term digital preservation - An end user's perspective, Sch. of Inf. Technol. and Eng., Ottawa, Univ., Ottawa, ON - Digital Information Management, 2007. ICDIM '07. 2nd International Conference on, v. 1, p. 146 - 151. Lyon, Outubro 2007.

[19] ETSI. European Telecommunications Standards Institute. Electronic Signatures and Infrastructures (ESI); Requirements for role and attribute certificates. ETSI TR 102 044. Dezembro 2002.

[20] EUROPA. Parlamento Europeu. Comissão das Comunidades Europeias. Diretiva 1999/93/CE de 13 de Dezembro de 1999, relativa a um quadro legal comunitário para as assinaturas eletrônicas. Jornal Oficial da União Européia. 19 de janeiro de 2000.

[21] FREEMAN, T. et al.(2007). RFC 5055 - Server-Based Certificate Validation Protocol (SCVP). Internet Engineering Task Force.

[22] GUTMAN, P. PKI: It's Not Dead, Just Resting. IEEE Computer. Agosto 2002.

[23] HOUSLEY, R.; FARRELL, S. (2002). RFC 3281 - An Internet Attribute Certificate Profile for Authorization. Internet Engineering Task Force.

[24] HOUSLEY, R. et al. (2008). RFC 5280 - Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile. Internet Engineering Task Force.

[25] ILIADIS, J. et al. (2003). Towards a framework for evaluating certificate status information mechanisms. Computer Communications, p. 1839-1850, v. 26, n. 16. 2003.

[26] ITI. Instituto Nacional de Tecnologia da Informação. Legislação da ICP-Brasil. 2009.

[27] LEKKAS, D.; GRITZALIS, D. (2007). Long-term verifiability of the electronic healthcare records' authenticity, International Journal of Medical Informatics, Volume 76, Issues 5-6, Virtual Biomedical Universities and E-Learning and Secure eHealth: Managing Risk to Patient Data - E-Learning and Secure eHealth Double S.I., p. 442-448. Maio-Junho 2007.

[28] MENKE, F. (2008). Die elektronische Signatur im deutschen und brasilianischen Recht: Eine rechtsvergleichende Studie (A assinatura eletrônica no direito alemão e brasileiro - um estudo comparado). Defendida perante a Universidade de Kassel, dezembro de 2008, pendente de publicação.

[29] STAPLETON, J.; DOYLE, P.; ESQUIRE, S. (2005). The digital signature paradox, Information Assurance Workshop, 2005. IAW '05. Proceedings from the Sixth Annual IEEE SMC, p. 456 - 457.

[30] THOMAZ, K. (2003). I Congresso de Tecnologias para Gestão de Dados e Metadados do Cone Sul.

Viviane Bertol Possui graduação em Engenharia Civil pela Universidade Federal do Rio Grande do Sul. (1980), Mestrado em Engenharia Elétrica pela Universidade de Brasília (2001) e Doutorado em Engenharia Elétrica pela Universidade de Brasília (2009). Trabalhou durante 15 anos nas áreas de redes de computadores e auditoria de sistemas do Banco do Brasil e durante 7 anos no Instituo Nacional de Tecnologia da Informação. Atualmente é consultora em certificação digital.

Rafael Timótel Jr. Graduado em Engenharia Elétrica pela Universidade Federal da Paraíba, Campina Grande (1984), mestrado (DEA) em Telemática e Sistemas de Informação pela Ecole Supérieure d'Electricité - SUPELEC (1985) e doutorado em Processamento de Sinais e Telecomunicações pela Université de Rennes I (França, 1988). Fez pós-doutorado na Ecole Supérieure d'Electricité - SUPELEC (2006-2007). Atualmente é professor adjunto da Universidade de Brasília, curso de Engenharia de Redes de Comunicação.

Laerte Peotta de Melo Possui graduação em Elétrica com ênfase em Eletrônica pela Universidade Presbiteriana Mackenzie-SP (1996), especialização em segurança de redes de computadores pela Universidade Católica de Brasília (2004), perito forense computacional pela Universidade Federal do Ceará (2007), Mestrado em Engenharia Elétrica pela Universidade de Brasília (2008). Atualmente é Doutorando Pesquisador pelo Banco do Brasil, trabalhando na área de segurança da informação.