Propostas para apoiar a preservação documental de longo prazo na ICP-Brasil

Rafael Timóteo de Sousa Jr[1]., Ricardo Felipe Custódio[2], Viviane Bertol[1]

[1] Universidade de Brasília, Faculdade de Tecnologia, Departamento de Engenharia Elétrica (ENE) - *Campus* Universitário Darcy Ribeiro, Brasília – BRASIL - CEP 70910-900 - Fax: +55 61 3274 6651 Telefones: +55 61 3307 2308 e 3273 5977

[2] Universidade Federal de Santa Catarina, Centro Tecnológico, Departamento de Informática e Estatística - *Campus* Universitário Cx.P. 476 - Florianópolis – SC - BRASIL - CEP 88040-900 Fax: +55 048 3721-7553 Telefone: +55 048 3721-9498

desousa@unb.br, custodio@inf.ufsc.br, bertol_viviane@yahoo.com

Resumo. Documentos eletrônicos estão sendo cada vez mais utilizados como substitutos para documentos em papel. A essa tecnologia somam-se as assinaturas eletrônicas – dentre as quais encontram-se as assinaturas digitais - que permitem conferir autenticidade e/ou autoria a um documento eletrônico. Uma importante questão que surge em decorrência da utilização de documentos eletrônicos assinados digitalmente é como preservá-los adequadamente no longo prazo. Neste artigo tratamos da preservação desse tipo de documentos, dando ênfase à situação na ICP-Brasil, a infraestrutura de chaves públicas criada pelo Governo brasileiro em 2001. Propomos diversas medidas com o objetivo de prover segurança aos processos de geração, guarda e recuperação de documentos eletrônicos assinados digitalmente no âmbito da ICP-Brasil.

Palavras-chave: ICP-Brasil, Assinatura Digital, Documento Eletrônico, Preservação a longo prazo

1 INTRODUÇÃO

Os documentos eletrônicos estão sendo cada vez mais utilizados pela sociedade como substitutos para os documentos em papel. Outra tecnologia que se soma ao documento eletrônico é a assinatura eletrônica, que permite assinar um documento eletrônico conferindo-lhe autenticidade ou autoria. Uma assinatura eletrônica pode ser obtida por meio de diversos dispositivos ou sistemas, como login/senha, biometria, impostação de PIN etc. Um dos tipos de assinatura eletrônica é a assinatura digital, que utiliza pares de chaves criptográficas associados a certificados digitais.

Essa situação levanta questões diversas, sendo uma delas: como preservar adequadamente um documento eletrônico assinado digitalmente, para que esteja disponível aos usuários legítimos no futuro? Estudos sobre esse tema estão sendo realizados por diversas áreas de pesquisa, sendo que muitos deles já sendo aplicados em projetos experimentais, porém não existe, ainda, um consenso sobre a melhor forma de se preservar esses documentos.

Neste artigo trata-se da preservação de documentos eletrônicos assinados digitalmente e dá-se ênfase às questões relacionadas com a preservação de documentos eletrônicos assinados com a utilização de chaves criptográficas privadas associadas a certificados digitais emitidos no âmbito da ICP-Brasil.

A ICP-Brasil é uma infraestrutura de chaves públicas criada pelo Governo Brasileiro em 2001, por meio da Medida Provisória 2.200-2, para emissão de certificados digitais que permitem aos seus titulares criar assinaturas digitais que possuam validade jurídica semelhante a de assinaturas de punho, perante a legislação brasileira.

Documentos assinados digitalmente no âmbito da ICP-Brasil estão sendo amplamente utilizados em inúmeras áreas de importância para o Brasil. Por esse motivo, a segurança desses documentos e a possibilidade de sua validação e recuperação no longo prazo são questões relevantes para o País.

O objetivo deste trabalho é analisar os processos utilizados atualmente para geração, arquivamento e recuperação de documentos assinados digitalmente no âmbito da ICP-Brasil e sugerir melhorias que facilitem sua preservação e validação segura no longo prazo.

Na sessão 2 faz-se um breve apanhado dos trabalhos científicos realizados sobre preservação documental e sobre preservação de documentos assinados digitalmente. Na sessão 3 propõem-se medidas, que agregariam segurança e aumentariam a disponibilidade dos documentos assinados no âmbito da ICP-Brasil. Essas medidas são analisadas na sessão 4 e as conclusões relatadas na sessão 5.

2 PRESERVAÇÃO DE DOCUMENTOS ASSINADOS DIGITALMENTE

2.1 Preservação de Documentos Eletrônicos

Segundo Thomaz [1], preservar informação em formato digital é mais difícil que preservar informação em formatos tradicionais, pois:

- a informação digital está cada vez mais distribuída;
- dados e metadados devem ser migrados para novas mídias, sistemas operacionais e sistemas aplicativos;
- representações e formatos devem obrigatoriamente acompanhar novas tecnologias e padrões;
- a informação digital precisa ser prontamente transportada de arquivo a arquivo.
- Uma das primeiras instituições a se preocupar com esse assunto foi o *National Space Science Data Center*, da NASA, que criou um comitê consultivo para preservação de dados espaciais, composto por um grupo internacional de agências espaciais.

Esse comitê desenvolveu diversos padrões independentes de área científica e se tornou, por volta de 1990, um grupo de trabalho do ISO TC 20/ SC 13.

A tarefa inicial foi o desenvolvimento de um modelo de referência para estabelecer termos e conceitos comuns. A seguir, o grupo definiu técnicas formais para especificação, como Diagramas de Fluxo de Dados para modelos funcionais e interfaces, e *Unified Modeling Language* (UML) para classes de dados. Por fim, foram desenvolvidos novos padrões para tratamento de arquivos.

O trabalho final, chamado de modelo de referência OAIS (*Open Archive Information System)* foi aprovado para publicação como padrão ISO 14721:2003 [2] em Fevereiro de 2003.

A ISO 14721:2003 especifica um modelo de referência para um sistema aberto de arquivamento de informação. O objetivo da ISO 14721:2003 é estabelecer um sistema para arquivar a informação, tanto digital quanto físico, com uma estrutura de organização composta de pessoas que aceitam a responsabilidade de preservar a informação e de torná-la disponível a um dado agrupamento de usuários.

Suas diretrizes aplicam-se a quaisquer tipos de organizações, mas principalmente para organizações com responsabilidade de tornar informação disponível por longo prazo como Arquivos, Bibliotecas e Centros de Pesquisa. Interessa, também, àquelas organizações e indivíduos que criam informação que pode vir a necessitar de preservação por longo prazo e àquelas que necessitam obter informação desses arquivos.

Outra iniciativa importante vem sendo conduzida pelo Public Record Office Victoria (PROV) da Austrália. Trata-se do projeto The Victorian Electronic Records Strategy (VERS), que objetiva fornecer uma solução de baixo custo para o problema de capturar, gerenciar e preservar registros eletrônicos no longo prazo. É um conjunto de padrões, guias, treinamentos, consultoria e projetos de implementação, centrado no objetivo de conferir confiabilidade e autenticidade aos registros eletrônicos arquivados. [3].

2.2 Preservação de Documentos Eletrônicos Assinados Digitalmente

Se já é um desafio armazenar documentos eletrônicos, um desafio ainda maior surge quando esses dados são assinados digitalmente. Isso ocorre porque a verificação da validade de uma assinatura digital depende da existência de diversas informações, além do próprio documento assinado. Entre essas informações estão:

- os certificados das autoridades certificadoras que compõem a cadeia de certificação
- as listas de certificados revogados ou as informações sobre revogação que foram obtidas quando da geração ou verificação da assinatura.

Além disso, muitas vezes é necessário que uma assinatura digital seja verificada muito tempo depois do prazo de validade dos certificados e dos carimbos de tempo que porventura tenham sido utilizados no documento eletrônico. Paralelamente, novas tecnologias podem ter surgido nesse intervalo de tempo, fragilizando os mecanismos criptográficos utilizados na geração da assinatura. Tudo isso implica a adoção de medidas adicionais, visando preservar a integridade da assinatura, tais como reassinatura, impostação de carimbos do tempo etc.

No meio acadêmico internacional, diversos autores já estudam o problema, como Ansper, Buldas e Willemson, que tratam da especificamente da validação de assinaturas a longo prazo em seu artigo [4]. Propõem a utilização de protocolo baseado em cadeias de *hashes*, que prescinde da utilização de notários ou terceiras partes confiáveis para garantir a validade das assinaturas.

No artigo [5], os autores Gritzalis e Lekkas questionam a utilização de cadeias de *hashes*, dada a dificuldade em fazer-se a conferência, num futuro distante, de todas as assinaturas apostas pelas autoridades de carimbo tempo, dado que essas podem nem mais existir, ou não ser mais confiáveis, na época da validação da assinatura. Além disso, citam as dificuldades que podem ocorrer em função das diferentes tecnologias e equipamentos usados ao longo do tempo, para geração e validação dos carimbos e assinaturas. Sugerem um esquema de Notarização Cumulativa, que, apesar de facilitar a validação das assinaturas, traz implícita a necessidade de que haja confiança nos notários por parte dos usuários da ICP.

No artigo [6], os autores Maniatis e Baker propõem, ao invés do uso de notarização, a utilização de mecanismos de carimbo do tempo combinados com um Serviço de Arquivamento de Chaves. Esse serviço guardaria em repositório seguro as chaves das Autoridades Certificadoras da ICP. Periodicamente, seus arquivos seriam carimbados por uma Autoridade de Carimbo de Tempo, como forma de provar aos usuários a existência dos certificados da AC, em dado instante de tempo. Com isso, entendem que ficaria assegurada a validação dos certificados emitidos, com a preservação da cadeia de certificação. Poderiam também ser arquivados nesse repositório seguro documentos, certificados digitais, trilhas de auditoria e demais arquivos com dados de grande valor.

O PKIX também tem buscado soluções para o problema. A RFC4810 *Long-Term Archive Service Requirements* [7] descreve uma classe de serviços de arquivamento para suportar a verificação de documentos assinados digitalmente a longo prazo e os requisitos técnicos para interagir com esse serviço. A RFC4998 *Evidence Record Syntax (ERS)* [8] especifica a sintaxe e o processamento de um Registro de Prova, que é uma estrutura destinada a apoiar por longo prazo o não-repúdio de dados existentes permitindo aos usuários provar a existência e a integridade dos dados, inclusive os assinados digitalmente.

No mercado, já existem soluções que utilizam processos de preservação que cuidam tanto da integridade como da autenticidade dos documentos digitais, fornecendo provas da autenticidade do documento. Porekar [9] examina essas soluções para determinar as melhores práticas de arquivamento no longo prazo e as captura de uma forma mais abstrata, num nível genérico, fornecendo um conjunto de padrões de segurança para arquivamento.a longo prazo. Classifica esses padrões em 4 categorias:

- 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.

A questão dos requisitos a serem observados pelos serviços de arquivamento de longo prazo também é analisada em [10], que propõe a criação de uma classe de

serviços que satisfaça os requisitos de preservação das características dos objetos de dados, interação entre os objetos arquivados, gerenciamento dos objetos arquivados, manutenção de sua integridade e evidências, política de arquivamento, agrupamento de objetos, transferência de dados e confidencialidade dos dados.

Por outro lado, a comunidade arquivística olha com certa desconfiança para a tecnologia de assinatura digital. Nos dizeres de Boudret [11]:

"....fica evidente que, a partir de um ponto de vista puramente arquivístico, as assinaturas digitais não são um método adequado para provar a autenticidade e integridade dos registros eletrônicos. Na área de autenticidade, as assinaturas digitais não dizem nada sobre a identidade dos registros eletrônicos. A declaração de autenticação nada mais é do que uma prova de que o documento foi assinado por algo / alguém na posse da chave privada do signatário. No que diz respeito à integridade, uma assinatura digital só prova que os bits transmitidos do documento estão intactos. As assinaturas digitais não impedem corrupções ou manipulações não permitidas."

Blanchette [12] define a dicotomia entre as abordagens técnica e arquivística como *"um choque entre dois conceitos diferentes de autenticidade eletrôn*ica". O primeiro conceito, abraçado pela comunidade técnica e por segmentos da comunidade legal, baseia-se na medição de uma propriedade física do documento: a integridade dos bits. Um documento é considerado íntegro se os bits que o compõem estão íntegros. O segundo conceito, abraçado pela comunidade arquivística, é de que a integridade de um documento pode ser melhor atestada analisando-se a integridade do contexto que envolve o documento, ou seja "*a totalidade dos controles e procedimentos, sejam humanos ou baseados em computadores, que asseguram a identidade e integridade de um registro eletrônico através de todo seu ciclo de vida."*

A solução para essa dicotomia está sendo buscada a partir de trabalhos conjuntos das comunidades envolvidas. Diversas iniciativas abrangentes vêm sendo realizadas. Uma das mais conhecidas é o InterPARES, acrônimo para International Research on Permanent Authentic Records in Electronic Systems, que visa a desenvolver o conhecimento essencial para a preservação a longo prazo de registros autênticos criados e/ou mantidos em forma digital e a prover as bases para padrões, políticas, estratégias e planos de ação capazes de assegurar a longevidade desse material e habilitar seus usuários a confiar em sua autenticidade.

Segundo Dumortier [13], que analisou a questão da preservação documental no ambiente da Comunidade Europeia, é necessário desenvolver padrões baseados nas melhores práticas e criar regulamentações que sirvam como uma janela legal mínima, de forma a trazer confiabilidade e estabilidade aos usuários de assinaturas digitais. Deve-se também reduzir a necessidade de migração usando padrões abertos para formatos de documentos (ex.: XML) e estimular a criação de serviços de arquivamento confiáveis, possivelmente separando serviços de arquivamento "normal" dos serviços de arquivamento "com guarda de assinatura".

A aplicação desses princípios já pode ser observada na Comunidade Europeia que, premida pela necessidade de arquivar os documentos relativos a faturas eletrônicas assinadas digitalmente, emitidas em diferentes países do bloco, criou em 2007 o padrão *ETSI TS 102573 Policy requirements for trust service providers signing and/or storing data for digital accounting* [14], que especifica os requisitos aplicáveis

aos Prestadores de Serviços de Confiança que assinam documentos fiscais eletrônicos relevantes e/ou os arquivam, em nome da pessoa taxada. Esse documento regulamenta a produção e a guarda de forma confiável dos documentos fiscais, mesmo por mais de dez anos. Admite para isso a utilização de medidas técnicas ou organizacionais, desde que permitam preservar o documento de forma adequada.

2.3 Situação na ICP-Brasil

A preservação de documentos eletrônicos no Brasil vem sendo objeto de atenção de diversas entidades, entre as quais o Arquivo Nacional, que está conduzindo estudos sobre criação, manutenção e recuperação de arquivos a longo prazo, com base no modelo OAIS.

Em 2003 foi criado, pelo Decreto 4915/2003, o Sistema de Gestão de Documentos de Arquivo - SIGA, pelo qual se organizam, sob a forma de sistema, as atividades de gestão de documentos de arquivo no âmbito dos órgãos e entidades da administração pública federal.

Em abril de 2007 foi publicada a Resolução 25, do CONARQ [15], que dispõe sobre a adoção do Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos (e-ARQ Brasil) pelos órgãos e entidades integrantes do Sistema Nacional de Arquivos - SINAR. Esse modelo orienta os responsáveis pela especificação, desenvolvimento e utilização de sistemas que tratam de preservação de informações eletrônicas, com relação aos procedimentos e operações técnicas para gestão dessas informações.

No meio acadêmico brasileiro há algumas entidades trabalhando nesse tema, como o Labsec, da Universidade Federal de Santa Catarina, que há vários anos realiza pesquisas sobre esse assunto, como se pode ver pelas publicações no sítio http://www.labsec.ufsc.br.

Quanto à preservação de documentos eletrônicos assinados digitalmente no âmbito da ICP-Brasil, o assunto somente foi regulamentado em 2009, com a publicação da Resolução 62 do Comitê Gestor [16]. Esse regulamento, todavia, tem por foco principal o formato das assinaturas, deixando em aberto algumas questões que podem comprometer o objetivo de propiciar segurança e disponibilidade no longo prazo aos documentos assinados digitalmente.

Tendo em vista que os certificados ICP-Brasil podem ser utilizados para assinar digitalmente documentos eletrônicos com validade jurídica, todos os processos que envolvem o ciclo de vida do certificado digital e da assinatura digital devem ser realizados com confiabilidade e segurança, contemplando-se, inclusive, requisitos de rastreabilidade e auditoria dos eventos crítico, para possibilitar a realização de perícias técnicas, em caso de eventuais disputas judiciais envolvendo a assinatura.

Na ICP-Brasil, os riscos inerentes aos processos relacionados ao ciclo de vida do certificado digital (Solicitação, Validação, Emissão e Revogação) estão suficientemente mapeados e controlados por meio de mecanismos de segurança física e lógica implantados nas entidades que executam os processos. Esses controles são checados por meio de auditorias anuais e fiscalizações realizadas pelo Governo Brasileiro.

Já o ciclo de vida de uma assinatura digital compreende os processos:

1. Criação - processo de criação de um resumo criptográfico logicamente associado a um conteúdo digital e a chave criptográfica privada do signatário;
2. Verificação Inicial - processo de verificação quanto à validade de uma ou mais assinaturas digitais logicamente associadas a um conteúdo digital;
3. Armazenamento – processo que trata da guarda da assinatura digital. Compreende, pelo menos, cuidados para conversão dos dados para mídias mais atuais, sempre que necessário;
4. Revalidação – processo que estende a validade do documento assinado, por meio da reassinatura dos documentos ou da aposição de carimbos do tempo, quando da expiração ou revogação dos certificados utilizados para gerar ou revalidar as assinaturas, ou ainda quando do enfraquecimento dos algoritmos ou tamanhos de chave utilizados;
5. Verificação Final – processo no qual o documento é apresentado como evidência para um juiz e a assinatura é novamente verificada, para se obter informações sobre a identidade do signatário e a integridade do documento.

Esses processos acontecem, em geral, em ambientes que não são auditados ou fiscalizados pela ICP-Brasil; entretanto os riscos relacionados às etapas de Criação, Verificação Inicial e Verificação Final podem ser minimizados com a utilização de sistemas e equipamentos homologados no âmbito da ICP-Brasil, em consonância com o regulamento constante da Resolução 36 do Comitê Gestor [17].

Já os processos de Armazenamento dos documentos assinados e de Revalidação das assinaturas digitais não estão regulamentados. Além disso, permanecem em aberto, nos regulamentos atuais, questões como:

- formato dos documentos eletrônicos a serem assinados;
- tratamento a ser dado aos documentos assinados digitalmente antes da publicação da Resolução 62;
- disponibilização de informações críticas, como versões anteriores de LCRs e de Políticas de Certificados, necessárias para validação da cadeia de certificação no longo prazo.

Para sanar essas lacunas, criaram-se as propostas apresentadas no capítulo seguinte.

3 PROPOSTA

Analisando os regulamentos da ICP-Brasil disponíveis no sítio www.iti.gov.br e tomando por base os trabalhos e experiências relatados anteriormente, foram encontradas lacunas na regulamentação de alguns processos executados na ICP-Brasil que podem dificultar a validação das assinaturas digitais de forma segura, a longo prazo.

Essas lacunas ensejaram a criação de propostas de melhoria na regulamentação brasileira, apresentadas a seguir.

3.1 Regulamentar o serviço de arquivamento

Nos regulamentos da ICP-Brasil não está prevista a criação de entidades voltadas ao armazenamento de documentos assinados digitalmente. Com isso, corre-se o risco de que eles sejam armazenados de maneira inapropriada ou insegura, o que pode colocar em xeque sua confiabilidade.

Uma medida importantíssima, então, para permitir a validação de documentos a longo prazo na ICP-Brasil seria a criação de entidades para atuar como Prestadores de Serviços de Arquivamento de Longo Prazo (PSA). O Comitê Gestor da ICP-Brasil regulamentaria os procedimentos operacionais, a segurança das suas instalações e sistemas e os requisitos de contratação de pessoal.

Nesse processo, seria importante o envolvimento do Arquivo Nacional, que poderia contribuir na elaboração das políticas e práticas arquivísticas a serem observadas por aquelas entidades, incluindo-se nessa discussão a definição de formatos aceitáveis para os os documentos eletrônicos e as medidas a serem adotadas quando da caducidade das assinaturas (revalidação).

Não se propõe aqui a implantação de uma entidade única, centralizada, que armazene todos os documentos assinados no âmbito da ICP-Brasil, que já passam de milhões. A utilização dos serviços do PSA seria facultativa: grandes usuários, que tenham milhares de documentos para armazenar, poderiam criar em seu próprio ambiente as condições para isso, desde que atendessem os requisitos para arquivamento definidos. Usuários menores, ou todos aqueles que não desejassem despender recursos com a criação de ambiente próprio, utilizariam os serviços de um PSA. O importante é que sejam observados procedimentos regulamentados para armazenamento e revalidação de assinaturas. Essa medida vem ao encontro da proposta de preservação documental explanada em [18].

3.2 Criar repositório seguro de informações críticas

Para permitir a verificação de assinaturas digitais a longo prazo é preciso reconstruir de forma correta o caminho de certificação e obter informações adicionais; é necessário, portanto, dispor de Listas de Certificados Digitais, Certificados Digitais de Autoridades Certificadoras e diferentes versões de documentos obrigatórios, como políticas de certificados e declarações de práticas de certificações.

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 aquelas entidades não realizem os procedimentos de arquivamento adequados. Assim, é importante que a ICP-Brasil crie um repositório seguro com essas informações ou designe um PSA para fazê-lo. Os arquivos publicados nesse repositório teriam sua confiabilidade garantida por medidas técnicas ou organizacionais, de forma a serem pontos de referência confiáveis para a validação das assinaturas digitais realizadas por todos os usuários da ICP-Brasil, em qualquer momento que necessário.

3.3 Criar manuais orientando os usuários sobre o tratamento do legado

Até a publicação da Resolução 62, as aplicações que usam assinatura digital eram criadas de acordo com a necessidade e conveniência de cada usuário ou desenvolvedor, sem respeitar a qualquer padrão quanto ao formato da assinatura. Isso gerou um enorme legado de documentos assinados que podem não possuir as características necessárias à preservação por longo prazo

De acordo com a Resolução 62, a definição dos critérios para validação desse legado ficou a cargo das partes interessadas. Como a definição desses critérios pode ser bastante complexa, especialmente para usuários leigos que não disponham de estrutura organizacional para apoiá-los, uma medida recomendada é a criação de um guia, orientando-os sobre as formas de realizar a validação e sobre os procedimentos a que os documentos assinados devem ser submetidos, em cada caso.

3.4 Alterar os termos de titularidade incluindo referências sobre arquivamento a longo prazo e formato dos documentos assinados

Ao adquirir um certificado digital, a maioria dos usuários conhece pouco ou quase nada sobre certificação digital, obsolescência de algoritmos criptográficos e a necessidade de realizar procedimentos complementares para manter documentos assinados com sua chave privada protegidos ante às ameaças já descritas.

Em função disso, recomenda-se que os documentos que esses usuários recebem ao obter um certificado ICP-Brasil (também conhecidos como "termos de titularidade") passem a incluir orientações sobre aspectos importantes da preservação dos documentos assinados no longo prazo, tais como:

- em que situações um documento assinado digitalmente precisará ser submetido a procedimentos adicionais;
- que procedimentos são esses, caso o próprio titular deseje armazenar o documento;
- relação dos prestadores de serviço de arquivamento, caso ele decida por usar os serviços dessas entidades;
- conveniência de escolher formatos para o documento eletrônico assinado que facilitem sua recuperação no longo prazo.

3.5 Revisar os tipos e a aplicabilidade dos certificados ICP-Brasil

Na ICP-Brasil estão aprovados 4 tipos de certificados digitais para assinatura, conforme DOC-ICP-04 [19]: tipos A1, A2, A3 e A4.

Os certificados do tipo A1 e A2, cujas chaves privadas correspondentes são geradas e/ou armazenadas em software, oferecem menor nível de segurança aos seus proprietários, mas podem ser utilizadas para assinar qualquer tipo documento.

Para evitar riscos, sugere-se que a utilização dos certificados tipo A1 e A2 fique restrita apenas para assinaturas com fins de autenticação (como acesso a sistemas), enquanto os certificados A3 e A4, cujas chaves privadas correspondentes estão armazenadas em dispositivos criptográficos mais seguros, como *smartcards* e *tokens*,

seriam usados para assinatura de documentos que representem comprometimento legal (como contratos, declarações etc.).

4 ANÁLISE DA PROPOSTA

As medidas propostas são bastante factíveis, pois apoiam-se em tecnologias já existentes e em utilização em outras ICPs. Sua implantação dependeria da criação e aprovação de regulamentos pelo Comitê Gestor da ICP-Brasil e, em alguns casos, do aporte de recursos para o órgão responsável pelas atividades operacionais da ICP-Brasil, o Instituto Nacional de Tecnologia da Informação (ITI).

A regulamentação do serviço de arquivamento, ao passo que criaria entidades na ICP-Brasil que precisariam ser credenciadas e auditadas periodicamente, aumentando a carga de trabalho do ITI, por outro lado traria evidentes vantagens, como:

- agregaria mais segurança aos documentos assinados e aos contratos e obrigações legais que eles representam;
- aproximaria as comunidades técnicas, legais e arquivísticas, em torno do objetivo de criar os regulamentos para as entidades de arquivamento por longo prazo;
- estimularia a geração e disseminação de conhecimentos nas áreas envolvidas.

A criação de repositório seguro de informações críticas, por sua vez, dependeria basicamente de decisão dos gestores da ICP-Brasil e de propiciar ao ITI as condições técnicas e humanas necessárias para gerir as bases de dados resultantes.

A criação de manuais orientando os usuários sobre o tratamento do legado e a alteração dos termos de titularidade são medidas que dependeriam apenas da disponibilidade de recursos humanos.

A revisão dos tipos e a aplicabilidade dos certificados ICP-Brasil necessitaria de ampla discussão por parte da sociedade brasileira, dadas as implicações legais decorrentes e face à existência de processos de negócio modelados para a utilização de certificados do tipo A1 e A2, que já geraram milhões de documentos assinados com aquele tipo de certificado.

5 CONCLUSÕES

Vários segmentos da sociedade e o crescimento da economia digital estão impulsionando a utilização de documentos eletrônicos e de assinaturas digitais. No Brasil, esse quadro é particularmente verdadeiro, dada a expansão observada no número de aplicações que utilizam assinaturas digitais com base em certificados emitidos pela ICP-Brasil. Assim, é de extrema importância para o País a regulamentação dos métodos, processos e soluções que serão empregados para criação, armazenamento e validação a longo prazo de documentos eletrônicos assinados digitalmente.

Analisando a regulamentação atual da ICP-Brasil, observa-se que algumas ações pontuais poderiam agregar um nível mais elevado de segurança e facilitar o atingimento de um dos seus principais objetivos, que é conferir validade legal a

documentos assinados digitalmente. Entre essas ações encontram-se medidas mais complexas, como a criação de novos tipos de entidades na ICP-Brasil até aquelas mais simples, como a criação de manuais e textos orientando os usuários.

Paralelamente, observa-se que ainda existe distanciamento entre as comunidades técnica e arquivística no que tange à preservação documental, não apenas no Brasil como no exterior. Essa situação deveria ser revertida o quanto antes, pois o arquivamento dos documentos eletrônicos assinados digitalmente possivelmente será realizado por especialistas arquivistas, cujas técnicas de preservação documental não visam a preservar a integridade dos bits, mas sim a dos documentos que estão representados pelos bits. Isso conflita com os processos usados na assinatura digital, onde a alteração de um único bit compromete a verificação de todo o documento. Uma solução para essa dicotomia deve ser buscada a partir de trabalho conjunto das comunidades envolvidas.

6 REFERÊNCIAS

1. Thomaz, K.: I Congresso de Tecnologias para Gestão de Dados e Metadados do Cone Sul (2003) Disponível em: <http://conged.deinfo.uepg.br >
2. International Organization for Standardization / International Electrotechnical Commission: ISO 14721:2003 - Space data and information transfer systems - Open archival information system - Reference model. Genève, Switzerland. ISO/IEC (2003)
3. Australia. Public Record Office Victoria. Management of Electronic Records PROS 99/007 (Version 2) http://www.prov.vic.gov.au/vers/standard/version2.htm
4. Ansper, A., et al.: Efficient long-term validation of digital signatures, in Proc. of 4th International Workshop on Practice and Theory in Public Key Cryptography (PKC 2001), pp. 402-415, Korea (2001)
5. Gritzalis, D., Lekkas, D.: Cumulative Notarization for Long-term Preservation of Digital Signatures, Computers & Security, Volume 23, Issue 5, July 2004, Pages 413-424, ISSN 0167-4048, DOI: 10.1016/j.cose.2004.03.002 (2004)
6. Maniatis, P., Baker, M.: Enabling the Archival Storage of Signed Documents, in Proc. of the FAST 2002 Conference on File and Storage Technologies, pp. 31-45, January 2002, USA (2002)
7. Wallace, C.: Long-Term Archive Service Requirements. Internet Engineering Task Force. RFC 4810 (2007). Disponível em: <http://www.ietf.org/rfc/rfc4810.txt>.
8. Gondrom, T.; Brandner, R.; Pordesch, U.: Evidence Record Syntax (ERS). Internet Engineering Task Force. RFC 4998 (2007) Disponível em: <http://www.ietf.org/rfc/rfc4998.txt>.
9. Porekar, J., Saljic, S., Klobucar, T., Jerman-Blazic, A.: Technical Patterns for Long Term Trusted Archiving. Digital Society, 2009. ICDS '09. Third International Conference on, PP 241 – 246, Mexico (2009)
10. Aleksej, B., Toma K., Borka J.: Long-term trusted preservation service using service interaction protocol and evidence records. Computer Standards & Interfaces archive, Volume 29, Issue 3 (March 2007). pp 398-412, Slovenia (2007)
11. Boudrez, F.: Digital signatures and electronic records. Expertisecentrum DAVID vzw. Antwerpen (2005) Disponível em: <http://www.expertisecentrumdavid.be/docs/digitalsignatures.pdf>
12. Blanchette, J.: The digital signature dilemma - Le dilemme de la signature numérique. Pour publication dans Annales des Télécommunications, Mai/Juin (2006)

13. Dumortier, J.: Legal Reflexions concerning Digital Archiving. ECPRD Twin Seminar Brussels - The Hague (2002)
14. European Telecommunications Standards Institute: Policy requirements for trust service providers signing and/or storing data for digital accounting. ETSI TS 102 573. (2007) Disponível em: <http://www.etsi.org/WebSite/Standards/Standard.aspx>.
15. Brasil: Resolução Conarq 25/2007. Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos (2007). Disponível em: http://www.conarq.arquivonacional.gov.br/Media/publicacoes/earqbrasilv1.pdf>.
16. 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. Infra-estrutura de Chaves Públicas Brasileira (2009). Disponível em: <http://www.iti.gov.br/twiki/bin/view/Certificacao/Legislacao>.
17. Brasil. Comitê Gestor da ICP-Brasil. Resolução N° 36, de 21 de Outubro de 2004 – Aprova o Regulamento para Homologação de Sistemas e Equipamentos de Certificação Digital no Âmbito da ICP-Brasil. Infra-estrutura de Chaves Públicas Brasileira (2004). Disponível em: <http://www.iti.gov.br/twiki/bin/view/Certificacao/Legislacao>.
18. Spanoudakis, G. et al. (eds.): Security and Dependability for Ambient Intelligence, Advances in Information Security 45, DOI: 10.1007/978-0-387-88775-3_19,© Springer Science + Business Media, LLC 2009 - In particular Chapter 19 "Applying the SERENITY methodology to the domain of trusted electronic archiving"
19. 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). Infra-estrutura de Chaves Públicas Brasileira (2008). Disponível em: <http://www.iti.gov.br/twiki/bin/view/Certificacao/Legislacao>.