Nelson da Silva
Thiago Acórdi Ramos

Preservação de Longo Prazo de Documentos Eletrônicos na CNSEC

Florianópolis

2007

Nelson da Silva
Thiago Acórdi Ramos

Preservação de Longo Prazo de Documentos Eletrônicos na CNSEC

Trabalho de conclusão de curso submetido à Universidade Federal de Santa Catarina como parte dos requisitos para obtenção do grau de Bacharel em Ciência da Computação.

Orientador:
Prof. Ricardo Felipe Custódio, Dr.

Co-orientador:
Prof. Ricardo Pereira e Silva, Dr.

UNIVERSIDADE FEDERAL DE SANTA CATARINA
DEPARTAMENTO DE INFORMÁTICA E ESTATÍSTICA
BACHARELADO EM CIÊNCIA DA COMPUTAÇÃO

Florianópolis

2007

Nelson da Silva
Thiago Acórdi Ramos

Preservação de Longo Prazo de Documentos Eletrônicos na CNSEC

Este trabalho de Conclusão de Curso foi julgado adequado para a obtenção do título de Bacharel em Ciência da Computação e aprovado em sua forma final pelo Departamento de Informática e Estatística da Universidade Federal de Santa Catarina.

Florianópolis, 29 de Outubro de 2007.

Prof. Luís Fernando Friedrich, Dr.
Coordenador do Curso

Banca Examinadora

Prof. Ricardo Felipe Custódio, Dr.
Orientador

Prof. Ricardo Pereira e Silva, Dr.
Co-Orientador

Prof. Carlos Roberto De Rolt, Dr.

Dejane Luiza Bortoli, M.Sc.

Juliano Romani

Marcelo Carlomagno Carlos, M.Sc.

AGRADECIMENTOS

Nossos mais sinceros agradecimentos àqueles que colaboraram direta ou indiretamente para a realização desta etapa do projeto.

Primeiramente gostaríamos de agradecer nossas famílias por tudo que fizeram para que chegássemos até aqui e pela paciência nos momentos de falta e cansaço.

Dando continuidade, gostaríamos de agradecer ao professores Ricardo Felipe Custódio e Ricardo Pereira e Silva pela orientação e co-orientação, respectivamente. Aos colegas do LabSEC que, direta ou indiretamente, contribuíram para a realização deste trabalho. E aos membros da banca avaliadora: Professor Carlos Roberto De Rolt, Dejane Luiza Bortoli, Juliano Romani e Marcelo Carlomagno Carlos.

Agradecemos também ao senhor Manuel Matos, presidente da Câmara Brasileira de Comércio Eletrônico (Câmara-e.net) e ao professor Ricardo Felipe Custódio pela oportunidade de participarmos desse grande projeto de modernização e integração das serventias extrajudiciais.

Para finalizar, agradecemos também aos seguintes colaboradores: Júlio da Silva Dias, Paulo Roberto Gaiger Ferreira, Paulo Tupinambá Vampré e Reinaldo de Almeida Fernandes.

"É da natureza do conhecimento que ele sofra mutações e que, portanto, as certezas de hoje se tornarão os absurdos de amanhã."(Peter Drucker)

RESUMO

Neste trabalho busca-se propor uma solução para a preservação de longo prazo de documentos eletrônicos no contexto das serventias extrajudiciais, os chamados cartórios. Inicialmente, é realizado um levantamento das propriedades desejáveis aos documentos eletrônicos nesse cenário, e como estas podem ser alcançadas tecnologicamente por meio de um projeto de integração e modernização das serventias extrajudiciais – a Central Notarial de Serviços Eletrônicos Compartilhados (CNSEC). Avaliam-se, então, os impactos que a preservação de longo prazo infringe nessas tecnologias. Por fim, apresenta-se uma solução, aderente ao Modelo de Referência Open Archival Information System (OAIS), capaz de conservar tais atributos por longo prazo, com foco na disponibilidade, interpretabilidade e eficácia probante.

Palavras-chave: segurança; preservação de longo prazo; central de serviços compartilhados; documento eletrônico.

ABSTRACT

The aim of this work is to propose a solution to the long-term preservation of electronic documents in a notary context. Initially, is accomplished a survey of the desirables properties of the electronic documents in this set and how they can be technologically raised through a modernization and integration project of the registry offices – the Notary Shared Electronic Services Center. Then, the impacts that the long-term preservation infrige on this technologies are evaluated. In the end, a solution is presented adherent at the Open Archival Information System (OAIS) Reference Model, able to conservate such attributes for long-term, with focus on the availability, interpretability and probable efficacy.

Key-words: security; long-term preservation; shared services center; electronic document.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
AC	Autoridade Certificadora
ACTempo	Autoridade de Carimbo do Tempo
AR	Autoridade de Registro
Archisig	Conclusive and secure long-term archiving of digitally signed documents
BPMN	Business Process Modeling Notation
CAdES	CMS Advanced Electronic Signatures
CCSDS	Consultative Committee for Space Data Systems
CEDARS	CURL Exemplars in Digital Archives
CITRA	Conférence Internationale de la Table Ronde des Archives
CNB	Colégio Notarial do Brasil
CNJ	Conselho Nacional de Justiça
CNSEC	Central Notarial de Serviços Eletrônicos Compartilhados
CONARQ	Conselho Nacional de Arquivos
CRC	Códigos de Redundância Cíclica
CSC	Central de Serviços Compartilhados
DPC	Declaração de Práticas de Certificação
DSSC	Data Structure for Security Suitabilities of Cryptographic Algorithm
e-PING	Padrões de Interoperabilidade de Governo Eletrônico
E-Sign Act	Electronic Signatures in Global and National Commerce Act
ETSI	European Telecommunications Standards Institute
GED	Gerência Eletrônica de Documentos
GNU	GNU is not UNIX
ICP	Infra-estrutura de Chaves Públicas
ICP-Brasil	Infra-estrutura de Chaves Públicas Brasileira
IDP	Informação de Descrição de Preservação
InterPARES	International Research on Permanent Authentic Records in Electronic Systems
LCR	Listas de Certificados Revogados
LTANS	Long-Term Archive and Notary Services
MARC	Machine-Readable Cataloging
MODS	Metadata Object Description Language
MP	Medida Provisória
NARA	National Archives and Records Administration
NEDLIB	Networked European Deposit Library
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OAB	Ordem dos Advogados do Brasil
OAIS	Open Archival Information System
OCLC/RLG	Online Computer Library Center/ Research Libraries Group
ODF	OpenDocument Format
ON	Observatório Nacional
PAI	Pacote de Arquivamento de Informação
PANDORA	Preserving and Accessing Networked Documentary Resources of Australia
PC	Políticas de Certificação
PD	Política de Datação
PDF	Portable Document Format
PDI	Pacote de Disseminação de Informação
PL	Projeto de Lei
PSI	Pacote de Submissão de Informação
RSA	Rivest, Shamir e Adleman
SaaS	Software as a Service
TI	Tecnologia de Informação
TIC	Tecnologia de Informação e Comunicação
TransiDoc	Legally secure transformation of signed documents
UNCITRAL	United Nations Commission on International Trade Law
UNESCO	Organização das Nações Unidas para a Educação, a Ciência e a Cultura
UVC	Universal Virtual Computer
VERS	Victorian Electronic Records Strategy
W3C	World Wide Web Consortium
XAdES	XML Advanced Electronic Signatures
XML	Extensible Markup Language
XMP	Extensible Metadata Platform

SUMÁRIO

1 INTRODUÇÃO

Desde a criação dos primeiros computadores, a partir da segunda guerra mundial, uma nova forma de registro de informações se tornou possível: os bits. O que antes era dependente de um substrato físico para tomar forma, agora poderia ser armazenado, numa representação intermediária, em meios ópticos ou magnéticos, trazendo benefícios quanto à transmissão e armazenamento de informação. Essa nova forma de registro constitui o documento eletrônico.

Aliado a Internet como meio de comunicação, e recentemente com a implantação de uma infra-estrutura de chaves públicas sólida e confiável no Brasil, tornou-se o documento eletrônico base para as relações humanas nessa nova realidade, sendo, inclusive meio alternativo ao papel para o registro dos atos jurídicos. A ele, graças a MP 2.200-2 de Agosto de 2001, que "Institui a Infra-Estrutura de Chaves Públicas Brasileira – ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências", foi possível atribuir a mesma eficácia probante que aquela despendida ao documento papel.

Neste sentido, é natural pensar-se em propor uma infra-estrutura para tratar adequadamente a segurança dos documentos eletrônicos, em especial aqueles orquestrados por uma serventia extrajudicial, os chamados cartórios. Sabe-se que são inúmeras as iniciativas já realizadas por algumas das serventias nesse caminho. Contudo, não há um modelo geral e independente que respeite os preceitos legais e de autonomia para modernização e integração dos serviços prestados pelas serventias extrajudiciais.

Assim, neste trabalho delineia-se tal infra-estrutura. Contudo, as particularidades dos documentos eletrônicos não podem ser ignoradas nem mitigadas, principalmente em se tratando de sua preservação por longo prazo. A eficácia probante, por exemplo, de um documento eletrônico, diferentemente de um documento papel, diminui com o passar do tempo. É foco deste trabalho, portanto, avaliar os impactos que essa preservação infringe aos atributos do documento eletrônico, e propor uma solução para a preservação, em especial, de suas propriedades de disponibilidade, interpretabilidade, e eficácia probante.

1.1 JUSTIFICATIVA

A partir da institucionalização da Infra-estrutura de Chaves Públicas Brasileira (ICP-Brasil) através da MP 2.200-2 foi possível a utilização de documentos eletrônicos com a mesma eficácia jurídica que o documento papel. Neste sentido, é natural pensar-se em propor uma infra-estrutura para tratar adequadamente a segurança dos documentos eletrônicos, em especial aqueles orquestrados por uma serventia extrajudicial, os chamados cartórios. Vislumbra-se que os certificados digitais e os processos advindos de assinatura digital e sigilo de documentos possam permitir o desenvolvimento de uma infra-estrutura, com serviços mínimos para a criação de um ambiente chamado Central Notarial de Serviços Eletrônicos Compartilhados (CNSEC).

Contudo, os fundamentos da eficácia probante dos documentos eletrônicos devem ser profundamente analisados, em especial seu comportamento em longo prazo. Pois, diferentemente do documento papel, as tecnologias utilizadas para descrever e suportar os requisitos de segurança de um documento eletrônico têm vida relativamente curta.

Faz-se necessário realizar um levantamento das tecnologias e estratégias existentes ou em desenvolvimento que possibilitem agregar à CNSEC a característica de preservação a longo prazo dos seus documentos, conservando as propriedades desejáveis aos documentos eletrônicos nela armazenados.

1.2 OBJETIVOS

1.2.1 OBJETIVO GERAL

Realizar um levantamento das propriedades desejáveis aos documentos eletrônicos no contexto das serventias extrajudiciais, definindo os meios pelos quais tais atributos poderão ser alcançados tecnologicamente, e estudando os impactos que o armazenamento de longo prazo infringe nessas tecnologias. Por fim, avaliar as melhores alternativas de preservação de longo prazo de documentos eletrônicos no tocante a Central Notarial de Serviços Eletrônicos Compartilhados (CNSEC), propondo um modelo para o armazenamento de tais documentos, o Arquivo da CNSEC.

1.2.2 OBJETIVOS ESPECÍFICOS

Os objetivos específicos são os seguintes:

- realizar um levantamento das propriedades desejáveis aos documentos eletrônicos no con-

texto das serventias extrajudiciais;

- definir como tais atributos poderão ser alcançados tecnologicamente;
- estudar os impactos que o armazenamento de longo prazo infringe nessas tecnologias;
- tomar conhecimento das estratégias existentes para a preservação de longo prazo de documentos eletrônicos;
- realizar um levantamento das soluções adotadas pelos maiores projetos existentes de preservação de documentos eletrônicos;
- estudar o Modelo de Referência OAIS, amplamente adotado como guia na preservação de documentos eletrônicos;
- avaliar as estratégias de preservação de longo prazo no tocante a Central Notarial de Serviços Eletrônicos Compartilhados (CNSEC);
- propor um modelo para o armazenamento dos documentos eletrônicos das serventias, o Arquivo CNSEC.

1.3 TRABALHOS RELACIONADOS

Existem diversos trabalhos nas diferentes esferas, a exemplo das universidades e governos, abordando a preservação em longo prazo para objetos digitais. Normalmente, cada projeto busca atender a uma demanda específica, limitando o escopo dos arquivos que serão armazenados. Segundo Thomaz (2004), essa preocupação com a rápida obsolescência digital já vem de muito tempo, com primeira abordagem em 1964. Mas considera-se como marco inicial o trabalho do professor Robert Henri Bautier, com discussões sobre os desafios do documento eletrônico para os arquivos, apresentado na *Conférence Internationale de la Table Ronde des Archives* – CITRA, na Alemanha, em 1971.

Os projetos pesquisados diferem, basicamente, na escolha das estratégias de preservação em longo prazo, visto que não se conhece uma solução ótima. Além das estratégias, as políticas relativas a cada instituição arquivística costumam variar bastante, principalmente quanto a questão do formato dos arquivos. Algumas delas só aceitam um determinado tipo de formato, por ser padrão ou aberto, por exemplo.

Mesmo com tantas pesquisas sendo realizadas, a grande maioria dos projetos, tais como CEDARS, CAMiLEON, NEDLIB, MINERVA, PANDORA e ERA, normalmente dão trata-

mento à qualquer tipo de objeto digital – a exemplo de sons, imagens, vídeos e objetos dinâmicos – e até por isso, não levam em conta objetos assinados digitalmente, pois esses tipos de arquivos não costumam ser autenticados. Entretanto, para o contexto dos serviços públicos delegados, o tratamento desse tipo de objeto é fundamental.

Nesse contexto, alguns projetos destacam-se por trabalharem com objetos autenticados: Archisig[1], InterPARES[2], LTANS[3], TransiDoc[4] e VERS[5].

O projeto *Conclusive and secure long-term archiving of digitally signed documents* (Archisig) busca, justamente, uma solução para uso de documentos assinados digitalmente, frente à degradação do valor probante ao longo do tempo. Este deu origem aos projetos *Long-Term Archive and Notary Services* (LTANS), e *Legally secure transformation of signed documents* (TransiDoc). Este se empenha em gerar evidências para que uma transição tenha validade legal, por exemplo, ao adicionar-se novos dados em um documento já assinado – o que invalida sua assinatura atual. Para atingir este objetivo, evidências são geradas sobre as alterações feitas e destaca-se o uso de notários para legalizar a situação. O LTANS é um grupo de trabalho que busca estudar requerimentos, estruturas de dados e protocolos para o uso seguro de arquivos necessários e serviços notariais. É deste grupo o estudo do registro de evidência, que está descrito na seção 4.4.2, e que é utilizado pelo Arquivo da CNSEC.

The International Research on Permanent Authentic Records in Electronic Systems (InterPARES) objetiva desenvolver conhecimento teórico e metodológico essencial para a preservação em longo prazo de registros autênticos criados e/ou mantidos em forma digital. Esse conhecimento deve prover as bases para formulação de modelos de políticas, estratégias e padrões capazes de garantir a longevidade desse tipo de material e a habilidade aos seus usuários para confiarem em sua autenticidade.

Por último, o *Victorian Electronic Records Strategy* (VERS), foi desenvolvido para prover liderança e direção na gerência de registros digitais, sendo uma solução mundialmente líder para o problema de capturar, gerenciar e preservar registros eletrônicos. VERS é um framework de padrões, orientação, treinamento, consultoria e projetos de implementação, que está centrado no objetivo de arquivar registros eletrônicos com integridade e autenticabilidade.

No Brasil, o Conselho Nacional de Arquivos – CONARQ[6], segundo descrição em sua

[1] http://www.archisig.de
[2] http://www.interpares.org
[3] http://www.ietf.org/html.charters/ltans-charter.html
[4] http://www.transidoc.de
[5] http://www.prov.vic.gov.au/vers/vers
[6] http://www.conarq.arquivonacional.gov.br

página, destaca-se como um órgão colegiado, vinculado ao Arquivo Nacional da Casa Civil da Presidência da República, que tem por finalidade definir a política nacional de arquivos públicos e privados, como órgão central de um Sistema Nacional de Arquivos, bem como exercer orientação normativa visando à gestão documental e à proteção especial aos documentos de arquivo. Em sua página é possível se obter publicações digitais como normas, dicionários de terminologia, recomendações, descrições e diretrizes arquivísticas.

1.4 ESTRUTURA DO TRABALHO

A presente seção descreve a organização e estrutura deste trabalho de conclusão de curso.

No capítulo 2, os fundamentos da criptografia que dão suporte às tecnologias e técnicas mencionadas ao longo deste trabalho, são recordados. Além da criptografia, as suas aplicações práticas – infra-estrutura de chaves pública, assinatura digital e carimbo do tempo – também são mostradas. O capítulo 3 aborda o documento eletrônico, as assinaturas digitais apostas sobre ele, e a questão da eficácia probante dos mesmos, frente à regulamentação vigente.

No capítulo seguinte, de número 4, apresentam-se as principais técnicas para a preservação de longo prazo para objetos digitais. Estas estão divididas em relação à conservação das propriedades desejáveis a um documento eletrônico: disponibilidade, interpretabilidade e eficácia probante. Como último tópico deste capítulo, apresenta-se o Open Archival Information System (OAIS), modelo de referência para sistemas arquivísticos, sendo um modelo conceitual que nomeia, atribui funções, e organiza entidades distintas que tomaram para si a responsabilidade da preservação em longo prazo.

O capítulo 5 é referente à Central Notarial de Serviços Eletrônicos Compartilhados (CNSEC), trazendo uma arquitetura básica para uma central de serviços compartilhados, aliada à conceitos de software como um serviço. Toda a elaboração da CNSEC leva em conta os princípios levantados junto às serventias extrajudiciais, atendendo aos seus anseios, provendo uma solução que traga realmente modernização e integração dos serviços públicos delegados.

Tomando como base as técnicas apresentadas no capítulo 4 e a estrutura e princípios da CNSEC delineados no capítulo 5, culmina-se no Arquivo da Central Notarial de Serviços Eletrônicos Compartilhados – o Arquivo da CNSEC, exposto no capítulo 6. A divisão deste capítulo está orientada pelo modelo de referência OAIS. O arquivo tem como objetivo prover o armazenamento e preservação em longo prazo de documentos eletrônicos para as serventias agregadas à CNSEC, propondo um esquema análogo à autenticação feita pelos cartórios atualmente a fim de transpor os problemas levantados no capítulo de preservação de longo prazo.

Por fim são feitas as considerações finais sobre este trabalho, indicados possíveis trabalhos futuros e listadas das referências da literatura consultadas para que a elaboração deste trabalho fosse possível. Nessas referências podem ser encontradas diversas informações sobre outros projetos, técnicas e estudos referentes à preservação de longo prazo de objetos digitais.

2 FUNDAMENTOS DA CRIPTOGRAFIA

2.1 INTRODUÇÃO

A palavra criptografia é derivada do grego *kryptós* (escondido) e o verbo *gráfo* (escrita). Ciframento é definido por Stallings (2005, p. 20) como o uso de algoritmos matemáticos para transformar dados em uma forma que não é inteligível por leitura. A transformação e subseqüente recuperação dos dados depende de um algoritmo e zero ou mais chaves criptográficas. CRL (2006) aponta três das técnicas de ciframento conhecidas e que são as bases para os mais modernos cifradores de hoje, mostradas a seguir.

Os Espartanos desenvolveram um cilindro chamado Scytale em que a mensagem era escrita em uma estreita tira de couro ou pergaminho, enrolada ao redor do Scytale, onde a escrita era feita. Esta tira, contendo uma seqüência de letras sem significado, era enviada ao receptor. A mensagem só podia ser entendida enrolando a tira em um Scytale de mesmo diâmetro. Esta técnica é conhecida como transposição, ou seja, as letras continuam as mesmas, mas a ordem é alterada.

Outra técnica é a substituição. Mensagens são codificadas substituindo as letras em um texto por outra um certo número de posições mais a frente. Por exemplo, um A deslocado de três posições tornar-se-ia um D, e assim sucessivamente. O primeiro registro de uso foi de Júlio César, sendo conhecido como cifrador de César.

Em 1466 o italiano Leon Battista Alberti, conhecido como pai da criptografia ocidental, descreveu a construção de um disco de cifragem, criando o conceito de cifradores polialfabéticos. O Francês Blaise de Vigenère implementou o conceito de Alberti. Stallings (2005, p. 45-48) mostra que a técnica consiste em escolher uma palavra secreta e repetí-la até atingir o tamanho do texto a ser codificado. A letra da palavra chave será o deslocamento (substituição) que deve ser feito na letra do texto, fazendo com que uma mesma letra do texto tenha diferentes chaves. É conhecido como cifrador de Vigenère.

Stallings (2005, p. 29) define alguns termos importantes para o entendimento desta seção:

a) a mensagem original é conhecida como texto plano enquanto a codificada é chamada texto cifrado; b) o processo de conversão do texto plano para o cifrado é a cifragem e caminho inverso a decifragem; c) os muitos esquemas utilizados para ciframento constituem a área de estudo conhecida como criptografia.

Nesta seção serão apresentados alguns conceitos básicos sobre segurança que tornam todo o trabalho possível: a) função de resumo criptográfico; b) criptografia simétrica; c) criptografia assimétrica; d) infra-estrutura de chaves públicas; e) assinatura digital; f) carimbo do tempo.

2.2 FUNÇÃO DE RESUMO CRIPTOGRÁFICO

É definida por Stallings (2005, p. 329) como uma função H que aceita uma mensagem M de tamanho variável como entrada e produz uma saída de tamanho fixo, referida como resumo (do inglês, hash) $H(M)$.

Uma função de resumo criptográfico segura, segundo Stallings (2005, p. 335), deve ainda satisfazer as seguintes propriedades:

- deve ser facilmente computável;
- sabendo-se do resumo de uma mensagem, deve ser computacionalmente inviável encontrar a mensagem que o originou;
- para uma dada mensagem, deve ser computacionalmente inviável encontrar outra que possua o mesmo resumo (colisão fraca);
- deve ser computacionalmente inviável produzir qualquer par de mensagens diferentes que possuam o mesmo resumo (colisão forte).

Tais propriedades tornam o resumo criptográfico seguro, uma representação única e compacta da mensagem, podendo eventualmente ocupar seu lugar por motivos de eficiência, como ocorre em assinaturas digitais.

Um exemplo, de tais funções é o SHA-1 projetado pela National Security Agency (NSA), e definido em Eastlake e Jones (2001). Basicamente, tal função divide a mensagem em blocos de 512 bits – caso o tamanho da mesma não seja múltiplo de 512, ela é complementada, o chamado "padding" – cada bloco, juntamente com a saída de 160 bits do bloco anterior, então passa por caixas de função resumo, que produzem 160 bits para a próxima caixa. Essa operação se repete até obter-se o valor de resumo final.

O fato de cada um das caixas também utilizar como entrada a saída da caixa anterior, fundamenta uma outra característica da função de resumo criptográfico – o efeito avalanche. Onde, mensagens levemente alteradas produzem resumos muito diferentes (idealmente a alteração de um bit da mensagem deve levar a alteração de todos os bits do resumo).

Sua aplicação é variada, incluindo detecção de erros, assinaturas digitais, e carimbos do tempo, os últimos detalhados nas seções 2.6 e 2.7, respectivamente.

2.3 CRIPTOGRAFIA SIMÉTRICA

Tal qual a criptografia assimétrica, a simétrica tem sua aplicação direta na cifragem e decifragem de mensagens, garantindo a privacidade ou a confidenciabilidade. Entretanto, na criptografia simétrica a mesma chave é utilizada nas duas operações, levando a necessidade de seu compartilhamento por algum canal seguro. A figura 1 ilustra essa configuração.

Figura 1: Cifragem simétrica com compartilhamento de chave por canal seguro.

Suas operações baseiam-se na transformação, guiada pela chave, de blocos de texto em claro, em blocos de texto cifrado, na cifragem e vice-versa na decifragem. O tamanho desses blocos classifica os algoritmos de cifragem simétrica em cifradores de bloco ou de fluxo, sendo o último uma especialização do primeiro para blocos de 1 bit ou 1 byte (STALLINGS, 2005, p. 64).

No tocante a sua implementação, em geral, tais cifradores seguem a estrutura proposta por Feistel (1973) baseada no uso de cifradores que alternam as operações de substituição e permutação. Na realidade trata-se de uma aplicação prática da proposta de Shannon (1949) que visava, pelo produto de dois ou mais cifradores, em seqüência, alcançar um cifrador com maior resistência a criptoanálise estatística que seus membros.

Apesar de possuírem implementações, em geral, mais complexas, os cifradores simétricos consomem menos recursos computacionais em suas operações que os assimétricos, sendo exemplos daqueles, os cifradores de bloco AES-256, Blowfish, CAST-256, DES, e o Triplo DES.

Contudo, os problemas de distribuição das chaves, e a impossibilidade de determinar qual

das partes, que compartilham a chave, realizou determinada operação, levaram ao desenvolvimento da criptografia assimétrica, conceito apresentado na seção 2.4.

2.4 CRIPTOGRAFIA ASSIMÉTRICA

Conceituada inicialmente em 1976 por Whitfield Diffie e Martin Hellman, a criptografia assimétrica ou de chaves públicas busca solucionar o problema de compartilhamento das chaves inerente à criptografia simétrica.

Baseia-se no uso de um par de chaves complementares – o que uma faz a outra desfaz. Uma das chaves é pública, devendo ser distribuída, a outra é privada, e deve ser mantida em segredo, sendo em geral armazenada em smart-cards, tokens, ou repositórios em software. Apesar da relação existente entre as duas, não é computacionalmente viável derivar a chave privada a partir da chave pública.

Tais propriedades do par de chaves permitem sua utilização tanto para a cifragem e decifragem, provendo confidenciabilidade, quanto para autenticação. A primeira, ilustrada na figura 2, consiste em cifrar o documento com a chave pública do destinatário. Somente ele poderá decifrar a mensagem, uma vez que, teoricamente, ele é o único a possuir a chave privada.

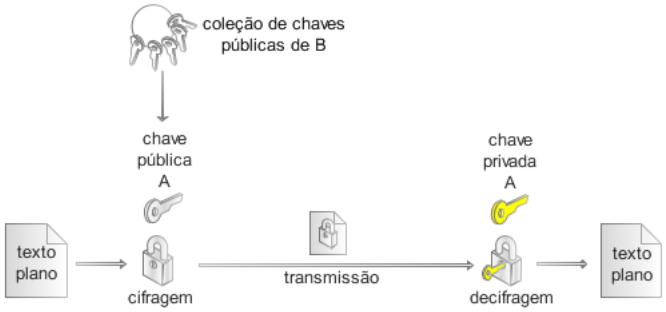

Figura 2: Uso da criptografia assimétrica para cifragem.

A autenticidade é, por sua vez, alcançada pela cifragem do documento com a chave privada. Nesse caso, qualquer um pode decifrar a mensagem, pois a chave pública capaz de realizar tal operação, é disponível a todos. Contudo, o fato da decifragem ser bem sucedida, permite concluir que a cifragem só pode ter sido realizada pelo titular da chave privada. Tal esquema é apresentado na figura 3.

O funcionamento dos algoritmos de criptografia assimétrica, diferentemente da criptografia simétrica, fundamenta-se na presunção da dificuldade de solucionar problemas matemáticos

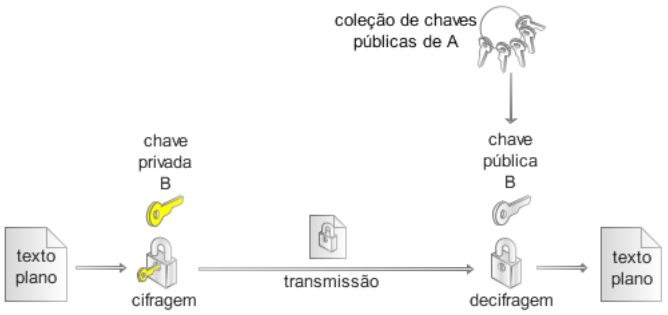

Figura 3: Emprego da criptografia assimétrica para a autenticidade.

como a fatoração do produto de números primos grandes, ou o cálculo de logaritmos discretos.

Sua implementação atualmente mais utilizada é o RSA, proposto em 1977 por Rivest, Shamir e Adleman. São igualmente exemplos de algoritmos de chaves públicas o DSS, El Gamal, e diversas técnicas de curvas elípticas.

Entretanto, apesar de possibilitar uma distribuição de chaves mais efetiva, a criptografia assimétrica possui certos problemas. O primeiro deles refere-se a sua lentidão – necessitam de muito mais recursos computacionais que os cifradores de bloco – nesse sentido, em geral sua aplicação se dá sobre pequenos blocos de informação, por exemplo, em chaves de sessão, onde a chave da cifragem simétrica utilizada num canal seguro é previamente cifrada de forma assimétrica e então trocada entre as partes, ou em resumos criptográficos, como acontece em assinaturas digitais, apresentado na seção 2.6.

Um segundo problema está em determinar se um par de chaves realmente pertence a quem diz possuí-la. Tal problema é solucionado por meio de infra-estruturas de chaves públicas, como aquela apresentada na seção 2.5, ou redes de confiança, onde acreditasse numa terceira parte confiável que afirma que determinado par de chaves realmente pertence a um determinado titular.

2.5 INFRA-ESTRUTURA DE CHAVES PÚBLICAS

Uma infra-estrutura de chaves públicas (ICP) viabiliza o uso de criptografia assimétrica, provendo meios de associar um par de chaves ao seu titular. Tal associação depende da confiança direta ou indireta numa Autoridade Certificadora (AC), que pode ser uma empresa, indivíduo, ou organização, público ou privado. E é ela a terceira parte confiável que atesta tal ligação por meio da emissão de certificados digitais.

Tais certificados são documentos eletrônicos assinados pela AC constando, entre outras

informações, sua validade, seu número serial, dados do titular e sua chave pública. Seu padrão mais amplamente difundido é o X.509v3 (HOUSLEY et al., 2002).

Nesse sentido, a emissão de um certificado depende da confirmação da titularidade do par de chaves. Por conveniência essa tarefa pode ser delegada a uma Autoridade de Registro (AR) que se incumbe de identificar o titular. Na ICP-Brasil, por exemplo, essa identificação é presencial. Uma vez identificado o titular, seus dados, e a chave pública são inseridos na requisição de certificado, assinado pela AR, e enviado para a AC. A Autoridade Certificadora, então, sem qualquer validação extra, entrega o certificado digital a AR.

Além de emitir os certificados digitais, uma AC deve manter informações sobre eles. Como as Listas de Certificados Revogados (LCR) – documentos eletrônicos por ela assinados, periodicamente publicados informando quais certificados foram revogados. Essa revogação ocorre quando essa titularidade das chaves não é mais correta, e o certificado ainda não expirou, seja, por exemplo, pelo comprometimento da chave privada.

Autoridades Certificadoras além de emitir certificados para usuários finais, podem, igualmente, emitir certificados para outras ACs. Em geral, a validade dos certificados daqueles variam entre um e três anos, e destes, de três a vinte anos. Quanto ao tamanho das chaves públicas, nos certificados finais, em geral, são de 1024 bits, e nos das ACs 2048 bits. Tal possibilidade gera uma hierarquia, onde a primeira delas, a AC-Raiz, possui certificado auto-assinado.

As regras que gerem tal infra-estrutura são especificadas nas Políticas de Certificação (PC), que estabelecem requisitos de alto nível, como por exemplo, a necessidade de identificação presencial dos titulares perante as AR. Cada AC então especifica por meio da Declaração de Práticas de Certificação (DPC) como ela implementa essas regras, seguindo o exemplo anterior, quais documentos de identificação devem ser apresentados. Tais políticas definem, igualmente, os requisitos de segurança que devem ser obedecidos.

2.6 ASSINATURA DIGITAL

As assinaturas digitais buscam atingir, para documentos eletrônicos, funções análogas àquelas alcançadas pela assinatura manuscrita. Assim como a primeira, uma vez aposta, tem por objetivo indicar o consentimento do signatário com o conteúdo do documento. Portanto, envolve duas propriedades básicas – a integridade do documento e a autenticidade.

Como visto na seção 2.2, a integridade do documento eletrônico pode ser determinada mediante comparação com um resumo criptográfico seguro obtido anteriormente – qualquer

alteração no conteúdo do documento implicaria em diferença nos resumos. A autenticidade, por sua vez, como detalhado na seção 2.4, pode ser alcançada por meio da cifragem assimétrica utilizando a chave privada.

Em vista disso, a aposição de uma assinatura digital pode ser realizada da seguinte forma:

1. aplica-se uma função de resumo criptográfico seguro sobre o documento eletrônico;
2. o resumo criptográfico obtido é então cifrado com a chave privada.

A verificação da assinatura depende da assinatura digital obtida acima, e do documento eletrônico.

- decifra-se o resumo cifrado recebido, utilizando a chave pública do signatário;
- aplica-se a função de resumo criptográfico seguro sobre o documento eletrônico;
- compara-se os dois resumos criptográficos – o recebido e o computado; caso não sejam iguais, a assinatura é invalidada.

Na correta validação da assinatura, deve-se ainda verificar se o par de chaves realmente pertence ao signatário. Nesse sentido faz-se necessário obter e validar os certificados de todo o caminho de certificação, formado pelo certificado do signatário até o certificado de alguma Autoridade Certificadora confiável. Essa validação envolve, entre outras operações, verificar se algum dos certificados expirou ou foi revogado.

Caso o caminho de certificação seja construído e validado com êxito, tem-se uma assinatura digital válida.

Nesse sentido, ainda resta um problema relacionado à expiração dos certificados. Uma assinatura manuscrita autêntica quando aposta, é considerada válida mesmo que o signatário fique posteriormente impossibilitado de assinar – caso venha a óbito, por exemplo. No caso de assinaturas digitais, tal expiração, a priori, como visto no processo de verificação acima, invalidaria a assinatura. Por conseguinte, faz-se necessário a datação da assinatura por meio de carimbos do tempo, apresentado na seção 2.7, de modo a comprovar que a assinatura foi aposta em tempo hábil.

São exemplos de estruturas de dados, que comportam tais assinaturas, e opcionalmente o documento eletrônico, os formatos CMS “SignedData” Attached, CMS “SignedData” Detached e XML Signature – especificados respectivamente em RFC3852 e XMLDSIG.

2.7 CARIMBO DO TEMPO

O carimbo do tempo é um documento eletrônico assinado por uma Autoridade de Carimbo do Tempo, que atesta a existência de um documento em um determinado momento, e permite verificar se sua integridade foi mantida desde então. Analogamente a Política de Certificação de uma ICP, uma Autoridade de Carimbo do tempo, segue as regras definidas na Política de Datação (PD) como detalhado em RFC3628.

Tal carimbo obtido seguindo os seguintes passos:

1. um resumo criptográfico do documento é computado;
2. envia-se esse resumo a Autoridade de Carimbo do Tempo (ACTempo), por meio de uma requisição. Esse processo garante a privacidade, por não expor o conteúdo do documento, apenas o resumo. Tal requisição é especificada em RFC3161;
3. a ACTempo obtém a data e hora por meio de uma fonte confiável de tempo;
4. um carimbo do tempo, igualmente especificado em RFC3161 é devolvido pela ACTempo, contendo entre outras informações o resumo criptográfico anteriormente submetido, a data e hora da submissão, e a assinatura da ACTempo.

A confiança em tal carimbo depende da validação da assinatura contida, da mesma forma que qualquer outra assinatura digital, como descrito na seção 2.6.

2.8 CONCLUSÃO

A criptografia já era utilizada muito antes do uso de computadores, sendo decisiva em operações secretas, onde o sigilo das mensagens é vital. As técnicas desenvolvidas durante a história são utilizadas pelos cifradores mais modernos de hoje.

A criptografia simétrica é ainda muito utilizada por seu baixo consumo computacional e razoável nível de segurança. Já a criptografia assimétrica tem sido o grande pilar de todas as tecnologias desenvolvidas para aumentar ainda mais a segurança, mas seu custo computacional a torna impraticável de ser usada como solução única. Uma das abordagens utilizadas é gerar uma chave simétrica, cifrá-la com a chave pública do receptor e enviá-la para que o mesmo a decifre com sua chave privada, criando um canal seguro para troca da chave.

A assinatura digital, o certificado digital e o uso de infra-estruturas de chaves públicas tornaram possível a identificação de uma pessoa do mesmo modo que ocorre com uma carteira

de identidade. Duas das técnicas que tornaram isso possível são a criptografia assimétrica e funções resumo. Esta torna aquela viável, uma vez que gera um resumo de tamanho fixo de qualquer arquivo, sendo necessário apenas cifrá-lo ao invés de cifrar o arquivo inteiro.

Por último, o carimbo do tempo, que tornou possível o uso de assinaturas digitais como meio de prova, fornecendo o suporte necessário para que infra-estruturas e políticas possam ser criadas a fim de prover a eficácia probante dos atos.

3 DOCUMENTO

3.1 INTRODUÇÃO

Desde a pré-história, o homem tenta passar, de algum modo, seu conhecimento, descoberta e vivências para as demais gerações. Os primeiros registros que se têm notícias são as pinturas em rochas. O marco de fim da pré-história, a invenção de sistemas de escrita, mostra essa determinação de se comunicar fatos. Nossa escrita de hoje, derivada do latino, teve origem no alfabeto fenício, aperfeiçoado pelos gregos, passando a ter vinte e quatro letras, entre vogais e consoantes. Após o desenvolvimento da escrita, utilizando-se de vários substratos físicos, a humanidade passou a registrar seu conhecimento. Desde pedras, passando-se por couro de animais, argila e o papiro, até chegar ao papel, desenvolvido na China (DIAS, 2004, p. 1-2).

Documento é definido por Bueno (1992, p. 380) como: "Título ou diploma que serve de prova; declaração escrita para servir de prova; demonstração." Parentoni (apud JúNIOR, 2000, p. 304-305) define documento, em sentido amplo, como sendo: "[...] é qualquer base de conhecimento, fixada materialmente e disposta de maneira que se possa utilizá-la para extrair cognição do que está registrado." No sentido estrito, um documento é "[...] a peça escrita ou gráfica que exprime algo de valor jurídico para esclarecer, instruir ou provar o que se alegou no processo pelas partes em lide.", mostrado por Parentoni (apud JúNIOR, 2000, p. 303).

Parentoni (2005) reforça que, tanto a idéia intuitiva quanto a definição gramatical e até mesmo a jurídica de documento, não se diferem muito. No sentido amplo, pode ser qualquer objeto material, como texto, imagem ou gravação e já no estrito, seria apenas texto. Ambos os sentidos referem documento como sendo destinado à provar um fato.

Nesta seção serão apresentadas as particularidades do documento eletrônico e da assinatura digital frente aos documentos tradicionais e as assinaturas manuscritas. Por fim, aborda-se a eficácia probante dos documentos eletrônicos.

3.2 PARTICULARIDADES DO DOCUMENTO ELETRÔNICO

Como analisado em Dias (2004), desde a criação dos primeiros computadores, a partir da segunda guerra mundial, uma nova forma de registro de informações se tornou possível: os bits. O que antes era dependente de um substrato físico para tomar forma, agora poderia ser armazenado, numa representação intermediária, em meios ópticos ou magnéticos, trazendo benefícios quanto a transmissão e armazenamento de informação. Essa nova forma de registro constitui o documento eletrônico.

Ainda graças à Internet, o documento eletrônico passou a ser a base das relações humanas nessa nova realidade, incluindo transações comerciais. Sua crescente importância para a sociedade leva a necessidade de um maior entendimento de suas peculiaridades. Suas diferenças em relação ao documento tradicional não podem ser ignoradas nem mitigadas. Só assim, com o seu correto tratamento, este poderá ser fundamento às relações antes baseadas no documento papel.

Em Dias (2004) analisa-se os atributos de segurança do documento papel, em contraponto ao documento eletrônico, que possibilitam sua aceitação em relações que demandam um maior nível de segurança, tal qual o contexto das serventias extrajudiciais. Tais atributos são a autenticidade, não-repúdio, integridade, tempestividade, e disponibilidade.

A autenticidade, ou seja, a possibilidade de determinar a autoria de um documento, está associada ao não-repúdio, leia-se: possibilidade de comprovar que o autor do documento realmente o criou, e tem conhecimento do seu conteúdo. Num documento papel, a autenticidade pode ser comprovada pela análise da letra ou da assinatura manuscrita – cuja forma, pressão e velocidade empregadas na sua escrita são teoricamente únicas, e passíveis de produção apenas pelo seu titular. O pressuposto conhecimento do conteúdo está relacionado ao fato de que no documento papel a conexão da informação com o próprio substrato físico tornam o suporte e a informação uma entidade única.

No caso de documentos eletrônicos, a ligação com o conteúdo é expressa pelo resumo criptográfico sobre o mesmo, evidenciando uma outra particularidade da assinatura digital – ela é única para cada documento. A autenticidade é então fundamentada na hipótese na qual a chave privada é de conhecimento apenas do suposto signatário. Além disso, como no documento eletrônico o que é realmente assinado é a representação intermediária da informação – os bits, supõe-se confiável todo o conjunto de componentes intermediários que possibilitam a visualização e assinatura do documento eletrônico. Além disso, características da escrita e da assinatura manuscrita que permitiriam identificar fatores emocionais do autor, evidenciando, por exemplo,

uma coação, não são perceptíveis nos seus análogos.

A natureza da assinatura digital ainda impossibilita um procedimento comum para assinaturas manuscritas – a assinatura prévia de um documento cujo conteúdo será fixado posteriormente.

Entretanto, a assinatura digital agrega uma funcionalidade que não é presente na assinatura manuscrita – a integridade. Por sua vez, a comprovação de que o conteúdo original do documento papel não foi alterado pode ser comprovado pela presença ou não de rasuras.

A tempestividade – possibilidade de comprovar a existência de um documento em determinado instante no tempo – no caso do documento papel pode ser alcançada pela análise do substrato físico, ou pela fixação da informação temporal, como um carimbo, por exemplo, por uma terceira parte confiável. Em documentos eletrônicos, essa âncora temporal pode ser alcançada pela aplicação de carimbos do tempo. Estes, contudo, sofrem de problemas semelhantes àqueles da assinatura digital.

Outra particularidade encontra-se na disponibilidade do documento, ou seja, a garantia de sua existência e acesso por aqueles autorizados. Em papel, está depende apenas da preservação e devida proteção do substrato físico. No caso do documento eletrônico sua preservação é complicada pela obsolescência induzida que será melhor descrita ao longo deste trabalho. Seu sigilo, quando baseado em técnicas criptográficas, ainda sofre da obsolescência característica de tais métodos.

Contudo, documentos eletrônicos têm sua disponibilidade favorecida pelo fato de que toda cópia é idêntica ao original, enquanto que o documento papel tende a sofrer o desgaste do tempo, e suas cópias, em geral, vão progressivamente perdendo a qualidade.

Essa obsolescência dos algoritmos criptográficos atinge igualmente as assinaturas digitais, e conseqüentemente os carimbos do tempo. Tal fato, em conjunto com outros fatores que do mesmo modo serão expostos ao longo deste trabalho, levam a mais uma particularidade dos documentos eletrônicos – sua eficácia probante, diferentemente do documento tradicional, diminui ao longo do tempo.

É interessante notar que para documentos em papel tanto a integridade quanto a tempestividade podem ser verificadas para partes destacadas do documento original, o que não é possível para documentos eletrônicos.

Em Fillingham (1997), ainda cita-se que uma última vantagem das assinaturas manuscritas frente as digitais é em relação à simplicidade e facilidade das primeiras. Em um caso de disputa judicial, as técnicas forenses usadas na detecção de fraudes podem ser facilmente explicadas a

advogados, juízes e júris. As assinaturas digitais, por outro lado, são extremamente complexas, envolvendo: teoria dos números, sistemas operacionais, protocolos de comunicação, processamento do caminho de certificação, políticas de certificação, entre outras coisas. Há um número limitado de pessoas que possuem o completo entendimento de todo o processo envolvido na geração e verificação de assinaturas digitais. Explicar estas etapas a advogados, juízes e júris não é tarefa fácil e o potencial de deixá-los confusos é grande.

Apesar da visível disparidade entre as formas documentais, os benefícios associados ao documento eletrônico tais como seu armazenamento e transmissão, tornam-no uma alternativa superior ao documento tradicional em diversas situações, o que tem levado a criação de diversas iniciativas, algumas delas citadas ao longo do presente trabalho, que visam agregar ao documento eletrônico atributos desejáveis nesse novo contexto.

3.3 EFICÁCIA PROBANTE DO DOCUMENTO ELETRÔNICO

Augusto T. R. Marcacini, presidente da Comissão de Informática Jurídica da OAB-SP, comenta que "O progresso da ciência sempre traz consigo uma mudança nos hábitos e comportamentos das pessoas. E destes novos relacionamentos humanos surgem novas relações jurídicas, ou novos fatos jurídicos a serem objeto de regulação por parte do Direito". Nesse sentido, o emprego do documento eletrônico para os mais diversos fins, incluindo transações, caracteriza uma nova forma de relacionamento e, por conseguinte, deve e está sendo objeto de regulamentação.

Tal regulamentação está intimamente ligada a própria finalidade de um documento – documentos, eletrônicos ou não, servem para comprovar um fato, sendo assim, a preocupação encontra-se na sua eficácia como instrumento de prova, a chamada "eficácia probante". Essa eficácia, em geral, está baseada em propriedades mínimas que o documento deve possuir. A Lei modelo da United Nations Commission on International Trade Law (UNCITRAL), por exemplo, requer do documento eletrônico, no mínimo, o exato grau de segurança que os documentos em papel oferecem, para que aqueles possam assim receber o mesmo nível de reconhecimento legal.

De modo geral, essas propriedades mínimas compreendem a garantia de autenticidade e integridade do documento. Sendo que, a tempestividade, pode se fazer necessária em alguns cenários. Por alcançar os dois primeiros atributos, a assinatura digital tem sido tema de diversas iniciativas no cenário mundial, em especial: a lei federal norte-americana Electronic Signatures in Global and National Commerce Act (E-Sign Act), de 2000; e a Diretiva 1999/93/EC do Parlamento Europeu.

No Brasil, a eficácia probatória dos documentos eletrônicos vem, igualmente, sendo objeto de regulamentação, por meio de iniciativas como: o projeto de lei do senado nº 22/96, que "Atribui valor jurídico à digitalização de documentos e dá outras providências"; o projeto de lei nº 1483/99, que "Institui a fatura eletrônica e a assinatura digital nas transações de "comércio" eletrônico"; o projeto de Lei nº 1589/99 proposto pela OAB/SP, que "Dispõe sobre o comércio eletrônico, a validade jurídica do documento eletrônico e a assinatura digital, e dá outras providências"; a Medida Provisória 2.200-2 e o projeto de lei 7316/02, que "Disciplina o uso de assinaturas eletrônicas e a prestação de serviços de certificação", que se destina a substituí-la.

Como exposto em Gandini, Jacob e Salomão (2001), quando editada em 29 de julho de 2001, pelo Presidente da República, a Medida Provisória de nº 2.200, que tratava da segurança jurídica do comércio eletrônico e do documento eletrônico, não mantinha paralelo com nenhuma legislação de país democrático, ou com a Lei Modelo da UNCITRAL, e tão pouco com os projetos de lei que tramitavam no Congresso. Divergia das leis da Diretiva Européia e do Projeto de Lei da OAB/SP em pontos como a obrigatoriedade da certificação das chaves junto a Autoridades Certificadoras credenciada pelo Comitê, além de falhas como o artigo n° 8, em que entre outras atividades, dava as Autoridades Certificadoras credenciadas, a responsabilidade de geração do par de chaves, pairando dúvidas quanto ao sigilo das mensagens dos titulares frente ao Governo Federal.

Posteriores edições da Mediada Provisória de nº 2.200, corrigiram esses e outros problemas, entretanto como descrito por Marcos da Costa, em Costa (2003), ainda restam questões, as quais nem a Medida Provisória 2.200-2 e nem o Projeto de Lei 1589/99 abordam.

É interessante esclarecer certos equívocos comuns no contexto das assinaturas digitais, em especial aquelas baseadas em certificados da ICP-Brasil. Entre eles encontra-se a idéia de que o titular do certificado não poderia negar a autoria de uma assinatura digital que lhe fosse atribuída – o chamado não-repúdio. Esta propriedade, contudo, é puramente técnica, e refere-se a relação existente entre o par de chaves. Juridicamente, como também esclarece Marcos da Costa: "Impedir alguém de negar uma assinatura, digital ou não, é a negação do Estado de Direito. Pode-se regular ônus de prova[1] de quem negar uma assinatura, mas jamais retirar de alguém o direito de impugná-la".

Outro erro é associar irretratabilidade ao não-repúdio. Tecnicamente, a irretratabilidade refere-se à impossibilidade de negar o conhecimento do conteúdo do documento, contudo, do ângulo jurídico, retratar-se significa arrepender-se, não querer mais cumprir um compromisso,

[1] "Ônus da prova é o encargo, atribuído pela lei a cada uma das partes, de demonstrar a ocorrência dos fatos de seu próprio interesse para as decisões a serem proferidas no processo" (DINAMARCO, , p. 71).

sem, entretanto, negar tê-lo assumido.

Em Costa (2003) ainda aponta-se a diferença entre certificados públicos e privados no contexto da Mediada Provisória de nº 2.200-2. Parte-se da noção de que um certificado nada mais é que um documento eletrônico assinado pelo emitente, e portanto deve-se aplicar a mesmas regras empregadas aos documentos públicos e privados – documentos públicos possuem a presunção de veracidade do Estado em face da sociedade, já o documento privado é aceito ou não em função da confiança que gera em seu destinatário. Assim, no tocante ao ônus da prova, a impugnação do relacionamento entre o titular e a chave, declarada no certificado, possui implicações diferentes para certificados ICP-Brasil, e certificados privados – para certificados privados o ônus da prova cabe a quem apresentou o certificado, já no caso de certificados ICP-Brasil, cabe a quem impugna, ou seja, ocorre a inversão do ônus da prova.

Por fim, como afirmado anteriormente, não é difícil imaginar cenários em que a tempestividade do documento torna-se um fator importante. No meio registral, por exemplo, existe o conceito de prioridade, no qual ocorre a prevalência dos direitos inscritos prioritariamente, em face dos direitos posteriormente registrados. Contudo, a tempestividade torna-se necessária também por questões técnicas – deve ser possível determinar a validade de um certificado no momento em que uma determinada assinatura digital foi aposta.

Os carimbos do tempo abordam esse problema. Estes são documentos digitais, assinados pela Autoridade de Carimbo do Tempo, que atestam que um determinado documento existia antes de um certo momento. Essas Autoridades de Carimbo do Tempo utilizam-se de fontes confiáveis para determinar a hora. Nesse sentido, a Lei nº 2.784, de 18 de junho de 1913, que "Determina a Hora Legal", e no seu regulamento, o Decreto nº 10.546, de 5 de novembro de 1913, que " Approva o regulamento para execução da Lei n. 2.784, de 18 de junho de 1913, sobre a hora legal", restabelecido e alterado pelo Decreto n° 4.264, de 10 de junho de 2002, que "Restabelece o regulamento aprovado pelo Decreto no 10.546, de 5 de novembro de 1913, que regulamenta a Lei no 2.784, de 18 de junho de 1913, e dá outras providências", definem o Observatório Nacional (ON) como fonte da Hora Legal do Brasil. Indo além, a criticada Portaria MCT nº 293, de 11 de maio de 2007, que "Dispõe sobre a execução dos serviços de natureza essencial relacionados à Hora Legal Brasileira, a serem oferecidos e assegurados pelo Observatório Nacional – ON", delega a ON, entre outras atividades, o controle sobre os carimbos do tempo no Brasil.

3.4 CONCLUSÃO

Primeiramente foram abordadas as questões sobre o documento eletrônico frente ao tradicional e sobre as assinaturas digitais frente às manuscritas. Esse processo de equivalência, como foi demonstrado, é de vital importância para que as novas tecnologias digitais possam desempenhar as mesmas tarefas que hoje são executadas pelas formas tradicionais. Como visto, esta demanda origina-se da popularização dos computadores pessoais e das redes de computadores, em especial a Internet.

Ainda na primeira seção, mostrou-se que mesmo com toda a tecnologia e processos análogos criados para que as novas ferramentas tecnológicas tenham as mesmas capacidades que as tradicionais, essas formas não são idênticas, mas podem ser equivalentes, desde que alguns critérios sejam atendidos. Assim, é possível se usufruir as vantagens que as novas tecnologias carregam, sem perder, por outro lado, as vantagens das formas anteriores que as tornam tão usuais, desde tempos remotos.

Na seção seguinte foram apresentados os requisitos necessários para que um documento tenha eficácia probante. Os documentos tradicionais, devido a grande facilidade, evolução, uso e independências externas, é mais utilizado hoje em dia, como forma de armazenar informações que possam vir a serem usadas como prova.

Os documentos eletrônicos, apesar de grandes vantagens em relação aos tradicionais, ainda não são largamente utilizados por depender de tecnologias para manter os requisitos de segurança, com a finalidade de ter valor jurídico. Entretanto, com a popularização dos computadores pessoais e a Internet, somado aos gastos com os documentos tradicionais, a demanda por este tipo de documento tem aumentando, tornando a existência dos dois tipos, com o mesmo valor, um fato.

4 PRESERVAÇÃO DE LONGO PRAZO DE DOCUMENTOS ELETRÔNICOS

4.1 INTRODUÇÃO

Desde a popularização dos computadores pessoais e em especial da rede mundial de computadores – a Internet, os documentos em papel vêm perdendo espaço para os documentos eletrônicos. Documentos em papel necessitam, por exemplo, de grandes espaços físicos para armazenamento, cuidados no manuseio e armazenamento e não são facilmente acessíveis. Já os documentos eletrônicos, entre outras coisas, não necessitam de muito espaço físico, possuem excelente disponibilidade e também requerem cuidados, mas apenas por quem os armazena – instituições de preservação e bibliotecas, para ilustrar. Os usuários podem receber uma cópia do arquivo, que será idêntica a "original", diferentemente dos documentos em papel.

Recentemente se iniciaram as preocupações com os arquivos digitais. Toda a história da humanidade está em arquivos: no passado, estavam armazenadas em papéis, pinturas e pedras, por exemplo. Hoje, muitas informações estão em meio eletrônico, sendo inviável transformá-las todas em papel, mesmo porque boa parte delas é de natureza dinâmica.

Pesquisas têm sido realizadas por diversas entidades, sejam acadêmicas, governamentais ou individuais, tamanha é a preocupação com o assunto. Um exemplo desta preocupação é a carta publicada pela UNESCO[1] chamando a atenção para a preservação digital. Os tratamentos que devem ser dados aos documentos eletrônicos, pesquisados até o momento, a fim de conservá-los disponíveis e utilizáveis, serão mostrados neste capítulo.

As duas primeiras seções tratam das duas principais propriedades de qualquer arquivo digital: a disponibilidade e interpretabilidade. A seguinte entra no mérito dos arquivos que necessitam de maior atenção por serem documentos, ou seja, que precisam ser aceitos por terceiros como documentos oficiais – o caráter probante. Por fim, a última seção trata do Open Archival Information System (OAIS), modelo de referência para sistemas de informação de caráter arquivístico.

[1] http://www.unesco.org.br/publicacoes/livros/cartapatrimonioarquivistico/mostra_documento

4.2 CONSERVAÇÃO DA DISPONIBILIDADE

A questão mais elementar, em se tratando da preservação de longo prazo de documentos eletrônicos, é a garantia da existência dos mesmos ao longo do tempo. Tal existência depende da integridade de seu suporte físico – as mídias – e estas podem falhar devido a exposição ao calor, umidade, contaminação ou mesmo por falhas nos dispositivos de leitura e escrita. Além disso tais dispositivos tendem a se tornar obsoletos com o passar do tempo.

Assim, a seleção de tais mídias mostra-se como um passo fundamental na conservação da disponibilidade dos documentos eletrônicos.

Nesse sentido, o Arquivo Nacional do Reino Unido recomenda que os seguintes pontos sejam levados em consideração ao escolher-se um tipo de mídia, mostrado em Paradigm Project (2007, p. 4):

- longevidade: deve durar pelo menos dez anos;
- capacidade: deve ser apropriada à quantidade de dados a serem armazenados e ao espaço físico do ambiente;
- viabilidade: deve possuir métodos robustos de detecção de erros para leitura e escrita de dados, sendo idealmente de escrita única (write-once);
- suporte de hardware, software e obsolescência: deve idealmente ser baseada em tecnologias maduras e amplamente disponíveis, preferencialmente padrões abertos;
- custo: comparações devem ser feitas no preço por base de MB/GB;
- a suscetibilidade da mídia a danos físicos;
- habilidade da mídia em tolerar condições ambientais diferentes.

As mídias estão divididas em três classes principais: magnética, óptica e de estado sólido.

As principais mídias magnéticas são as fitas, discos rígidos e disquetes. As fitas magnéticas são mais utilizadas em sistemas de backup off-line. Alguns tipos são utilizados pela indústria de áudio para seu armazenamento, pois as cópias não sofrem degradação. Para longo prazo, é necessário um controle da seqüência de bits (bitstream) e renovação constante da mídia. Os disquetes já existiram em diferentes tamanhos e capacidades, mas estão gradativamente desaparecendo devido a sua fragilidade e baixa capacidade. O grande destaque desta classe são os discos rígidos (HDs). É a tecnologia dominante como memória não volátil para os PCs,

pois são relativamente baratos e possuem boa capacidade de armazenamento, em comparação à outras tecnologias. Possuem vários tipos de interfaces, por exemplo, IDE, SATA e SCSI, com diferentes preços e performances. Sua longevidade gira em torno de cinco anos.

Segunda classe, as mídias ópticas possuem boa popularidade por serem freqüentemente utilizadas pelo comércio como suporte para vendas de álbuns de música, filmes, jogos e softwares – para citar alguns. Os CDs, que se expandiram substituindo os antigos discos de vinil como suporte de material fonográfico, e os DVDs, que são principalmente usados em substituição as fitas VHS, são os exemplos mais conhecidos. Claro que CDs e DVDs podem conter qualquer tipo de arquivo digital, não apenas músicas e vídeos. Para ambos existem as variações R e RW, respectivamente graváveis e regraváveis. Mais recentemente surgiram os discos de HD DVD e Blue-ray, mas que ainda não estão tão difundidos e estão competindo no mercado para ver qual das tecnologias dominará. Quanto a capacidade de armazenamento, temos os CDs, DVDs, HD DVD e Blue-ray, sendo que estes já possuem discos de 100 GB. Os CDs e DVDs possuem vida útil de 2 à 75 anos, segundo os fabricantes, dependendo das condições de uso, manejamento e armazenamento.

Como última classe, os dispositivos de estado sólido utilizam as chamadas memórias flash e são relativamente novos, em comparação às tecnologias anteriores. Os exemplos mais conhecidos são os cartões de memória, pen drives e mp3 players. Alguns discos rígidos foram lançados com essa tecnologia, por serem mais compactos, robustos, estáticos e eficientes em relação aos magnéticos, mas o preço ainda é uma barreira e a capacidade de armazenamento ainda não atingiu o patamar em que se encontram os discos rígidos magnéticos. As propriedades desse tipo de tecnologia, para longo prazo, ainda não são bem conhecidas.

Levando em consideração a longevidade das mídias, tecnologias e capacidades, é perceptível que os arquivos armazenados não são garantidos por longos períodos. Independente da mídia escolhida, mais cedo ou mais tarde, os arquivos nela armazenados precisarão ser copiados para uma nova mídia, podendo ser igual à mídia anterior ou diferente, neste caso não podendo haver alteração na seqüência de bits (bitstream). Essa estratégia de cópia é conhecida como renovação (do inglês refresh). A renovação deve ser feita com base na validade de uma tecnologia de armazenamento imposta pelo fabricante.

Em um serviço de armazenamento de documentos eletrônicos, um ponto de destaque deve ser a tolerância a falha em relação às mídias. O sistema precisa, de algum modo, possuir cópias de segurança (backup) a fim de evitar que algum arquivo seja perdido. Mídias magnéticas, por exemplo, não podem receber radiação eletromagnética, ou todos os dados serão perdidos. Mídias regraváveis são suscetíveis a uma regravação ou remoção acidentais, a exemplo dos

disquetes. Enfim, manter cópias de segurança dos arquivos é sempre uma boa prática.

Recomenda-se também manter cópias de segurança em mídias de diferentes naturezas, com o intuito de obter independência tecnológica – evitando um ponto único de falha. Caso as cópias sejam em mesmo tipo de mídia, deve-se tomar o cuidado de utilizar mídias de diferentes lotes, a fim de evitar que um lote defeituoso possa comprometer os arquivos armazenados.

4.3 CONSERVAÇÃO DA INTEPRETABILIDADE

Desde o advento dos computadores, principalmente os pessoais (PCs), existem esforços em questões de usabilidade, a fim de torná-los mais intuitivos e amigáveis com seus usuários e programadores. Neste sentido, a computação vem sofrendo constantes mudanças e atualizações, seja nos sistemas operacionais (a exemplo os gerenciadores gráficos, multiusuários ou multitarefas), seja nos programas executados sobre a plataforma. Juntando isso com outros fatores, como a grande concorrência entre empresas de softwares, a nenhuma regulamentação sobre os mesmos e a diversidade de soluções que podem ser propostas para um mesmo problema, chega-se ao atual estado de diversidade, ampliando as complicações em relação a interpretabilidade.

Em se tratando da preservação de longo prazo, a manutenção da propriedade de interpretabilidade esbarra em dois grupos de problemas: obsolescência de formatos e perda de contexto.

4.3.1 OBSOLESCÊNCIA DE FORMATOS

A eletrônica digital é baseada no sistema binário, cuja origem incerta é mais comumente atribuída a Leibniz no começo de 1666 (SCHWEICKERT, 2000). Este sistema está em vigor até os dias de hoje, devido a sua vantagem sobre outros mais complexos, como o decimal. Mas os bits precisam estar organizados, de alguma maneira, para serem processados e expressarem a vontade de seu criador. Surge então os arquivos, abstrações do mundo real para representar os itens em um sistema computacional. Todavia, existem diferentes tipos de arquivos, gerando a necessidade de formalizar a interpretação do conteúdo, culminando nos formatos.

Entretanto, levando em consideração as constantes atualizações no mundo digital, como por exemplo, falência de empresas, falta de documentação das soluções e patentes, formatos e seus respectivos softwares processadores acabam tornando-se marginais, desaparecendo pouco a pouco, e junto, seus conteúdos e suporte.

Com relação ao formato do arquivo digital, duas precauções são necessárias à preservação

de longo prazo: seleção de formatos e estratégias de preservação (em relação a interpretabilidade).

4.3.1.1 SELEÇÃO DE FORMATOS

A seleção de formatos para preservação de longo prazo não é uma tarefa trivial e devido sua complexidade, os pontos comentados a seguir devem ser analisados com cautela. Mclellan (2006, p. 6), em seu relatório final ao projeto InterPARES 2, aponta como critérios de seleção: uso bem difundido, origem não-proprietária, disponibilidade de especificações, independência de plataforma (interoperabilidade) e compressão. Brown (2003b, p. 5), no guia de preservação digital do Arquivo Nacional do Reino Unido, complementa essa lista com: estabilidade, suporte a metadados, conjunto de especificações, viabilidade, autenticidade, processabilidade e apresentação.

A escolha de um ou mais formatos deve ser orientada pensando-se em suprir a maior quantidade dos critérios listados. Levando em conta a literatura pesquisada sobre o assunto, três formatos são destacados, em especial os dois últimos: XML, PDF e ODF.

XML padrão aberto, é uma linguagem de marcação de propósito geral, recomendada e definida pelo W3C, derivada do padrão ISO SGML com a finalidade de ser simples e muito flexível como formato de texto (W3C, 1998). É dita linguagem extensível por permitir que o usuário defina suas próprias marcas (tags). Possui extensões, a exemplo, para validação e visualização. A principal vantagem é a preservação do conteúdo, pois o mesmo encontra-se separado da parte visual; a principal desvantagem é que um documento convertido poderá perder muito de sua formatação e leiaute.

PDF formato criado pela Adobe Systems para distribuição e troca mais seguras e confiáveis de documentos eletrônicos. Preserva a aparência dos documentos originais por carregar fontes, imagens, elementos gráficos e de leiaute dos mesmos (ADOBE SYSTEMS, 2007). É um padrão aberto e está sendo preparado para submissão à ISO. A principal vantagem é a preservação completa das características geradas por seu autor; a principal desvantagem é custo em processamento gerado por sua vantagem.

PDF/A padrão ISO desde outubro de 2005, baseado na referência do PDF – versão 1.4, foi desenhado especificamente para arquivamento de longo prazo de documentos eletrônicos. Impõe uma série de restrições a um PDF comum, como conteúdo dinâmico, para este fim. A Administração de Registros e Arquivos Nacional (NARA) dos Estados Unidos e o Arquivo Nacional da Suécia estão utilizando-o (BORSTEIN, 2007). A principal vantagem

é ser autocontido[2]. A principal desvantagem é possuir poucos softwares para criação e validação do formato, sendo os que existem proprietários. Entretanto o projeto GNU diz em seu site que futuramente lhe fornecerá suporte[3].

ODF padrão ISO/IEC, é um formato de arquivo para documentos de escritório eletrônico (a exemplo dos processadores de texto e planilhas) que aproveita sempre que possível padrões existentes para sua composição. Utiliza, por exemplo, XML para guardar o conteúdo e dados sobre o arquivo e é compacto por fazer uso do padrão ZIP de compressão, tornando o tamanho de seus arquivos reduzidos. A ABNT recentemente anunciou que pretende adotar o padrão ODF como norma brasileira até o fim do ano[4]. A principal vantagem é ser implementado por uma gama de software, proprietários e livres, além do apoio de grandes companhias como Sun Microsystems, IBM, Novell, Oracle – para citar algumas; a principal desvantagem é deixar a renderização por conta da interpretação da plataforma computacional, podendo trazer pequenas diferenças visuais entre diferentes softwares/SOs (OASIS, 2006).

4.3.1.2 ESTRATÉGIAS DE PRESERVAÇÃO

A escolha de um ou mais formatos que se adéqüem a uma determinada estrutura de armazenamento de longo prazo, mesmo que bem feita, possivelmente não será eterna. Novos formatos, mais adequados, compactos – enfim melhores, podem surgir, ou mesmo o suporte aos antigos deixar de existir, seja por mudanças no cenário de software ou hardware. Logo, é preciso pensar em estratégias para que o formato defasado possa ser processado ou transformado, com a finalidade de manter seu conteúdo legível às novas tecnologias.

Consoante Paradigm Project (2007, p. 16), as estratégias existentes são, principalmente, a migração e emulação. Das demais, consideradas variantes das mesmas, pode-se citar o encapsulamento, preservação tecnológica e arqueologia digital.

4.3.1.2.1 MIGRAÇÃO

> Migração é a transferência periódica de materiais digitais de uma configuração de hardware/software para outra, ou de uma geração de tecnologia de computação para uma geração subseqüente. O propósito da migração é para preservar a integridade dos objetos digitais e para conservar a capacidade de clientes para recuperar, exibir e usá-los em face da constante evolução tecnológica (RLG, 1996, p. 6, tradução nossa).

[2] Possuir todas as dependências necessárias para sua renderização.
[3] http://www.gnu.org/software/pdf/GoalsAndMotivations.html
[4] http://idgnow.uol.com.br/computacao_corporativa/2007/09/06/idgnoticia.2007-09-06.2579203921/

Com esta definição, a estratégia de migração seria o mesmo que a renovação. Mas, como reforçado por RLG (1996, p. 6), a migração inclui a renovação, diferindo no sentido que nem sempre é possível fazer uma réplica de um objeto digital de uma tecnologia em outra, trazendo maior complexidade em sua execução.

Apesar de os arquivos digitais não apresentarem o conceito de original (são réplicas perfeitas entre si), o processo de migração não é uma simples cópia, e devido a diferenças e peculiaridades dos formatos envolvidos na conversão, pode-se ter perdas semânticas, ou mesmo, de partes do conteúdo. Por esse motivo é considerado um movimento de risco.

Entretanto a migração não é nenhuma novidade, principalmente em se tratando da indústria da computação. Mesmo os mais modernos processadores x86 de hoje são compatíveis com as primeiras versões lançadas há anos. Não somente em hardware, mas em software existe essa grande preocupação em manter compatibilidade com versões anteriores. Normalmente, os fabricantes esforçam-se para que as novas versões não substituam as anteriores, pois com isso perderiam mercado. Os usuários não atualizariam seus programas e equipamentos se perdessem todo o conteúdo gerado em versões passadas dos mesmos. Todavia, essa compatibilidade costuma ser limitada, não só a poucas gerações, como também em funcionalidade – devido a complexidade de se validar as transições, fazendo com que informações sejam perdidas.

Segundo Paradigm Project (2007, p. 17), a migração é um campo vasto da preservação digital, possuindo muitas variações da abordagem geral. Abaixo são apresentadas três destas:

normalização "É a conversão de um objeto fonte de seu formato de dados original em um formato para arquivamento baseado em XML. O trabalho da conversão é automatizado pelo uso de aplicações específicas de software, chamados normalizadores, que convertem o objeto fonte original em XML." (HESLOP; DAVIS; WILSON, 2002, p. 18-19, tradução nossa). O Arquivo Nacional da Austrália utiliza-se desta técnica.

migração na obsolescência "Envolve a migração em andamento de um objeto digital para novos formatos, ou novas versões do formato original, no último momento possível antes que o formato existente torne-se obsoleto. Esta abordagem busca tirar vantagem da economia em escala e avanços em técnicas de migração, e depende do acesso a informação de confiança para entender o ciclo de vida dos formatos de arquivos. O Arquivo Nacional do Reino Unido é um defensor desta abordagem." (WILSON, 2007, p. 3, tradução nossa).

migração na requisição conforme Mellor, Wheatley e Sergeant (2002, p. 1-4), esta técnica, utilizada pelo projeto CAMiLEON, consiste em arquivar o objeto digital em seu formato

original. Ao receber uma requisição ao objeto, este deve ter suas informações extraídas para um formato intermediário que alimentará um módulo de saída, criando um novo objeto em um formato atual. Essa abordagem pretende se beneficiar de evoluções nas técnicas de migração, diminuir o esforço de programação (só é preciso programar o módulo de saída quando um formato expirar) e não carregar erros de conversão para os arquivos futuros.

4.3.1.2.2 EMULAÇÃO

> Um emulador [...] é o incorporamento binário de uma configuração específica de hardware na forma binária que pode ser preservado junto com metadados e dados. Com emuladores, um conjunto completo de softwares suportados, metadados, e o dado, o ambiente inteiro do documento pode ser recriado a partir dos bits armazenados em qualquer ponto do futuro (GILHEANY, 1998, p. 3, tradução nossa).

Ou seja, consiste na imitação do ambiente, parcial ou completa, em que o formato do arquivo era válido e das tecnologias envolvidas no período da criação do arquivo – conservando as exatas aparência e funcionalidade que seu criador desejou.

Do mesmo modo que a migração, essa técnica possui várias abordagens, mas poucas foram amplamente testadas. A emulação possui a grande vantagem de, em se tratando da preservação de arquivos, poder mostrá-lo como realmente foi feito, no melhor ambiente possível – comparado à migração.

Assim como a estratégia anterior, esta abordagem também não é nova na área da computação. Muitos fabricantes a utilizam para projetar, e assim poder testar, antes de produzir, reduzindo os custos. Um exemplo facilmente encontrado na Internet são os emuladores de jogos, tanto para as plataformas mais modernas – como o Playstation, quanto para outras que já não se encontram no mercado – como o Atari.

Paradigm Project (2007) cita que essa técnica está dividida em duas categorias: software emulando hardware e máquinas virtuais. Na primeira, um software é criado para imitar um hardware real. Por exemplo, podemos criar um software em um computador de arquitetura x86 para emular a arquitetura AVR. Já na segunda, um emulador imita uma máquina fictícia. Talvez o exemplo de máquina virtual mais conhecido de hoje seja a JVM, que possui implementação para diversas arquiteturas diferentes, mas todas as camadas superiores são as mesmas.

Utilizando-se desse conceito de máquina virtual, Lorie (2002) propôs a Universal Virtual Computer (UVC), técnica híbrida de emulação e migração, em um estudo de métodos de preservação de documentos digitais para a Biblioteca Nacional dos Países Baixos (Koninklijke Bib-

liotheek). A idéia principal da UVC é ser simples o bastante para ser relevante por um longo período de tempo.

O arquivo original a ser armazenado pode ser arquivado de dois modos (LORIE, 2002, p. 12-13):

a) o formato não é alterado de nenhuma forma a fim de simplificar a decodificação (e o programa UVC, indiretamente) – ilustrado na figura 4;

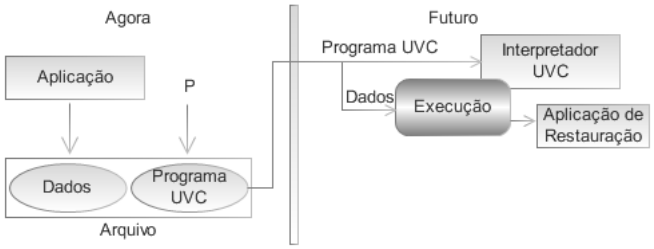

Figura 4: Opção 1.

b) extrair os dados relevantes do arquivo original e organizá-los em uma representação interna diferente – ilustrado na figura 5.

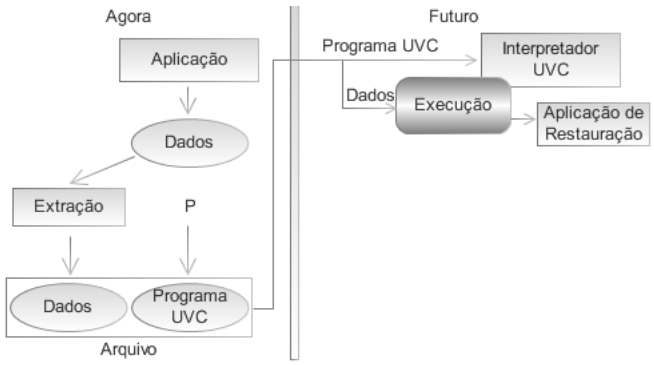

Figura 5: Opção 2.

Lorie (2002, p. 7-12) define os passos necessários a serem seguidos em cada período. Em tempo de arquivamento deve-se: a) definir o esquema lógico apropriado; b) escolher uma representação interna; c) escrever o programa UVC para a interpretação dos dados; d) arquivar a informação do esquema. Em tempo de restauração deve-se: a) ter certeza que um emulador está disponível para a máquina atual; b) escrever um programa de restauração para restaurar os dados; c) escrever um programa de restauração para restaurar o esquema.

No arquivamento, os dados e um programa P (que decodifica estes dados) são armazenados e têm sua seqüência de bits (bitstream) preservados. No futuro, o programa P é passado pelo

interpretador UVC (um emulador) sob controle do programa da aplicação de restauração. Como o programa de restauração repetidamente invoca o interpretador, cada iteração retorna um item de dado marcado. As marcações essencialmente associam um significado semântico com um item de dado (LORIE, 2002, p. 5). Este processo é mostrado na figura 6.

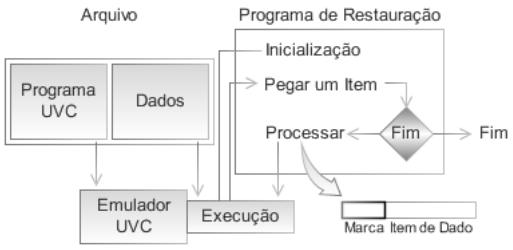

Figura 6: Execução.

4.3.1.2.3 ENCAPSULAMENTO

Técnica que consiste em agrupar, junto ao arquivo, instruções, softwares, especificações, metadados de preservação e qualquer utilidade para prover acesso ao objeto digital. Com esses detalhes de como interpretar os bits é possível proteger-se da obsolescência. É atingida fazendo-se uso de estruturas lógicas chamadas de containers ou wrappers, que oferecem um relacionamento entre as informações componentes.

Beagrie e Jones (2002) citam como vantagens: garante que toda a informação de suporte necessária para acesso seja mantida como uma entidade; pode, potencialmente, superar parte de grandes desvantagens de estratégias alternativas; provê um meio útil de concentrar atenção em quais elementos são necessários para acesso. E como desvantagens: pode produzir arquivos com duplicação muito grandes (a exemplo dos visualizadores) ao longo da coleção a menos que essas ligações sejam mantidas; software encapsulado ainda é aberto para uma rápida obsolescência tecnológica.

4.3.1.2.4 PRESERVAÇÃO TECNOLÓGICA

> Como a emulação, esta abordagem concentra-se no ambiente tecnológico ao contrário do objeto digital. Ao invés de imitar o ambiente original, esta abordagem envolve a preservação do objeto digital junto com todo o hardware e software atuais requeridos para manter acesso ao objeto; isto inclui sistemas operacionais, software de aplicação original e dispositivos de mídia (PARADIGM PROJECT, 2007, p. 24).

Beagrie e Jones (2002) citam como vantagens: retenção da funcionalidade e aparência do arquivo original; ganha-se tempo quando outra estratégia de preservação for necessária; talvez

seja a estratégia mais prática para recursos digitais complexos em médio prazo. E como desvantagens: não é viável para longo período, podendo ser usada apenas para curto e médio prazos; suporte técnico vai, inevitavelmente, desaparecer em um tempo relativamente curto; facilitação de acesso tornar-se-á gradativamente problemática com o passar do tempo. Paradigm Project (2007, p. 24) ainda acrescenta como desvantagens: implicações em custo e espaço para adquirir e manter grande quantidades de hardware são proibitivos; licenças de softwares (aplicações e sistema operacionais) precisam ser adquiridas; a capacidade de ler certos tipos de arquivos antigos degradar-se-á devido ao degradamento, e conseqüente diminuição das máquinas até suas falhas; documentação para ambientes de computação antigos podem ser difíceis de localizar.

4.3.1.2.5 ARQUEOLOGIA DIGITAL

> Arqueologia digital é um neologismo que significa restaurar, através de trabalho altamente especializado, fontes digitais que se tornaram inacessíveis como resultado da obsolescência tecnológica e/ou degradação de mídia. De fato, não se trata de uma estratégia em si, uma vez que será aplicada sempre que objetos digitais ficarem fora do programa sistemático de preservação digital (THOMAZ, 2004, p. 134)

É vista como o último recurso na preservação digital: uma vez que todas as técnicas aplicadas falharam, o objeto digital deixa de ser acessível. Mas se sua seqüência de bits foi conservada, pode-se recuperar a informação, mesmo que parcialmente.

Beagrie e Jones (2002) apontam como vantagens: crescente número de serviços terceirizados especializados oferecendo este serviço; tem-se mostrado tecnicamente possível recuperar grande parte das informações de mídias danificadas ou obsoletas. E como desvantagens: muito mais custosa em longo prazo que estratégias de preservação digital verdadeiras; é improvável ter custo efetivo pra outra coisa senão o mais valioso dos recursos digitais; materiais potencialmente úteis que não justificam os custos envolvidos serão perdidos; risco de alguns materiais digitais não poderem ser recuperados com sucesso; gerenciamento inferior do investimento inicial.

4.3.2 PERDA DE CONTEXTO

No cenário atual, um número grande de documentos está em forma digital, e a tendência é que esse volume aumente cada vez mais, pois a Internet e os computadores pessoais têm se popularizado. Em uma biblioteca, por exemplo, os livros são organizados por seções e estas por estantes, com rótulos informando a categoria dos livros, assunto, entre outras informações. No mundo digital é preciso ter uma referência análoga – os metadados, pois sem eles ter-se-ia

grandes gastos computacionais na pesquisa de um determinado documento, inviabilizando o armazenamento digital.

Cunningham (2001) cita que o termo metadado emergiu da comunidade de TI há muitos anos e que se refere somente aos dados necessários para que os dados armazenados em um sistema de computador façam sentido. A imprecisão da definição de metadados como "dados sobre dados" permitiu que esta fosse aplicada para qualquer informação descritiva relacionada a computadores e que se tornou tão flexível que agora não precisa sempre estar relacionado à tecnologia de computadores. Sua proposta de definição para metadados é: "Informação estruturada que descreve e/ou permite encontrar, gerenciar, controlar, entender ou preservar outra informação ao longo do tempo".

Ou seja, metadados são informações associadas a um determinado arquivo que permitem descrever características importantes sobre a obra, facilitando o processo de armazenamento e busca. No contexto da preservação de longo prazo, também são utilizados para criar e armazenar um histórico do documento. Caso um documento precise ser modificado, a exemplo de um processo de migração, o fato seria registrado em seus metadados.

Do mesmo modo que qualquer documento, os metadados precisam de um formato. Tendo como base os formatos de arquivos expostos anteriormente (XML, PDF e ODF), são apresentados aqui alguns formatos de metadados a eles relacionados:

XMP (eXtensible Metadata Platform) criado pela Adobe Systems para seus produtos, é codificado em texto XML formatado, usando o RDF[5] do W3C (ADOBE SYSTEMS, 2005).

MARC (Machine-Readable Cataloging): é um padrão para informações bibliográficas que inclui uma descrição do item, entrada principal e adicionadas, cabeçalho de assunto e classificação (podendo conter bastantes mais informações) com a finalidade de ser lido por máquinas. É utilizado principalmente por bibliotecas (FURRIE, 2003).

Dublin Core é um padrão para descrição de recursos que atravessam domínios (cross-domain), não limitando o escopo do que pode ser um recurso. É também baseado no RDF do W3C (NISO, 2007). É utilizado por importantes projetos, como por exemplo, o ODF.

MODS (Metadata Object Description Language) esquema para um conjunto de elementos bibliográficos que pode ser usado para uma variedade de objetivos, em particular para aplicações de biblioteca. É expresso utilizando esquemas XML do W3C, com o intuito

[5] "Integra uma variedade de aplicações desde catálogos bibliográficos [...] e conteúdo para coleções pessoais de música, fotos, e eventos usando XML como uma sintaxe de intercâmbio. A especificação RDF provê um sistema ontológico leve para suportar a troca de conhecimento na Web" (W3C, 2004, tradução nossa).

de poder utilizar MARCs já existentes assim como permitir a criação de registros de descrição de recursos originais (THE LIBRARY OF CONGRESS, 2007).

4.4 CONSERVAÇÃO DA EFICÁCIA PROBANTE

Muitos são os cenários nos quais a eficácia probante de um documento deve ser mantida por um longo ou até mesmo indefinido período. Em se tratando de documentos eletrônicos, tal eficácia, como visto, é atualmente alcançada com o emprego de assinaturas digitais. Entretanto, diferentemente das assinaturas tradicionais, essas assinaturas não mantêm sua validade ao longo do tempo. Assim, caso não sejam tomadas as devidas precauções, um documento que hoje possui eficácia probante, num futuro não a terá mais.

4.4.1 COMPROMETIMENTO DAS INFORMAÇÕES DE VALIDAÇÃO

A constatação da validade de uma assinatura é dependente de inúmeros fatores, que vão desde a confiança nas tecnologias criptográficas utilizadas, até a disponibilidade e validade das informações necessárias à verificação da assinatura. Em curto prazo, por exemplo, uma assinatura que anteriormente era válida, pode deixar de ser, devido à expiração do certificado do assinante, ou mesmo de qualquer outro certificado do caminho de certificação, e a impossibilidade de determinar se tal assinatura foi feita antes ou depois da expiração. Obviamente, nesse caso, a adição de um carimbo do tempo à assinatura, antes de tal expiração, seria suficiente pra demonstrar tal ato foi realizado enquanto os certificados eram válidos. Pensando em problemas como esses, extensões para as assinaturas nos formatos CMS e XMLDSig foram propostas – respectivamente CMS Advanced Electronic Signatures (CAdES) (ETSI, 2007) e XML Advanced Electronic Signatures (XAdES) (ETSI, 2006). Essas extensões assumem diferentes formas dependendo das informações mínimas que devam possuir.

A formas CAdES-T e XAdES-T, adicionam um carimbo do tempo a assinatura convencional. Como no exemplo acima, esse carimbo do tempo permite constatar que a assinatura digital foi aposta enquanto os certificados do caminho de certificação eram válidos. Ou seja, que os certificados que formam o caminho desde o certificado correspondente a chave privada usada na assinatura até uma ancora confiável não tinham sido revogados e estavam dentro do período de validade.

Em longo prazo, contudo, esses dados de validação – certificados e informações de revogação – podem não estar mais disponíveis, impossibilitando a verificação da validade da assinatura. Nesse sentido, as formas CAdES-C e XAdES-C permitem referenciar essas infor-

mações, de forma que estas possam ser guardadas num repositório local.

No acaso do comprometimento de alguma das chaves utilizadas pelos provedores das informações de validação, por exemplo, a chave privada de alguma Autoridade Certificadora, seria possível forjar os dados de validação. Nesse caso, numa disputa, a apresentação desses dados, com o intuito de demonstrar a validade de uma assinatura, seria questionável, pois não seria possível determinar se o certificado foi criado antes ou depois do comprometimento. Novamente, um carimbo do tempo é empregado de forma a ser possível constatar que tais informações foram obtidas em tempo hábil. Tal estrutura é especificada nas formas CAdES-X e XAdES-X. Tem-se, ainda, ao anexar os dados de validação à própria assinatura, as formas CAdES-X-L e XAdES-X-L.

As formas autocontidas CAdES-X-L e XAdES-X-L, portanto, provêem as informações necessárias a verificação em longo prazo de uma assinatura digital. No entanto, tais esquemas estão alicerçados em algoritmos criptográficos que devem suprir determinadas propriedades. Um algoritmo de resumo criptográfico, por exemplo, deve ser resistente a colisões.

4.4.2 OBSOLESCÊNCIA DE ALGORÍTMOS E PARÂMETROS

A história mostra que esquemas criptográficos, com o passar do tempo, tendem a perder suas propriedades frente aos avanços nas áreas da criptografia e o aumento do poder computacional. A função de resumo criptográfico MD5, desenvolvida por Ronald Rivest em 1991, por exemplo, foi amplamente adotada pelo mercado, porém, em 1996 Dobbertin descobriu uma falha no algoritmo (DOBBERTIN, 1996) suficientemente grave para levar a comunidade a desaconselhar seu uso para certas aplicações. O mesmo acontece atualmente com o algoritmo SHA-1 (NIST, 2007), e do mesmo modo aconteceu com toda a série MD.

Em se tratando de assinaturas digitais, como detalhado em Stallings (2005), dentre suas propriedades espera-se que seja impossível construir uma nova mensagem para uma dada assinatura e, seja igualmente impossível forjar uma assinatura para uma dada mensagem. Assim, uma assinatura que faça uso de um algoritmo de resumo criptográfico que não mais seja resistente à colisão perderá a primeira propriedade. Nesse caso, numa disputa a apresentação dessa assinatura teria utilidade questionável, pois, teoricamente, a outra parte poderia apresentar a mesma assinatura apontado para outro documento.

A segunda propriedade seria perdida caso, por exemplo, o algoritmo de cifragem assimétrica venha a se tornar fraco, possibilitando que a chave privada seja deduzida a partir da chave pública e, portanto, permitindo a um atacante assinar qualquer documento em nome do titular da

chave privada. Por conseguinte, a apresentação numa eventual disputa de tal assinatura, mesmo que tenha sido aposta enquanto o algoritmo era considerado forte, também é questionável, uma vez que qualquer documento poderia ter sido assinado com essa chave.

É perceptível que a perda de credibilidade de tais assinaturas ocorrem pela impossibilidade de determinar se estas foram apostas antes ou depois do comprometimento das tecnologias criptográficas envolvidas. Sendo assim, o emprego de carimbos do tempo, mais uma vez, torna-se necessário. Apesar de mesmo as formas CAdES-T e XAdES-T já possuírem carimbos do tempo, estes por sua vez também tornam-se vítimas da obsolescência dos algoritmos e parâmetros utilizados, sendo necessário, portanto, um processo contínuo.

Ilustrando, supondo que um documento com assinatura na forma CAdES-X-L, cujo carimbo do tempo tenha sido assinado por meio da combinação SHA-1 e RSA, com comprimento de chave de 768 bits, deva manter seu valor probante até 2016. Seguindo as recomendações da ETSI, tal combinação seria confiável até 2008, não sendo mais segura a partir de 2015. Contudo, a mesma recomendação especula que a combinação SHA 224 e RSA com chave de 2048 bits será segura mesmo a partir dessa data. Sendo assim, é aconselhável aplicar um novo carimbo do tempo antes de 2008 utilizando a segunda combinação. Teoricamente, dessa forma, em 2016 seria possível provar que o documento foi assinado enquanto a primeira combinação era válida.

As formas CAdES-A e XAdES-A suportam tal procedimento, porém é necessário monitorar continuamente as tecnologias criptográficas envolvidas na assinatura. Entidades como o NIST, a ETSI, e a Federal Network Agency da Alemanha desenvolvem este trabalho, e publicam periodicamente seus resultados. Essas publicações, todavia, são textuais. Nessa direção o grupo de trabalho Long-Term Archive and Notary Services (LTANS), busca a padronização de uma estrutura de dados que permita o processamento por maquina de tais informações (KUNZ; OKUNICK; PORDESCH, 2007).

O mesmo grupo tem trabalhado na definição de estruturas de dados e protocolos para o uso seguro de serviços notariais e de arquivamento de longo prazo, dentre eles Wallace (2007a), Blazic, Sylvester e Wallace (2007), Wallace (2007b), e Gondrom, Brandner e Pordesch (2007). Este último generaliza a estratégia empregada nos formatos CAdES-A e XAdES-A, com foco no tratamento de grandes volumes de documentos.

Uma primeira questão abordada refere-se ao número de carimbos do tempo necessários – os documentos são arbitrariamente agrupados, sendo necessário apenas um para cada conjunto. Tal procedimento é justificável uma vez que a aplicação de um carimbo do tempo é um processo lento, que entre outras etapas envolve a interação, em geral, pela rede, com a Autoridade de Carimbo do Tempo.

Uma forma possível de implementar esse mecanismo seria por listas de resumo criptográfico *L*, seguindo os seguintes passos:

1. a função de resumo criptográfico é aplicada a cada um dos *N* documentos do conjunto;
2. os resumos criptográficos obtidos são ordenados de forma crescente, e então concatenados, formando *L*;
3. aplica-se $d = H(L)$;
4. o carimbo do tempo é aplicado sobre *d*.

Contudo, como o carimbo não é aplicado diretamente sobre o documento, mas sim sobre uma estrutura de dados *L* que representa de forma não ambígua o conjunto de documentos, é necessário provar que o documento em questão pertencia ao conjunto. No caso acima, juntamente com o carimbo do tempo, seria necessário, portanto, prover *N-1* resumos criptográficos como prova de associação. O que torna a abordagem inviável.

Assim, em Gondrom, Brandner e Pordesch (2007), faz-se uso de árvores de resumo criptográfico, primeiramente apresentadas por Merkle (1980), onde:

1. a função de resumo criptográfico é aplicada a cada um dos *N* documentos do conjunto. Os resumos criptográficos obtidos serão as folhas da árvore;
2. para cada grupo de resumos, com mais de um elemento, os resumos do grupo são ordenados de forma crescente, e então concatenados, formando *L*. Caso seja interessante ter uma árvore onde cada nó pai tem o mesmo número de nós filhos, pode-se acrescentar resumos criptográficos de dados arbitrários a *L*;
3. aplica-se $H(L)$;
4. se ainda há grupos de resumos, com mais de um elemento, repetir os passos 2 e 3 até existir apenas um resumo criptográfico d, que será a raiz da árvore;
5. o carimbo do tempo é aplicado sobre *d*.

Nesse caso a prova de associação para um documento em específico, denotada por *P*, é a redução dessa árvore, seguindo os seguintes passos:

1. obtém-se o resumo criptográfico *h* do documento;

2. seleciona-se todos os resumos criptográficos que possuem o mesmo nó pai que h;

3. os resumos selecionados são ordenados de forma crescente, e então concatenados. O resultado é inserido em P;

4. aplica-se os passos 2 a 3, para o nó pai, até alcançar a raiz da árvore. Os nós pai não são inseridos, pois são computáveis.

Dessa forma tem-se provas de associação menores, onde o tamanho é $O(log|N|)$. Tomando-se grupos de 1024 documentos, por exemplo, na primeira abordagem, a prova de associação teria 1023 elementos, na segunda, com o uso de árvores binárias, apenas 10. Um segundo ponto tratado na especificação, refere-se a diferenciação dos eventos críticos.

Como visto na seção 2.7, um carimbo do tempo é um documento eletrônico assinado pela Autoridade de Carimbo do Tempo, composto por, entre outras informações, o resumo criptográfico dos dados que se quer provar a existência, e o momento da emissão do carimbo.

Nas formas de assinatura avançada CAdES-A e XAdES-A, na ocasião de qualquer evento crítico o carimbo do tempo é aplicado sobre os documentos que foram assinados, as propriedades assinadas, as assinaturas, as informações de validação, e os carimbos do tempo anteriores. Em Gondrom, Brandner e Pordesch (2007), no entanto, o novo carimbo do tempo é aposto apenas aos dados comprometido pelo evento crítico ocorrido.

Assim, naqueles eventos em que se torna necessário provar que o carimbo atual foi feito antes que fosse possível forjar um carimbo para uma mensagem arbitrária, o novo carimbo do tempo cobre apenas o antigo. Tais eventos são: comprometimento da chave privada da Autoridade de Carimbo do Tempo; expiração do certificado da Autoridade de Carimbo do Tempo; enfraquecimento do algoritmo assimétrico, parâmetros ou algoritmo da função resumo criptográfico utilizado no último carimbo do tempo. A esse procedimento dá-se o nome de Renovação de Carimbo do Tempo.

Quando se torna possível a alteração dos dados protegidos pelo último carimbo do tempo, sem invalidar a assinatura da Autoridade de Carimbo do Tempo, o carimbo é, então, aplicado sobre todos os dados, incluindo os carimbos do tempo anteriores, da mesma forma que ocorre nas formas de assinatura avançadas anteriormente detalhadas. Tal evento ocorre quando algoritmo da função resumo criptográfico utilizado na árvore de resumo criptográfico não é mais seguro. A esse procedimento dá-se o nome de Renovação da Árvore de Resumo Criptográfico.

A estrutura que comporta os mecanismos acima descritos, é especificada em Gondrom, Brandner e Pordesch (2007), pela Sintaxe de Registro de Evidência. Um Registro de Evidência

é, portanto, uma estrutura de dados, contendo um conjunto de carimbos do tempo, e um conjunto de provas de associação. Nesse sentido, para provar a manutenção da eficácia probante de um documento eletrônico, é necessária a apresentação de um Registro de Evidência, cujas operações de Renovação de Carimbo do Tempo, e Renovação da Árvore de Resumo Criptográfico tenham sido feitas em tempo hábil.

Uma última abordagem critica as anteriores pela necessidade de em tais esquemas as primeiras assinaturas precisarem ser validadas em longo prazo. Apontam, que nesse caso, no futuro, as terceiras partes confiáveis, envolvidas nas etapas iniciais, podem não mais ser confiáveis, ou sequer conhecidas. Igualmente, apontam o problema de determinar se os eventos críticos realmente aconteceram depois da aplicação dos carimbos do tempo. Esquemas como aqueles detalhados em Lekkas e Gritzalis (2004) e Ansper et al. (2001) focam na utilização dos serviços notariais, com foco na transição sucessiva de confiança, para solucionar tais problemas.

4.4.3 O PROBLEMA DA CONVERSÃO DE FORMATOS

A preservação da eficácia probante de documentos eletrônicos é ainda mais dificultada quando a estratégia de conservação da interpretabilidade adotada é a migração de formatos.

Na seção 4.4.2, viu-se que a preservação da eficácia probante baseia-se nos conceitos de assinatura digital e carimbo do tempo, vistos nas seções 2.6 e 2.7, respectivamente; ambos são baseados no resumo criptográfico, sendo esta característica que torna a migração um problema a mais.

Na estratégia de migração, apresentada na seção 4.3.1.2.1, os bits que constituem o documento eletrônico sofrem transformação para adequar-se a um novo formato, levando o novo documento a possuir resumo criptográfico diferente do original.

Essa diferença, por conseguinte, implica na inutilização dos dados que garantem a eficácia probante. Estes não são válidos para o novo documento, e o sendo para o antigo, o conteúdo deste último tende a perder a interpretabilidade.

Problema similar ocorre na impressão de documentos eletrônicos com assinaturas digitais e carimbos do tempo apostos – estes perdem o sentido no documento papel.

Projetos como o BMWi (2004) abordam tal problema, formalizando a conversão dos documentos. Contudo apontam para a necessidade do ateste de um notário como garantia da preservação da semântica do conteúdo após a migração de formato. Além disso, o mesmo ateste pode vir a confirmar a validade das assinaturas apostas.

4.5 MODELO DE REFERÊNCIA OPEN ARCHIVAL INFORMATION SYSTEM (OAIS)

O modelo de referência Open Archival Information System (OAIS) é um arcabouço conceitual para a discussão e comparação de arquivos. Na realidade, o modelo não especifica uma forma de implementação em particular, apenas define uma terminologia e um conjunto de conceitos, bastante genéricos, que visam elucidar as principais atividades relativas a preservação da informação.

Sua adoção tem-se dado entre as instituições de maior renome na área de preservação digital, sendo base para projetos como: CURL Exemplars in Digital Archives (CEDARS), Networked European Deposit Library (NEDLIB), Online Computer Library Center/ Research Libraries Group (OCLC/RLG), Preserving and Accessing Networked Documentary Resources of Australia (PANDORA) e DSpace.

Desenvolvido pela Consultative Committee for Space Data Systems (CCSDS), foi aprovado como CCSDS 650.0-B-1 em janeiro de 2002, tornando-se padrão ISO 14721 em 2003 e, posteriormente, servindo de base para a norma ABNT NBR 15472, publicada em 2007.

Mais especificamente, trata-se de um modelo de referência para um OAIS – organização de pessoas e sistemas que assumiu a responsabilidade de preservar informação por longo prazo e torná-la acessível a determinada classe de consumidores definida como comunidade-alvo. Provendo, nesse sentido: uma terminologia, na qual espera-se encontrar termos análogos aqueles já usados em disciplinas e organizações de preservação de informação; a identificação de áreas potenciais para o desenvolvimento de padrões relacionados; um arcabouço conceitual, onde se especifica: o ambiente OAIS, o modelo de informação e o modelo funcional; os requisitos mínimos a um arquivo para estar em conformidade com o modelo de referência OAIS; e esquemas de interoperabilidade de arquivos.

4.5.1 O AMBIENTE OAIS

O ambiente OAIS compreende o próprio arquivo, e aquelas entidades que com ele interagem, sendo elas: os produtores, consumidores, e a administração. Como produtores entende-se aqueles – pessoas ou sistemas clientes – que exercem o papel de provedor da informação a ser preservada. Os consumidores são as entidades interessadas nessas informações, sendo a comunidade-alvo, uma classe especial de consumidores, para os quais o OAIS tem a responsabilidade de manter as informações compreensíveis. E, por último, a administração, que cuida de assuntos mais gerais do arquivo – por exemplo, estabelecimento de políticas, avaliação dos

processos, e resolução de conflitos – não se envolvendo na rotina diária do OAIS. A figura 7 ilustra esse ambiente.

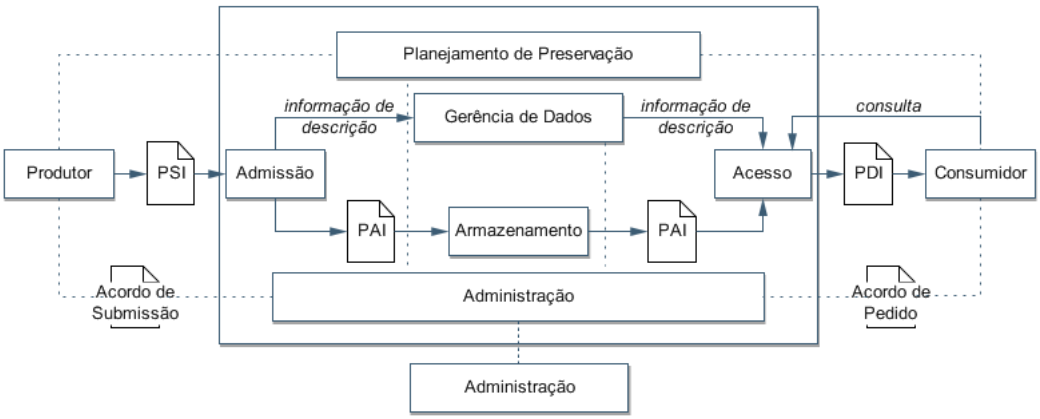

Figura 7: Ambiente OAIS

4.5.2 MODELO DE INFORMAÇÃO

No modelo de referência OAIS, uma informação significativa – ou um objeto de informação para a comunidade alvo, é dado pela interpretação do objeto de dados por meio da informação de representação a ele associada combinada com a base de conhecimento do consumidor. Por exemplo, o entendimento das informações contidas num documento digital, no formato ASCII, contendo um texto em inglês, depende da interpretação do objeto de dados – seqüência de bits, por meio da informação de representação – que define como a seqüência de bits será mapeada em símbolos, combinada à base de conhecimento do leitor – compreensão da língua inglesa escrita.

A informação de representação possui um caráter recursivo, pois, do mesmo modo, necessita ser interpretada – dando origem a uma rede de representação. O modelo de referência, por sua vez, aconselha que essa recursão termine num documento físico. Essa mesma informação de representação, entretanto, pode estar inserida no código fonte de um software de acesso. O problema dessa abordagem, no entanto, é o claro entendimento dessa informação uma vez que a mesma encontra-se misturada com algoritmos de processamento e desenho, sendo o problema ainda mais agravado no caso de formatos proprietários.

No ambiente OAIS, os objetos de informações, quando armazenados ou quando objetos de submissões ou disseminações levam consigo informações adicionais recebendo o nome de pacotes de informação. Um pacote de informação identifica e liga – lógica ou fisicamente – a informação de conteúdo e a informação de descrição de preservação (IDP) por meio da

informação de empacotamento.

A informação de conteúdo é o objeto de informação que se quer preservar, a IDP é o objeto de informação associado de forma a identificar claramente a informação de conteúdo e explicitar o contexto no qual ela foi criada.

Uma IDP possui quatro tipos de informação de preservação: a referência, que identifica de forma única à informação de conteúdo; o contexto, que explicita como a informação de conteúdo se relaciona com outras informações externas, por exemplo, descrevendo o motivo de sua criação, ou sua relação com outras informações de conteúdo; a proveniência que descreve sua cadeia de custódia, desde sua origem; e a fixidez que protege a informação de conteúdo de alterações não documentadas – tal proteção é alcançada, por exemplo, com a utilização de códigos de redundância cíclica (CRC) e de assinaturas digitais.

Associado a um pacote de informação, ainda encontra-se a informação descritiva que compreende o conjunto de informações de apoio para a localização e recuperação do pacote.

É interessante notar que tanto a informação de conteúdo, quanto a IDP, a informação de empacotamento, e a informação descritiva são objetos de informação e, portanto possuem redes de representação associadas.

Dependendo da sua função dentro do ambiente OAIS, os pacotes de informação especializam-se em pacote de submissão de informação (PSI), pacote de arquivamento de informação (PAI) e pacote de disseminação de informação (PDI). O PSI é provido pelo produtor, e segue as políticas descritas no acordo de submissão estabelecido entre ele e o OAIS. O PAI é o pacote que é efetivamente preservado. Por último, o PDI é o pacote obtido pelo consumidor seguindo as políticas do acordo de pedido estabelecido entre ele e o OAIS.

4.5.3 MODELO FUNCIONAL

Os processos-chave, típicos da maioria dos arquivos dedicados a preservação de informação digital, são identificados no Modelo de Referência OAIS por meio das entidades funcionais, sendo elas: Admissão, Arquivamento, Gerenciamento de Dados, Administração do Sistema, Planejamento de preservação e Acesso.

A Admissão provê os serviços e funções para o recebimento de PSIs dos produtores, ou de elementos internos ao arquivo, e a preparação do pacote para ser gerenciado e armazenado no OAIS. Sendo assim, suas funções incluem: recebimento e verificação da qualidade dos PSIs; geração e envio dos PAIs para a entidade de Arquivamento; e geração e envio das informações de descrição dos PAIs para a entidade de Arquivamento.

O Arquivamento provê os serviços e funções para o armazenamento, manutenção e resgate de PAIs. Desse modo, suas funções incluem: recebimento de PAIs da entidade de Admissão; posicionamento de novos PAIs na área de armazenamento de acordo com critérios como, por exemplo, taxa de utilização esperada e requisitos de suporte; gerência da hierarquia da área de armazenamento; renovação de mídias; execução de rotinas de verificação de erro; execução de procedimentos para a recuperação de desastres; e fornecimento de cópias dos PAIs para a entidade de acesso.

O Gerenciamento de Dados provê os serviços e funções para atualização e acesso de informações descritivas e de gerência de PAIs. Sendo assim, suas funções incluem: administração das bases de dados de informações descritivas e de gerência; e geração de relatórios sobre esses dados.

A Administração do Sistema provê os serviços e funções para as operações mais gerais do arquivo. Dentre elas: estabelecimento e cumprimento de políticas; avaliação dos processos; migração e atualização do conteúdo do arquivo; configurações de software e hardware; e suporte aos clientes.

O Planejamento de Preservação provê os serviços e funções de monitoramento do ambiente OAIS provendo recomendações para garantir que as informações arquivadas se mantêm acessíveis a comunidade-alvo com o passar do tempo, mesmo que o ambiente computacional original torne-se obsoleto. Dessa forma, suas funções incluem: monitoramento das mudanças no ambiente tecnológico, nas demandas de serviço e da base de conhecimento da comunidade-alvo; recomendações para migrações de informações arquivadas, para o modelo dos pacotes de informação e para padrões e políticas do arquivo; e desenvolvimento de planos de migração, protótipos, e planos de teste de forma a habilitar a Administração a efetuar migrações.

O Acesso provê os serviços e funções de suporte aos consumidores de forma que estes possam determinar a existência, localização, descrição e disponibilidade das informações armazenadas no OAIS, permitindo que estes requisitem e recebam produtos dessas informações. Suas funções incluem: suporte a comunicação com os consumidores para recebimento de solicitações; aplicação de controles para limitação de acesso; coordenação da execução de solicitações de forma que sejam corretamente atendidas; geração e entrega de PDIs aos consumidores.

4.5.4 INTEROPERABILIDADE

Diversos motivos podem levar a interação ou cooperação entre diferentes arquivos, como por exemplo, a redução de custos ou a melhoria da qualidade de serviço. O Modelo de Refer-

ência OAIS descreve quatro categorias formadas por essas associações, sendo elas: arquivos independentes, cooperados, federados e arquivos de recursos compartilhados.

Arquivos independentes são motivados apenas por preocupações locais sendo assim definidos pela falta de gerência ou interação técnica entre eles. Tais arquivos atendem apenas a uma comunidade-alvo.

Cooperações de arquivos ocorrem quando estes possuem em comum potencias produtores, padrões de submissão e de disseminação, porém não possuem as mesmas facilidades de busca.

Arquivos federados, por sua vez, são formados por comunidades-alvo originais, e uma comunidade-alvo estendida que influencia os arquivos de forma a proverem uma ou mais facilidades de busca em comum.

Enfim, a categoria de arquivos de recursos compartilhados compreende aqueles arquivos que estabelecem acordos com outros arquivos a fim de compartilhar recursos, provavelmente para a redução de custos. Entretanto, tais acordos não alteram a percepção do arquivo pela comunidade.

4.5.5 CONFORMIDADE

A implementação de arquivo é dita em conformidade com o Modelo de Referência OAIS quando esta suporta o modelo de informação e adota as responsabilidades mínimas especificadas no documento. Tais responsabilidades são: negociar e aceitar informação adequada de produtores de informação; manter o efetivo controle da informação para garantir a sua preservação por longo prazo; determinar, por si mesmo ou em conjunto com outros parceiros, que comunidades devam-se tornar comunidades-alvo e, portanto, devam ser capazes de entender a informação fornecida; garantir que a informação seja compreensível para a comunidade-alvo sem o auxílio dos produtores de informação; seguir políticas e procedimentos documentados, garantindo que a informação seja preservada contra todas as contingências cabíveis e possibilitando que a mesma seja disseminada como cópias autênticas do original ou rastreável até o original; e tornar a informação preservada disponível para a comunidade-alvo.

4.6 CONCLUSÃO

Ao longo deste capítulo viu-se que existem vários esforços, estudos, projetos e idéias a fim de elucidar a problemática da preservação de longo prazo de documentos eletrônicos. Ficou igualmente claro que ainda não há solução ótima, visto que as abordagens normalmente são

tomadas direcionadas aos objetos que serão arquivados, não se tendo um padrão definido e garantido que solucione a questão.

Na seção Conservação da Disponibilidade foi visto o tratamento básico que deve ser dado à preservação de um arquivo digital – o armazenamento da seqüência de bits (bistream). Os suportes desta, a mídia, mostraram-se as classes desses dispositivos e um breve levantamento sobre suas características. Apresentou-se também a técnica de renovação das mídias (refresh) que consiste em copiar os dados de uma mídia antiga para uma nova antes de aquela expirar sua validade, renovando assim o tempo de vida dos arquivos armazenados. Por último reforçou-se a importância, principalmente para uma estrutura de arquivamento, de manter cópias de segurança (backups) de todos os arquivos guardados.

Em Conservação da Interpretabilidade foram tratados os tópicos relevantes à manutenção desta característica, uma vez que os objetos digitais arquivados possivelmente serão visualizados no futuro. A primeira menção foi quanto à obsolescência de formatos, exibindo características e principais formatos de arquivos em seleção de formatos. Após, mostrou-se as estratégias utilizadas para se visualizar esses documentos no futuro, sendo as principais migração e emulação. A migração consiste em mover o conteúdo de um formato antigo para um novo com a finalidade de manter o arquivo interpretável em uma tecnologia atual. Já a emulação foca em imitar o ambiente (hardware e software) necessário para que o formato de arquivo seja interpretável na tecnologia atual. O último tópico ressalva a necessidade de manterem-se informações e históricos sobre cada arquivo, facilitando buscas e gerando evidências do tratamento dado ao arquivo ao longo do tempo.

Em Conservação da Eficácia Probante viram-se os procedimentos necessários para enfrentar a obsolescência dos algoritmos e parâmetros utilizados em resumos criptográficos, carimbos do tempo e assinaturas digitais. Também foi exposto os formatos CAdES e XAdES que, com suas variações, podem comportar todos os dados necessários para que se tenha a eficácia probante de um documento eletrônico – tornando-o autocontido. Mostraram-se as dificuldades de manter o valor probatório dos documentos, com o passar do tempo, sobre as tecnologias utilizadas. Outro problema encontrado com relação a este item é quanto à conversão de formatos: uma assinatura digital é dependente do conteúdo assinado e caso o mesmo seja mudado de formato, tem-se a invalidação da mesma.

Por último tratou-se do modelo de referência OAIS, um alicerce para a preservação de longo prazo, trazendo conceitos genéricos e papéis de cada entidade a fim de prover um arcabouço conceitual para a discussão e comparação de arquivos. Este modelo tem sido amplamente adotado por várias instituições arquivísticas, facilitando a compreensão das implementações e a

comparação das mesmas com as de outras instituições.

5 CENTRAL NOTARIAL DE SERVIÇOS ELETRÔNICOS COMPARTILHADOS

5.1 INTRODUÇÃO

As serventias extrajudiciais têm contribuído para a garantia da publicidade, autenticidade, segurança e eficácia dos atos jurídicos no Brasil. Até recentemente, o "papel" era o único meio material utilizado para o registro e certeza da integridade destes atos. Com o surgimento do computador, a popularização da Internet como meio de comunicação e mais recentemente a implantação de uma infra-estrutura de chaves públicas sólida e confiável no Brasil, tornou-se o documento eletrônico, com várias vantagens, meio alternativo ao papel para o registro dos atos jurídicos. A lei nº 11.419, de 19 de dezembro de 2006, que "Dispõe sobre a informatização do processo judicial; altera a Lei no 5.869, de 11 de janeiro de 1973 – Código de Processo Civil; e dá outras providências", foi uma das respostas ao desenvolvimento destas novidades tecnológicas. Entretanto, apesar das inúmeras iniciativas já realizadas por algumas das serventias, não há um modelo geral e independente, que respeite os preceitos legais e de autonomia das serventias, para modernização e integração dos serviços prestados pelas serventias extrajudiciais.

Um dos principais focos a ser tratado no projeto de modernização é a possibilidade da interoperabilidade, ou seja, o compartilhamento e troca de informações entre as serventias extrajudiciais. A interoperabilidade vai ajudar as serventias a prover, ao cidadão e ao Estado, maior facilidade de acesso e de novos e melhores serviços. Uma vez que a interoperabilidade é necessária não somente às serventias, mas a todos os serviços prestados pelo Estado ao cidadão, o Governo Federal desenvolveu a arquitetura Padrões de Interoperabilidade de Governo Eletrônico (e-PING). Esta arquitetura define um conjunto mínimo de premissas, políticas e especificações técnicas que regulamentam a utilização da Tecnologia de Informação e Comunicação (TIC) na interoperabilidade de Serviços de Governo Eletrônico, estabelecendo as condições de interação com os demais Poderes e esferas de governo e com a sociedade em geral. As áreas cobertas pela e-PING estão segmentadas em: interconexão, segurança, meios de acesso, organização e intercâmbio de informações e áreas de integração para governo eletrônico. Para cada um desses segmentos foram especificados componentes, para os quais são estabelecidos padrões. A ini-

ciativa do Governo Federal tem sido reconhecida e os padrões estabelecidos nesta arquitetura também serão adotados no desenvolvimento da CNSEC.

Como mencionado, o e-PING, no que tange aos aspectos tecnológicos, atende plenamente aos requisitos de interoperabilidade do projeto. Há, porém, uma outra vertente, a processual, que no caso dos serviços públicos delegados, deve ser observada para que o desenvolvimento alcance o sucesso esperado devido à sua assimetria normativa, o maior problema a ser resolvido. Nesta área o Conselho Nacional de Justiça (CNJ), pode em trabalho conjunto com as outras entidades envolvidas, corregedorias e serviço público delegado, trabalhar com o objetivo de padronizar a compreensão de todos sobre a utilização de tecnologia da informação e comunicação neste contexto.

Este capítulo procura inicialmente descrever o contexto no qual os serviços públicos delegados encontram-se inseridos, fundamentando a necessidade do esforço cooperado para a modernização dos serviços oferecidos. Essa cooperação deve alinhar-se nos aspectos tecnológicos à arquitetura e-PING, e, nos aspectos processuais, desenvolver trabalhos de pesquisa que permitam a padronização normativa e processual, lançando as bases do sucesso da Central Notarial de Serviços Eletrônicos Compartilhados (CNSEC).

É com base nessa contextualização que foram determinadas as premissas básicas que norteiam todo o processo de pesquisa, desenvolvimento e operação da CNSEC. Em momento anterior à sua apresentação, são discutidos o processo que levou ao levantamento das premissas e a configuração do modelo de desenvolvimento. O restante do capítulo apresenta sua arquitetura, descrevendo o modelo conceitual e também os principais módulos que a compõem.

5.2 UM OLHAR PARA O AMBIENTE COMPETITIVO

Em um contexto ambiental de mercados dinâmicos, onde a visão estratégica contempla a identificação das necessidades de mercado, a previsão de futuro, a definição de metas e a inovação, ocorrem impactos na estrutura organizacional e operacional de uma organização competitiva.

Como impactos de maior visibilidade estão a redução e horizontalização dos níveis hierárquicos, a formações de grupos interdisciplinares e a intensificação do uso da tecnologia da informação e comunicação (TIC). Os impactos maiores com relação a estrutura operacional estão na visão baseada em processos e atuação na competência essencial. Em um mercado dinâmico é difícil para uma organização se manter competitiva em todas as atividades de sua cadeia de valor. A estratégia competitiva para enfrentar o mercado dinâmico é baseada na co-

operação entre organizações.

As redes dinâmicas de empresas são formadas a partir de plataformas de empresas interdependentes que estão dispostas a compartilhar as competências essenciais em projetos temporários para aproveitar as oportunidades de mercado. Neste ambiente dinâmico a velocidade é um fator crítico de sucesso.

Evidentemente que a base multiempresarial das redes de empresas dificulta as relações de responsabilidade para com os clientes ou mesmo entre os seus integrantes. Isto se traduz na dualidade que precisa ser gerida pela necessidade de velocidade imposta pelo mercado versus a segurança jurídica que deve haver nas relações humanas – em específico as comerciais – para que sejam harmoniosas e duradouras.

Não há espaço neste novo ambiente competitivo para processos que não agregam valor. Agregar valor significa velocidade e custos adequados. Sem estes requisitos competitivos, os prestadores de serviços tendem a desaparecer através da obsolescência. Mesmo para aqueles negócios que são protegidos por barreiras de entrada criadas pela legislação, existe o risco de que a competitividade seja ameaçada pela inovação.

Para os serviços públicos delegados – também conhecidos como serventias extrajudiciais ou cartórios – a intensificação do uso do documento eletrônico e a institucionalização de seu uso no Brasil através da MP 2.200-2 atestam este risco. Mas o que a principio foi visto por muitos como uma ameaça, é na verdade uma oportunidade não aproveitada por aqueles que já tinham o amparo legal para fazê-lo, ou seja, o setor Notarial.

As inovações tecnológicas associadas ao documento eletrônico, tal como a possibilidade de se produzir assinatura, já haviam sido propostas desde o final da década de 1970, mas somente agora, 25 anos após sua concepção têm sido alvo de discussões por parte do setor Notarial. Inúmeras outras tecnologias surgiram e estão sendo propostas, praticamente ignoradas, poderiam estar no foco das preocupações das serventias extrajudiciais. Estas inovações são produtos de pesquisa científica e tecnológica, realizadas por centros de pesquisa e universidades. É estratégica às serventias uma cooperação cercana a estes grupos. As serventias poderão se beneficiar fortemente dos resultados das pesquisas, recuperar o tempo perdido, e estar sempre à frente de qualquer outra iniciativa de modernização do Estado brasileiro.

A figura 8 ilustra o relacionamento entre as entidades que deverão cooperar neste projeto de modernização.

Um projeto de modernização e integração dos serviços de serventias extrajudiciais por especialidade deve estruturar a transformação para aproveitar estas oportunidades.

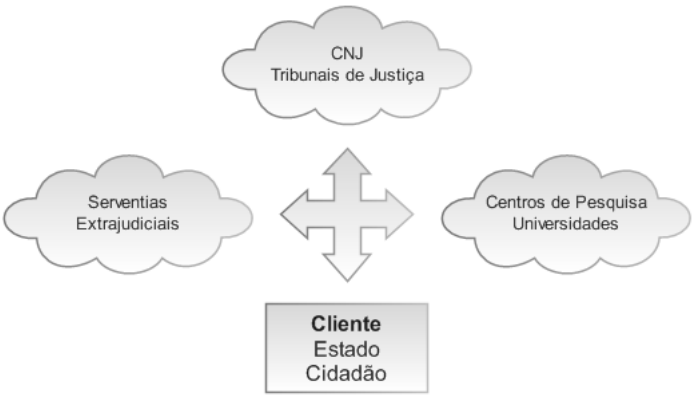

Figura 8: Participantes.

5.3 CONFIGURAÇÃO CONCEITUAL DO MODELO DE DESENVOLVIMENTO DA CNSEC

O desenvolvimento integral da Central Notarial de Serviços Eletrônicos Compartilhados passa por várias etapas bem definidas, com a aplicação de ferramentas e metodologias específicas, para que o resultado apresente eficiência, eficácia e demais qualidades desejadas. É fundamental que os envolvidos nesta atividade apresentem aprofundado conhecimento dos processos de negócio das organizações, bem como das normas, padrões e melhores práticas de desenvolvimento e gestão de serviços de tecnologia da informação e comunicação.

A criação de relacionamentos entre as organizações que utilizem de forma efetiva as competências de cada um dos envolvidos, uma cooperação por competências, é o modelo considerado mais adequado para o desenvolvimento da CNSEC – dada sua necessidade de evolução constante.

No presente contexto, a universidade é um instrumento de inovação e desenvolvimento das competências requeridas no desenvolvimento contínuo da CNSEC. Os serviços públicos delegados reúnem o conhecimento sobre a legislação, processos e a forma de operacionalizar um serviço complexo com vários relacionamentos. O Conselho Nacional de Justiça deve atuar junto às corregedorias estaduais e serviços públicos delegados, facilitando o desenvolvimento de soluções de tecnologia da informação e comunicação através da redução da assimetria normativa. A implementação de toda a infra-estrutura física e dos aplicativos destinados a operacionalização da CNSEC é realizada através de uma rede de organizações que apresenta comprovado conhecimento em técnicas, ferramentas e procedimentos essenciais a atividade.

Uma atividade básica em desenvolvimento é a contextualização do ambiente atual no qual estão inseridas as organizações cooperadas. A partir desta atividade foram estruturadas as pre-

missas básicas, apresentadas na próxima seção, que norteiam o desenvolvimento da CNSEC.

Outra tarefa inicial refere-se ao estudo e mapeamento dos processos de negócio das serventias e das interações com seus clientes. Nesta atividade utiliza-se a notação Business Process Modeling Notation (BPMN), que apresenta um padrão para modelagem de processos de negócio. Esta metodologia foi selecionada por ter suporte nas ferramentas de mercado, ser uma notação de fácil compreensão – facilitando a comunicação entre os atores envolvidos (pesquisadores, serventias e desenvolvedores) e pela capacidade de modelagem de processos complexos – sendo possível atingir um nível bastante refinado do comportamento do processo agregando informações que futuramente facilitarão o desenvolvimento e manutenção de sistemas para a execução destes processos. Ao realizar o mapeamento dos processos, busca-se determinar um modelo de organização do ponto de vista dos seus processos de negócio. Além da documentação, padronização e possível melhoria dos processos, obtém-se também um conjunto desejável de requisitos funcionais e não funcionais dos sistemas a serem utilizados na automação dos processos.

Estas duas etapas iniciais, definição dos princípios básicos da CNSEC e levantamento dos processos e seus requisitos, são fundamentais para o sucesso da iniciativa. Deve-se nesse momento notar que o reconhecimento dos atores, mecanismos e processos existentes não têm como objetivo uma simples automatização de uma série de atividades desenvolvidas nesse contexto. Como enfatizado por Sergio Lozinsky, líder de Estratégia Corporativa da IBM Global Business Services, a abordagem de Centro de Serviços Compartilhados vai além:

> Os chamados Shared Services Center (Centros de Serviços Compartilhados – CSCs) acabaram por estabelecer-se como uma solução comprovada de aumento da eficiência operacional com redução dos custos. A idéia é descobrir as atividades que se repetem em várias partes da organização (em geral de maneira não uniforme ou padronizada) e reuni-las em um único local (o "centro") onde passarão a utilizar processos e tecnologias mais sofisticadas ou eficazes, e ganharão economias de escala.

Esta unificação de esforços dá-se ainda com a adoção de sistemas que permitam interoperabilidade e utilizem padrões abertos alinhados à arquitetura e-PING. Esta abordagem permite a centralização e implantação racional de aplicações genéricas, ao mesmo tempo em que fornece autonomia às serventias para a execução dos serviços e guarda dos dados.

Os processos, quando analisados a partir dessa perspectiva, não serão tratados de forma isolada e sim de forma conjunta, alinhados com os objetivos das serventias – que por sua vez estarão alinhados com as necessidades do Estado e dos cidadãos.

Os modelos de gestão de serviços de tecnologia da informação e comunicação permitirão à

CNSEC desenvolver indicadores/métricas e ferramentas gerenciais aos seus gestores e usuários que possibilitem a identificação de fragilidades e potencialidades. A constante monitorização destes indicadores permitirá aos gestores efetuar o controle dos riscos envolvidos, mantendo-a funcional em níveis de qualidade adequados, realizando as melhorias quando for necessário. A redução dos prazos envolvidos e o aumento da confiabilidade na prestação destes serviços tendem a fazer com que os usuários os utilizem em escala crescente.

5.4 PRINCÍPIOS DA CNSEC

A Central Notarial de Serviços Eletrônicos Compartilhados é fundamentada em princípios básicos. Os princípios foram determinados pelos pesquisadores, por meio do estudo dos requisitos de cada um dos atores envolvidos, com o objetivo de potencializar a cooperação dos interessados na modernização dos serviços prestados pelas serventias extrajudiciais.

Os princípios que norteiam o desenvolvimento da CNSEC são apresentados na tabela 1:

5.5 ELEMENTOS DA CNSEC

A modernização e integração das serventias extrajudiciais representam um conjunto de desafios constituídos pela complexidade dos sistemas, especificidades regionais de cada especialidade, necessidade permanente de investimentos em infra-estrutura, capacitação e modernização tecnológica. A superação destes desafios depende em primeiro lugar de capacidade de gestão, ou seja, de como a classe vai se organizar para atuar cooperadamente em seu esforço de modernização.

Assim, a CNSEC possui e desenvolve um modelo de gestão composto por quatro elementos básicos: os associados, o gestor, o Conselho Nacional de Justiça (CNJ) e as cooperações, conforme ilustra a figura 9. Elementos básicos

Os Associados atuam independentemente, mas estão reunidos em uma plataforma representada pelos mecanismos de integração, identidade comum e objetivos de modernização. Para participar desta plataforma precisam desenvolver requisitos de virtualização de processos. A integração das serventias extrajudiciais à CNSEC é mais ou menos automatizada conforme seu grau de virtualização. Cada serventia integra-se ao modelo conforme as suas necessidade e capacidade de investimento, com base em um plano de integração que a levará da situação atual àquela almejada com a busca da plenitude de modernização. Uma vez definido o plano de integração, seu desenvolvimento pode ser acelerado via mecanismos de financiamento.

Princípio	Descrição
Autonomia administrativa	Onde são respeitadas as particularidades de cada entidade. A independência entre os institutos membros é observada nesta premissa. Cada serventia deve ter autonomia na seleção da forma de utilização do sistema proposto. Os dados gerados pelas serventias são de sua propriedade e ficam sob sua responsabilidade.
Autonomia tecnológica	Onde cada entidade tem autonomia na seleção de ferramentas e aplicativos utilizados, respeitando a adoção de padrões e protocolos abertos. A seleção de soluções tecnológicas como forma de armazenamento e utilização dos dados é atribuição das serventias, respeitando a sua autonomia administrativa e os padrões pré-definidos.
Identidade compartilhada	De forma que especialidade represente, com sua marca, os princípios da cooperação, evitando iniciativas isoladas internas oferecidas pelas serventias e as externas oferecidas por outros prestadores de serviços.
Simetria normativa	Busca diminuir a assimetria gerada por diferentes interpretações das Corregedorias Estaduais sobre a utilização da Tecnologia da Informação e Comunicação nos serviços públicos delegados.
Gestão cooperada	Utilização de mecanismos de gestão que possibilitem a operação em rede de organizações centradas em sua competência central, otimizando a aplicação de recursos através da cooperação, dos consórcios e do compartilhamento de infra-estrutura.
Confiança	Constituída com base em pré-acordos e modelo jurídico que viabilizem a ação rápida e cooperada do esforço de modernização.
Domínio tecnológico	Através da promoção do desenvolvimento de tecnologia própria de forma que seja possível minimizar a dependência dos fornecedores de tecnologia sobre os processos de negócios das serventias.
Segurança dos dados	Deve-se primar pela manutenção da integridade, não-repúdio, disponibilidade e tolerância à falha dos dados de responsabilidade das serventias. O serviço deve apresentar alta disponibilidade, não sendo possíveis atividades que possam levar à ocorrência de fraudes.
Integridade em longo prazo	É uma premissa particularmente importante, uma vez que as serventias se responsabilizam pela guarda de grande número de documentos, que afetam toda a sociedade. As serventias devem se preocupar com a manutenção desta importante propriedade ao longo dos anos.
Gerência de documentos eletrônicos	Permitir às serventias a digitalização, armazenamento e indexação dos documentos. Todo o ciclo de vida dos documentos será controlado por sistema de gerência de documentos eletrônicos, facilitando o uso por parte das serventias.
Interoperabilidade	Interoperabilidade na qual deve-se garantir a comunicação entre as aplicações e serventias de forma transparente, utilizando padrões e protocolos abertos. A aderência a arquitetura e-PING é um requisito.
Respeito a especialização	Onde as soluções devem respeitar as características próprias de cada especialização.
Respeito ao legado	Respeito aos sistemas legados onde os sistemas existentes serão aproveitados sempre que haja interesse da entidade.
Flexibilidade	Na qual o sistema possa ser reconfigurado para se adaptar às mudanças nas regulamentações e à implementação de novos serviços.

Tabela 1: Princípios Norteadores.

O Gestor – sendo o Colégio Notarial do Brasil (CNB) um candidato, por representar a especialidade dos notários – é o representante legítimo dos participantes da plataforma que possui a responsabilidade de gerenciar o esforço de modernização e a manutenção dos serviços compartilhados. A legitimidade é baseada principalmente em capacidade de gestão da cooperação, que

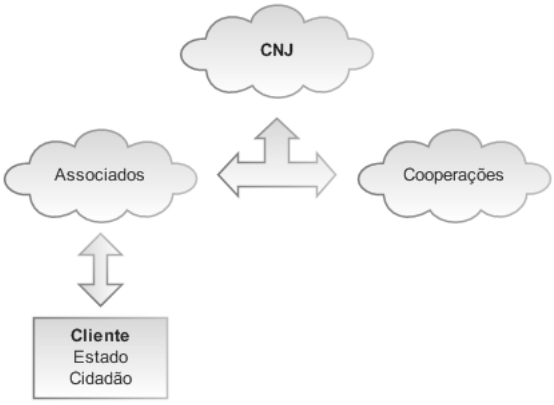

Figura 9: Elementos básicos.

envolve a criação e manutenção da plataforma e a formação de cooperação com a comunidade de especialistas externos, corregedorias estaduais e com o Conselho Nacional de Justiça para o rápido desenvolvimento de serviços modernos e ajustados à realidade atual.

O Conselho Nacional de Justiça atua em sintonia com o gestor do esforço de modernização e com as corregedorias estaduais para reduzir as assimetrias normativas, possibilitando o trabalho do gestor e uma maior padronização dos processos de negócio.

As cooperações são a essência do modelo. Os desafios da modernização contrastados com a velocidade em que são necessárias, obrigam o gestor a buscar competências externas, principalmente no que se refere a infra-estrutura e tecnologias. A CNSEC disponibiliza um conjunto de serviços que envolvem infra-estrutura, pessoal, sistemas, conhecimento e outros insumos não encontrados em sua totalidade no ambiente interno da cooperação. Assim sendo, é estratégico desenvolver alianças com redes de especialistas externos que dominam elementos e competências essenciais a serem agregadas ao negócio das serventias para que estas se modernizem e ofereçam uma gama de serviços que extrapole o atual portfólio, agregando novos serviços, aproximando a oferta do desejo da demanda.

O desenvolvimento de qualquer aplicativo ou serviço a ser utilizado pela CNSEC deve utilizar tecnologias existentes e comprovadamente estáveis. O estabelecimento de uma rede de organizações fortalece a iniciativa, em que cada uma das organizações apresenta uma competência específica. A complementaridade destas competências deve ser utilizada para o desenvolvimento de tecnologias de uso comum.

5.6 CENTRAL NOTARIAL DE SERVIÇOS ELETRÔNICOS COMPARTILHADOS

5.6.1 VISÃO GERAL

Nesta seção é descrita a arquitetura da Central Notarial de Serviços Eletrônicos Compartilhados (CNSEC). O modelo apresentado a seguir foi engendrado seguindo as premissas apresentadas na seção Princípios da Central Notarial de Serviços Eletrônicos Compartilhados. O projeto descrito neste capítulo e a arquitetura apresentada foram concebidos de forma que possam facilmente se adaptar a eventuais mudanças nos princípios norteadores, estes sujeitos às políticas estabelecidas pelo CNB, serventias extrajudiciais ou CNJ.

O conceito de arquitetura desenvolvido leva em consideração a existência de diferentes tipos de serventias e que estas apresentam diferentes contextos sociais e econômicos. Essa heterogeneidade também se reflete numa disparidade tecnológica entre elas; muitas serventias já possuem sistemas informatizados de gestão da serventia, e algumas inclusive, soluções de prestação de serviço on-line. É necessário, portanto, que a arquitetura permita a integração destes sistemas. A CNSEC o faz através de portas de integração, conectadas ao Canal de Integração – cada porta especifica a forma pela qual a serventia associada se vincula à estrutura.

No sentido de permitir a interoperabilidade com esses sistemas mantidos pelas serventias, a CNSEC foi projetada para suportar a comunicação entre aplicações através da troca de mensagens XML bem definidas – como preconizado pela tecnologia Web Services. Assim, esses sistemas ficam aptos a receber ou responder a requisições advindas da CNSEC, ou usar serviços genéricos por ela disponibilizados, como, por exemplo, a Autoridade de Carimbo do Tempo.

Para aquelas serventias que não possuem sistemas de gestão informatizados, ou que pretendem desenvolvê-los no futuro, mas desejam integração imediata à CNSEC, é disponibilizado o Cartório Digital, dentro do modelo de distribuição Software como um Serviço. Neste modelo, o sistema de gestão é mantido junto à CNSEC, que se responsabiliza pela sua manutenção, respeitando os princípios de independência preconizados anteriormente. Para acessá-lo, a serventia necessita apenas de um computador com um navegador Web, mantendo os gastos com recursos de Tecnologia da Informação (TI) num patamar mínimo.

A flexibilidade almejada, dentro dos princípios de autonomia administrativa e tecnológica, é adicionalmente complementada através da abstração, pela arquitetura, da localização física dos dados, suportando que os mesmos, opcionalmente, possam estar armazenados junto a um Centro de Armazenamento de Dados do CNB ou de suas seccionais. Do mesmo modo, é necessário levar em consideração: a) a necessidade da estrutura atual continuar em funcionamento, mesmo

durante o processo de transição dessa para uma outra situação em que os documentos eletrônicos sejam utilizados em larga escala; e b) sabe-se das vantagens do documento eletrônico em relação ao documento papel, mas já é consenso que são vários os casos práticos onde se faz necessária a manutenção do documento papel – nestes casos, o documento eletrônico não substitui o papel. Com esse intento, a arquitetura proposta prevê, também, o uso de documento papel.

O modelo visa, igualmente, proporcionar aos cartórios uma integração gradual, oferecendo a eles meios de se vincularem à CNSEC de forma progressiva, conforme percebam resultados ou adquiram confiança. Um cartório pode, por exemplo, ingressar no sistema apenas o utilizando como forma de atingir a uma gama maior de interessados em seus serviços, uma vez que estes seriam expostos pela CNSEC e, por ela, novas requisições chegariam. Posteriormente, a serventia poderia optar, por exemplo, por automatizar certos serviços, dando a ela condições de se concentrar naqueles de maior valor agregado. Essas modificações podem ser efetuadas junto à Gestão de Integração.

A adoção de uma Arquitetura Orientada a Serviços, visa do mesmo modo, facilitar a adaptação da CNSEC, favorecendo a criação de novos serviços, e habilitando as serventias a responderem de forma mais rápida e econômica às mudanças inerentes aos serviços cartoriais. Pedidos de ajuste na estrutura podem ser encaminhados através da Central de Comunicação e Suporte, que oferece um canal de comunicação com a administração da CNSEC.

Ainda no sentido de comunicação com as serventias, a CNSEC oferece a Central de Capacitação, que busca, diante das longas distâncias geográficas encontradas no país, tratar o aprimoramento técnico dos notários e da reciclagem de prepostos e profissionais que atuam na área, por meio de educação a distância.

Sendo premissa básica a oferta dos serviços e informações cartoriais de forma conveniente e segura aos interessados, o modelo possibilita acesso personalizado aos serviços, acomodando os diferentes perfis dos usuários em portas de serviço, conectadas ao Canal de Serviço. Tais portas identificam por quem e de que forma um dado serviço pode ser acessado. Desse modo, um serviço pode, por exemplo, ser utilizado pelos cidadãos por meio da página Web (Portal de Serviços e Informações) ou de aplicativos do Poder Judiciário – através da troca de mensagens XML. É interessante notar que essa possibilidade de comunicação entre aplicativos, alcançada pela troca de mensagens XML, impulsiona a automatização de tarefas por aqueles cujos serviços das serventias são importantes na cadeia de valor de seus negócios.

O projeto da CNSEC visa a interoperabilidade, sendo aderente aos padrões e-PING, e tem por princípio permitir a integração e oferta de serviços de forma segura, garantindo segurança

fim-a-fim, nas trocas de mensagens, e ponto-a-ponto, nos acessos diretos. Além disso, os dados das serventias, quando sob responsabilidade da CNSEC, são selados e acessíveis apenas por aqueles autorizados pelas serventias.

Por fim, com o intuito de garantir estabilidade e credibilidade ao sistema e facilitar seu acompanhamento, o mesmo possui facilidades que permitem o monitoramento, auditoria e contabilidade de suas atividades.

A figura 10 ilustra a visão geral descrita.

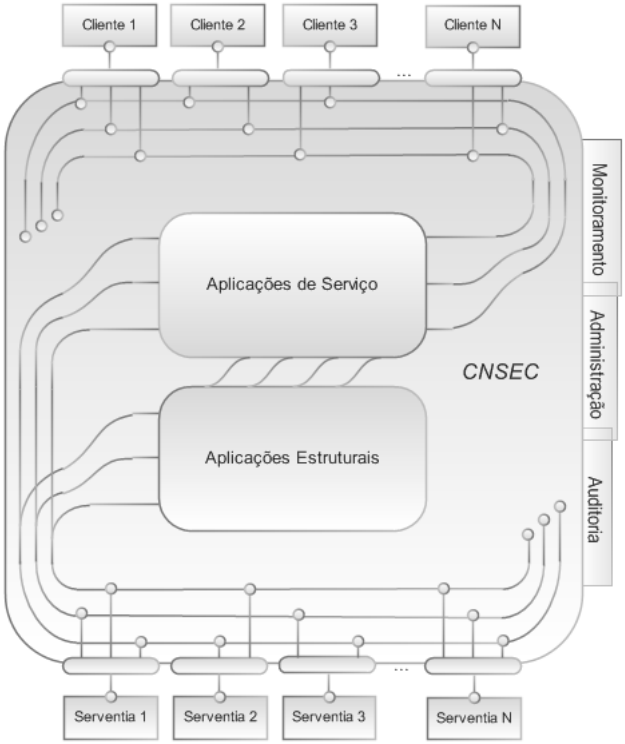

Figura 10: Visão Geral da CNSEC.

5.7 COMPONENTES

5.7.1 CANAIS E PORTAS

Os canais e portas buscam atender, essencialmente, aos princípios de interoperabilidade, respeito aos sistemas legados, flexibilidade e autonomia tecnológica e administrativa.

Todo o acesso ou prestação de serviços é dado por meio de portas que especificam, por completo, como é feita a comunicação entre as partes e a CNSEC. A extensibilidade da estrutura é dada pela capacidade de adição de novas portas aos canais, permitindo, assim, a vinculação de novos participantes à central.

A comunicação efetuada por meio dos canais dá-se de forma segura, e a autenticação das partes é, em geral, realizada com base em certificados digitais emitidos por autoridades certificadoras credenciadas à Infra-estrutura de Chaves Públicas Brasileira (ICP-Brasil). Toda informação que circula pelos canais é protegida contra a leitura ou alteração por terceiros, graças a mecanismos de garantia de confidenciabilidade e integridade providos por aqueles. Mensagens trocadas pelas partes possuem, do mesmo modo, eficácia jurídica – propriedade fornecida pelos certificados ICP-Brasil, conforme preconiza a legislação vigente. Por último, a fim de garantir a interoperabilidade, a comunicação é realizada de forma aderente aos padrões e-PING.

Neste contexto, os canais apresentam-se como uma solução extensível, que garante todas as funcionalidades de segurança e controle inerentes a um Centro de Serviços Compartilhados, protegendo toda a estrutura contra o uso não autorizado ou que viole as políticas estabelecidas pelo arcabouço jurídico vigente e pelo gestor da Central.

Dependendo das partes envolvidas na comunicação, os canais dividem-se em Canal de Serviços e Canal de Integração.

5.7.1.1 CANAL DE SERVIÇOS

Ao Canal de Serviços conectam-se aqueles que buscam algum serviço oferecido por um ou mais integrantes da CNSEC conforme ilustra a figura 11. As diferentes necessidades e possibilidades desses clientes são acomodadas em suas respectivas portas de serviço. A estas portas estão associadas todas as requisições que um dado cliente pode efetuar, e de que forma essas requisições serão feitas – seja através de mensagens XML oriundas de aplicativos diversos, ou por páginas Web.

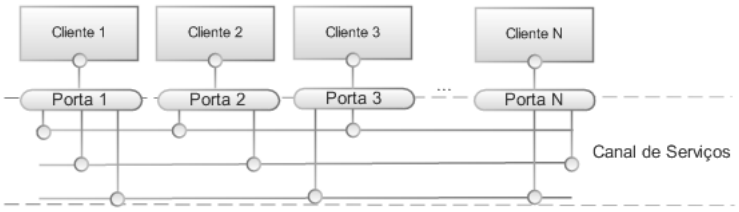

Figura 11: Clientes acessando o Canal de Serviços através de suas respectivas portas de serviço.

5.7.1.2 CANAL DE INTEGRAÇÃO

Ao Canal de Integração conectam-se aqueles que proverão serviços por meio da CNSEC conforme ilustra a figura 12. As diferentes necessidades e possibilidades desses provedores

de serviços são acomodadas em suas respectivas portas de integração. O prestador de serviço define para cada uma das portas os serviços que responderá e de que forma. A CNSEC disponibiliza uma gama de opções para que o prestador de serviço se integre do modo que lhe for mais conveniente. Essas opções ainda variam conforme o perfil do provedor. No caso de serventias ingressantes, podemos citar:

- a forma como as requisições aos serviços serão encaminhadas, seja através do Cartório Digital, por meio de mensagens XML dirigidas à uma aplicação local, ou respondidas de forma automática por meio de algum provedor de aplicações de serviço;
- como os dados serão armazenados, seja em papel, ou em bancos de dados. E caso sejam em bancos de dados, quais deseja utilizar;
- o modo como os serviços deverão ser ofertados pela CNSEC, mais precisamente, através de quais portas de serviço.

Além das serventias, podem vincular-se prestadores de serviços que são auxiliares a elas, como, por exemplo, fornecedores, ou integrantes da CNSEC que desejem oferecer alguma infraestrutura de TI, tais como bancos de dados. Nesses casos são oferecidas a eles as devidas opções de integração.

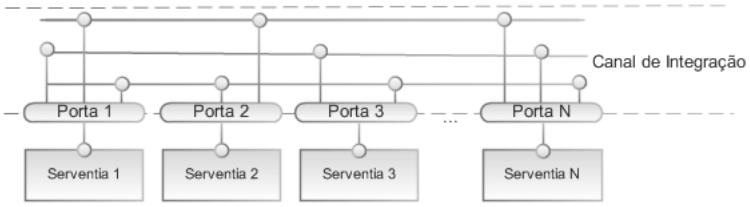

Figura 12: Serventias acessando o Canal de Integração através de suas respectivas portas de integração.

5.7.2 GESTÃO DE INTEGRAÇÃO

As serventias extrajudiciais vivenciam diferentes contextos sociais e econômicos, e esses são fatores determinantes na integração das mesmas à Central Notarial de Serviços Eletrônicos Compartilhados. Ainda nesse contexto, é princípio do projeto oferecer às serventias autonomia tecnológica e administrativa e cabe, portanto, à CNSEC acomodar tais decisões.

Essas decisões podem ser efetuadas junto à Gestão de Integração por meio de uma página Web, e visam oferecer às serventias os meios necessários para que essas possam oferecer seus

serviços da forma que lhes for mais conveniente. Algumas dessas configurações podem ser feitas serviço-a-serviço, possibilitando à serventia dar maior atenção àquelas tarefas que lhe são críticas, ou cujos dados lhe são mais relevantes. É, então, com base nessas especificações que uma porta de integração é criada ou adaptada. Dentre essas opções estão:

5.7.2.1 SERVIÇOS PRESTADOS

A serventia especifica, com base na sua especialidade e nas suas possibilidades, quais serviços deseja oferecer por meio da CNSEC, como por exemplo, consultas à escrituras e procurações ou emissão de certidões.

Para cada um desses serviços é fornecida a opção de definir a forma de atendimento as requisições, a forma de armazenamento dos dados, e por quais portas de serviço deseja oferecê-los.

5.7.2.2 FORMA DE ATENDIMENTO AS REQUISIÇÕES

Cartório Digital As requisições desse serviço, endereçadas à serventia, são por ela recebidas ao acessar a página Web Cartório Digital. Essa página oferece às serventias as funcionalidades necessárias para o acompanhamento e resposta de pedidos recebidos.

Sistema local de gestão da serventia Os pedidos a esse serviço são encaminhados ao sistema local de gestão da serventia, por meio de mensagens XML. Quando preciso, a resposta aos mesmos se dará por mensagens XML originadas por esses sistemas. Esse conjunto de mensagens deve ser previamente padronizado.

Automatizada Caso deseje, a serventia pode automatizar um serviço ou parte dele, dependendo do nível de dependência desse serviço em relação ao tabelião, e da acessibilidade dos dados necessários para a execução do mesmo. A implementação dessa lógica de serviço, chamada de aplicação de serviço no contexto da CNSEC, é dada por algum provedor de aplicações de serviço. Essas aplicações de serviço possuem uma interface bem definida, provida por um conjunto de mensagens XML de requisições e respostas. Portanto, a serventia pode apontar para qualquer provedor que suporte esse conjunto de mensagens – seja ele um sistema da própria serventia, ou a implementação fornecida pela CNSEC por meio do Provedor de Aplicações de Serviço.

5.7.2.3 FORMA DE ARMAZENAMENTO DOS DADOS

Os dados relativos aos serviços dos cartórios estarão sob responsabilidade dos mesmos e serão acessíveis somente por eles. Sob o domínio da CNSEC estarão apenas os índices dessas informações – mas não a informação em si. Por exemplo, no caso de testamentos, se a serventia armazenar tais dados da forma tradicional – em documento papel – a CNSEC seria alimentada com informações como o nome completo do testador, números de CPF e RG, espécie e data do ato, livro e folhas em que foi lavrado. Caso a forma de armazenamento em questão seja bancos de dados, informações análogas seriam utilizadas.

A única exceção à regra ocorre quando a serventia, por algum motivo, delega à CNSEC a execução de algum serviço. Nesse caso, a serventia autoriza a CNSEC a acessar os dados relativos ao mesmo.

As formas de armazenamento dos dados são as seguintes:

Tradicional Os dados do serviço serão armazenados na forma tradicional – documento papel. Assim sendo, quando esses precisam servir de resposta em meio eletrônico, sua digitalização e posterior aposição da assinatura digital, tornam-se necessárias.

Banco de Dados As informações são armazenadas em um ou mais bancos de dados. À serventia é dada a opção de apontar qual quer utilizar – seja ele pertencente a um Centro de Armazenamento de Dados do CNB ou da própria serventia, ou mesmo de outros participantes da CNSEC que disponibilizem sua infra-estrutura. A escolha de um conjunto de bancos de dados, conforme ilustra a figura 13, oferece maior segurança, uma vez que os dados são replicados, garantindo tolerância a falhas. É importante notar que estes dados, independentemente de estarem em bancos de dados de terceiros, são acessíveis apenas pela serventia que os possui ou por membros por ela autorizados, uma vez que estão devidamente protegidos.

5.7.2.4 PORTAS DE SERVIÇO

As portas de serviço do Canal de Serviços acomodam as diferentes necessidades de acesso dos usuários dos serviços. Definir que um serviço será ofertado por uma dada porta, implica em estabelecer como o serviço será acessado, e por quem. Como exemplos podemos citar aplicativos do Poder Judiciário interessados no serviço comunicando-se por mensagens XML, ou pessoas físicas acessando o Portal de Serviços e Informações.

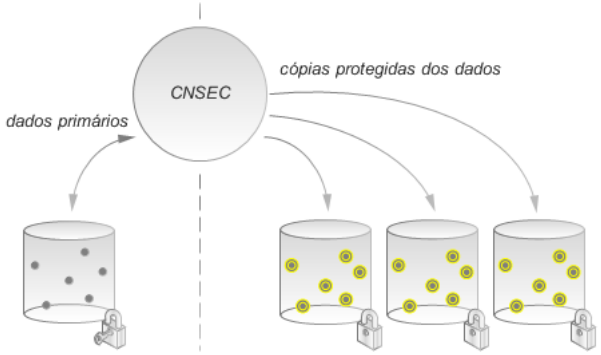

Figura 13: Dados protegidos sendo replicados e distribuídos em diferentes bancos de dados.

É importante notar que estas opções de integração possuem interações entre si, o que significa que a escolha de certas opções pode levar à obrigação ou restrição de outras. Tais interações, no entanto, são devidamente tratadas pelo sistema – de forma transparente, no momento da escolha das opções pela serventia.

Ainda sobre essas escolhas, vale salientar que as mesmas podem ser modificadas posteriormente. A serventia pode passar a oferecer novos serviços, ou deixar de oferecer outros, ou mesmo modificar a forma como são oferecidos. Isto permite aos cartórios uma integração progressiva ao sistema.

A integração, entretanto, não se restringe aos cartórios – podem vincular-se, igualmente, prestadores de serviços auxiliares a elas, como fornecedores ou ingressantes da CNSEC que desejem oferecer alguma infra-estrutura de TI, tais como bancos de dados. Nesses casos são oferecidas a eles as devidas opções de integração.

Uma vez terminadas essas configurações, a infra-estrutura necessária para suportá-las é gerada ou adaptada – idealmente de forma automática, porém dependendo da configuração, pode ser necessária alguma intervenção de pessoal técnico.

5.7.3 APLICAÇÕES DE SERVIÇOS

As Aplicações de Serviço destinam-se ao atendimento de requisições realizadas pelos usuários finais. Neste contexto, o usuário final pode ser a Justiça, o Poder Público, Instituições Bancárias ou até mesmo o cidadão comum.

Essas aplicações são responsáveis por toda a lógica necessária para o atendimento, ou redirecionamento das requisições de serviço. Essa lógica pode envolver a distribuição de requisições para um ou mais cartórios, ou mesmo todo o procedimento necessário para a execução

de um serviço, ou parte dele – no caso de delegação de serviços à CNSEC.

A implementação dessas aplicações ocorre por meio de algum Provedor de Aplicações de Serviço. A CNSEC oferece, por padrão, o seu próprio provedor. Entrentanto, graças ao fato de as mensagens que invocam esses serviços serem formalmente especificadas – interfaces bem definidas – outros provedores podem ser desenvolvidos.

Alguns exemplos de Aplicações de Serviço são a consulta de escrituras, procurações, testamentos e a emissão de certidões.

O acesso a elas se dá por meio de portas de serviço, em geral facilitado pelo uso de Aplicações de Acesso.

5.7.4 PROVEDOR DE APLICAÇÕES DE SERVIÇO

Alguns serviços ou partes deles podem ser automatizados. Essa automatização é influenciada por fatores como o nível de dependência do serviço em relação ao tabelião, e da acessibilidade dos dados necessários para a execução dos mesmos. Dentre esses serviços, podemos citar consultas a escrituras e procurações ou emissão de certidões. A implementação dessa lógica de negócio, chamada de aplicação de serviço no contexto da CNSEC, é dada por algum provedor de aplicações de serviço. Essas aplicações de serviço possuem uma interface bem definida, provida por um conjunto de mensagens XML de requisições e respostas. Portanto, a serventia pode apontar para qualquer provedor que suporte esse conjunto de mensagens.

Nesse sentido, a CNSEC oferece a sua própria implementação – o Provedor de Aplicações de Serviço. As aplicações de serviços por ele fornecidas são criadas com base no estudo dos serviços prestados pelas serventias, e a criação de novas aplicações pode ser proposta pelos cartórios. Essas também podem ser formadas por composições de outras aplicações, permitindo, por exemplo, a distribuição de requisições a todos os cartórios de uma dada localidade.

É interessante notar que as aplicações de serviços fornecidas por esse provedor são beneficiadas por executarem sobre uma plataforma idealmente segura – a CNSEC.

5.7.5 APLICAÇÕES DE ACESSO

As Aplicações de Acesso são aplicações, em geral criadas sob demanda, que visam facilitar o acesso às aplicações estruturais ou de serviços. São oferecidas por meio de portas de serviço ou de integração, e a autenticação dos usuários geralmente ocorre por meio de certificados digitais ICP-Brasil.

A princípio são oferecidas duas Aplicações de Acesso: Portal de Serviços e Informações, para o acesso por parte dos clientes, e Cartório Digital, para acesso por parte das serventias.

5.7.5.1 PORTAL DE SERVIÇOS E INFORMAÇÕES

A CNSEC deve atender um número crescente de clientes que possuem basicamente navegadores como ferramentas para acesso às aplicações. O atendimento a este tipo de usuário será realizado por meio do Portal de Serviços e Informações, que é um endereço na Web, concebido para disponibilizar ao cidadão, governo ou entidades públicas e privadas o conjunto de serviços apropriados ao seu perfil.

O Portal de Serviços e Informações é um mecanismo que permite ao usuário o acesso às aplicações de serviço através de uma interface na Internet, não sendo necessário o uso de aplicativos dedicados. Toda a conexão entre o usuário e as aplicações é implementada pelo Portal de Serviços e Informações de forma transparente para o usuário.

O fornecimento de informações é uma atribuição complementar do Portal de Serviços e Informações. É através desta funcionalidade que os usuários têm acesso às informações e a forma de utilização dos serviços disponibilizados. Qualquer dúvida que o usuário vier a apresentar sobre a CNSEC deve ser encaminhada por meio do Portal de Serviços e Informações que se encarregará de obter uma resposta e enviá-la ao solicitante.

5.7.5.2 CARTÓRIO DIGITAL

O Cartório Digital é um sistema Web de gestão de cartórios extrajudiciais para aqueles que optarem por utilizar um serviço na modalidade Software as a Service (SaaS). É acessível por uma página Web (através de um navegador), cujo design ergonômico visa oferecer ao cartorário mais produtividade no exercício de sua função. Idealmente, deve oferecer, quando possível, abstrações dos processos aos quais o mesmo está acostumado.

O modelo SaaS tem sido amplamente utilizado nos casos em que as empresas não têm como objetivo o desenvolvimento e manutenção de sistemas. No contexto das serventias, os recursos computacionais são subutilizados e requerem a contratação de equipe técnica de suporte e desenvolvimento, acentuando os custos envolvidos. Para minimizar os recursos necessários, uma parte da estrutura é mantida em um provedor institucional que pode prover toda a infra-estrutura necessária, gerando economia a todas as entidades usuárias do serviço.

No modelo SaaS o sistema é desenvolvido e fica localizado junto à Central Notarial de Serviços Compartilhados e a serventia faz uso deste remotamente, minimizando o uso de sis-

temas locais. A prestação de serviços pelas serventias envolve basicamente o recebimento de requisições vindas de interessados em seus serviços, seu devido tratamento, e resposta, se necessário. No contexto de documentos eletrônicos, ainda podemos incluir a lida com tais documentos, e o uso de ferramentas sobre esses documentos a fim de conferir-lhes eficácia jurídica. O exercício de sua função também pode envolver a requisição de serviços a outros cartórios, órgãos, etc. O Cartório Digital objetiva oferecer um meio para a gestão das serventias, provendo soluções para os itens acima citados.

Deve-se viabilizar o atendimento de requisições de serviço recebidas, tanto através da Central Notarial de Serviços Eletrônicos Compartilhados, quanto no próprio espaço físico da serventia. Para essas requisições, deve ser possível acompanhar o andamento dos processos necessários ao seu devido tratamento – como, por exemplo, requisições feitas pela serventia a outros integrantes da CNSEC.

O objetivo deste modelo, no presente contexto, é permitir à serventia que se concentre na prestação dos serviços existentes bem como no desenvolvimento de novos serviços requisitados pelos usuários. A manutenção de sistemas de informação e a prestação de suporte não são essenciais aos seus processos e podem ter seu custo reduzido com a utilização desta infra-estrutura compartilhada. Esta será uma das opções de adesão aos serviços da Central Notarial de Serviços Eletrônicos Compartilhados para as serventias que optarem por investimentos menores em infra-estrutura ou que desejem iniciar o uso da infra-estrutura imediatamente e adotar outra solução própria ao longo do tempo.

O sistema Cartório Digital estará plenamente integrado computacionalmente às aplicações estruturais e aos canais de serviços e integração. Engloba os processos de negócios dos notários ajustados para o novo ambiente competitivo, alicerçado na utilização plena do documento eletrônico.

Esta aplicação contribui para a criação de uma identidade compartilhada com elevada aceitação pela sociedade que espera serviços confiáveis e velozes. A possibilidade de todas as serventias disponibilizarem serviços neste nível – mesmo as que apresentam menor capacidade econômica, está alinhada a este objetivo.

5.7.6 APLICAÇÕES ESTRUTURAIS

Aplicações estruturais oferecem o arcabouço necessário para a implantação dos serviços cartoriais nesse novo contexto. São aplicações básicas que requerem infra-estrutura e investimentos consideráveis para a sua implantação – característica que impulsiona a racionalização

resultante do modelo cooperado. De forma simplificada, estas são aplicações que todos precisam e que individualmente a demanda não justifica o custo de sua implantação.

As Aplicações Estruturais, além de servirem de alicerce para as aplicações internas, podem ser fontes de novos serviços externos e, principalmente, elementos de fortalecimento de uma identidade conjunta da comunidade notarial.

Suas partes constituintes são determinadas a partir do levantamento dos processos de negócios nos quais as serventias estão inseridas, complementado com o levantamento da regulamentação que disciplina a prestação destes serviços por parte das serventias e das necessidades dos clientes.

Estas aplicações estão subdivididas em quatro grupos funcionais: Confiança no Documento Eletrônico, Armazenamento e Gerência Eletrônica de Documentos, Aplicações de Controle e Capacitação e Suporte. Esta é uma classificação funcional, mas deve-se salientar que estas aplicações apresentam funcionalidades complementares. É o conjunto destas funcionalidades que fortalece a Central Notarial de Serviços Eletrônicos Compartilhados.

5.7.6.1 CONFIANÇA NO DOCUMENTO ELETRÔNICO

O documento eletrônico deve ser utilizado em larga escala no âmbito da CNSEC, sendo a confiança nestes documentos fundamental para o seu funcionamento. Pesquisas desenvolvidas nesta área apontam que há uma série de requisitos a serem atendidos para que o uso seguro de documentos eletrônicos seja possível. Os três aspectos fundamentais neste aspecto são os relacionados com a autenticidade/integridade, existência de uma âncora temporal e integridade das plataformas computacionais.

A autenticidade e a integridade dos documentos são atendidas por técnicas criptográficas como assinatura digital. A Autoridade Certificadora Notarial e o Assinador Notarial serão operacionalizados com o objetivo de atender a estes requisitos.

A âncora temporal fornece evidências da existência dos documentos em determinado instante do tempo. A Autoridade de Carimbo do Tempo Notarial fornecerá o serviço de datação para a CNSEC.

O foco da Central Notarial de Serviços Eletrônicos Compartilhados é garantir a qualidade e segurança dos serviços prestados, mesmo na presença de plataformas computacionais maliciosas. Para este fim, nesta seção, são descritas as aplicações que garantem o uso de documentos eletrônicos nesse contexto.

5.7.6.1.1 AUTORIDADE CERTIFICADORA NOTARIAL

O objetivo da ICP-Brasil é estabelecer confiança no uso da certificação digital, tanto para fins de assinatura digital quanto para o sigilo dos documentos eletrônicos. A ICP-Brasil é composta por uma autoridade gestora de políticas, pelas Autoridades de Registro (AR) e pela cadeia de autoridades certificadoras; esta composta pela Autoridade Certificadora Raiz (AC-Raiz) e pelas Autoridades Certificadoras (AC).

Os certificados digitais para usuários finais são emitidos por ACs geralmente subordinadas às ACs normativas. As chaves criptográficas utilizadas nas assinaturas digitais são certificadas por esta entidade. Compete às Autoridades de Registro, entidades operacionalmente vinculadas a determinada AC, identificar e cadastrar usuários na presença destes, encaminhar solicitações de certificados às ACs e manter registros de suas operações.

Os usuários, de posse de um certificado, podem assinar digitalmente documentos e também se autenticar perante sistemas seguros.

As características específicas de cada aplicação que utiliza este serviço fazem com que existam diferentes políticas e práticas de certificação. A Autoridade Certificadora Notarial apresenta desta forma políticas e práticas de certificação adequadas ao funcionamento da Central Notarial de Serviços Eletrônicos Compartilhados.

Segundo divulgado pelo ITI em 19 de junho, as entidades que representam os cartórios de notas e registro tornar-se-ão Autoridades Certificadoras de segundo nível, podendo receber solicitações de emissão de certificados digitais. Com isso, as serventias poderão exercer o papel de Autoridade de Registro, bastando apenas credenciá-las como ARs junto à Autoridade Certificadora Notarial.

O certificado digital é um insumo básico em todas as aplicações de serviços ou estruturais que as utilizam para garantia dos requisitos de autenticidade, integridade, validade jurídica e interoperabilidade da ICP-Brasil.

5.7.6.1.2 AUTORIDADE DE CARIMBO DO TEMPO NOTARIAL

A datação de documentos eletrônicos é necessária para que estes possam ser utilizados da mesma forma que documentos tradicionais em papel. A datação fornece uma referência temporal, a qual permite determinar a existência de um documento eletrônico em determinado instante do tempo. Outro aspecto da datação de documentos eletrônicos que deve ser levado em consideração está ligado ao uso de assinaturas digitais. Uma assinatura digital tem sua

eficácia jurídica associada à validade do certificado digital do signatário. Sem uma referência temporal, não é possível determinar se a assinatura foi produzida enquanto o certificado era válido. Uma das prerrogativas do sistema notarial brasileiro é exatamente a prioridade, ou seja, a determinação da hora/data legal de um documento para efeitos de pré-notação e eficácia jurídica perante terceiros.

A datação é estabelecida pela entidade confiável, responsável por produzir o carimbo do tempo (timestamp) de um documento. A tarefa de datar um documento eletrônico requer um relógio de referência para a emissão de carimbos do tempo confiáveis por parte de um sistema que possa ter suas atividades auditadas. A forma de viabilizar o processo de datação é a utilização de uma entidade confiável que possa ser auditada e que apresente um relógio de alta precisão e confiabilidade. A fonte de tempo da hora legal brasileira é o Observatório Nacional e a instituição constitucionalmente responsável pela determinação perante terceiros da datação de documentos eletrônicos pode ser a Central Notarial de Serviços Eletrônicos Compartilhados com base na prerrogativa legal de estabelecer prioridade que os notários possuem.

O Carimbo do Tempo é um documento eletrônico assinado por uma terceira parte confiável denominada de Autoridade de Carimbo do Tempo, e que serve como evidência irrefutável da existência de uma informação digital numa determinada data e hora. Da mesma forma como é necessária uma infra-estrutura para a emissão de certificados digitais, denominada de infra-estrutura de chaves públicas (ICP), também é necessária uma infra-estrutura para a emissão de carimbos do tempo. Esta é denominada Autoridade de Carimbo do Tempo Notarial.

5.7.6.1.3 FRAMEWORK NOTARIAL DE DOCUMENTO ELETRÔNICO CONFIÁVEL

O Framework Notarial de Documento Eletrônico Confiável é um arcabouço que fornece todas as ferramentas necessárias à garantia da integridade, autenticidade e não-repúdio de documentos eletrônicos. Como exemplo de ferramentas fornecidas por este serviço tem-se o Assinador Notarial de Documentos Eletrônicos que realiza assinaturas digitais, verifica a integridade e autenticidade dos documentos. Além desse exemplo, o framework engloba um conjunto de ferramentas padronizadas e homologadas de desenvolvimento de sistemas. Aqueles cartórios que possuem sistemas próprios podem utilizar os “kits de integração” disponíveis no framework para integrarem-se à CNSEC.

O Framework Notarial de Documento Eletrônico Confiável é responsável pelo acompanhamento do estado das tecnologias utilizadas dentro das aplicações componentes deste sistema e pelo acompanhamento do marco regulatório que garante a eficácia jurídica do documento

eletrônico. Estas tecnologias podem tornar-se obsoletas, fazendo com que a integridade destes documentos seja ameaçada. Neste caso, o framework realiza, de forma automática, a substituição antes que possíveis problemas possam ocorrer, garantindo vida longa ao documento eletrônico.

Todos os notários, através desta aplicação, independente do sistema computacional utilizado, padronizarão o uso dos recursos de certificação digital – definindo um "norte" para a questão da confiança no documento eletrônico.

Como uma ferramenta gerencial, esta estrutura proporciona um rumo padronizado, único, participativo e com sinergia, para a evolução das aplicações computacionais – que gradual e progressivamente podem incorporar os protocolos criptográficos que desenham as mais diversas aplicações notariais.

O framewok também faz uso da Autoridade Certificadora Notarial e da Autoridade de Carimbo do Tempo Notarial para garantir a confiança dos documentos eletrônicos utilizados pela Central Notarial de Serviços Eletrônicos Compartilhados. Isso evidencia a flexibilidade do ambiente proposto e como os mais diversos e diferentes serviços podem ser utilizados para produzir novas aplicações herdando os benefícios das existentes.

5.7.6.2 ARMAZENAMENTO E GERÊNCIA ELETRÔNICA DE DOCUMENTOS

A gerência eletrônica de documentos é imprescindível, devido à grande quantidade de documentos e à grande diversidade de processos e tipos de documentos – que tornam inviável qualquer outro tipo de gerência.

O levantamento de processo realizado identificou três áreas: (i) Gerência Eletrônica de Documentos (GED); (ii) Depósito Sigiloso e (iii) Autoridade Certificadora Temporal Notarial.

5.7.6.2.1 GERÊNCIA ELETRÔNICA DE DOCUMENTOS (GED)

O tratamento de documentos deixou de ser visto como simples arquivamento, para ser encarado como estratégico. A gestão documental não é um conceito novo, nem uma tecnologia. Trata-se de uma metodologia de tratamento de documentos e informações, que tem a finalidade de mantê-los de forma organizada, acessível e segura.

No documento físico, onde a informação está escrita normalmente em papel, é comum que cópias sejam feitas em um maior número de vias. Porém, em documentos eletrônicos a cópia não difere do documento original: sempre será igual à matriz. Por isso, não existem cópias nem

vias de documentos eletrônicos, enquanto ele for mantido nesta forma.

Se o documento tem origem em meio eletrônico, devidamente assinado, este pode ser utilizado para gerar uma versão impressa. Neste caso, a cópia é o papel e o documento original é o arquivo eletrônico contendo a assinatura digital. Da mesma forma, um documento em papel pode ser desmaterializado para o meio digital, por meio de um scanner, que digitaliza a imagem do documento, para fins de consulta ou transmissão.

Para que uma cópia tenha a mesma validade de um documento original há a necessidade de autenticação. O tabelião pode e deve assinar a cópia eletrônica, garantindo-lhe a devida autenticidade, da mesma forma que tradicionalmente o faz através de carimbos e selos no documento papel. Portanto, a mudança do documento digital para o papel, ou vice-versa, trás sempre a necessidade também de autenticá-lo.

Mediante estes argumentos, propõe-se um componente estrutural denominado Gerência Eletrônica de Documentos que permita o controle de todo o ciclo de vida de um documento, desde sua criação ou digitalização até o momento de armazenamento em base de dados. Esta aplicação pode conter mecanismos de digitalização ou impressão de documentos eletrônicos (desmaterialização/materialização de documentos).

Este tipo de serviço, prestado pela Gerência Eletrônica de Documentos, da CNSEC, é de importância fundamental em um ambiente onde a quantidade de documentos é substancialmente elevada e a falta de controle pode tornar a prestação de serviço excessivamente lenta ou até mesmo inviabilizá-la. Todos os documentos seriam indexados e armazenados de forma a facilitar qualquer operação de consulta.

A Gerência Eletrônica de Documentos apresenta um mecanismo completo para controle do ciclo de vida dos documentos eletrônicos. Os documentos gerenciados pela CNSEC sempre pertencem a uma serventia, que estabelece as políticas de seu uso. Um documento somente poderá ser alterado se for permitido ao interessado realizar esta tarefa. Neste mecanismo, um ponto fundamental é o controle de versões automatizado que gerencia as várias versões de um documento, as anotações realizadas, as alterações realizadas ao longo do tempo e as alterações futuras sugeridas pelos editores.

Esta aplicação em conjunto com o Framework Notarial de Documento Eletrônico Confiável forma um núcleo básico que atende às necessidades das serventias na prestação de vários serviços, mas também permite o desenvolvimento de novos de forma rápida e confiável.

5.7.6.2.2 DEPÓSITO SIGILOSO

Uma das formas de se garantir o sigilo do documento em papel é inserindo-o em um envelope e depois o lacrando. Uma vez que o lacre esteja intacto, o destinatário do documento tem a garantia de que este foi mantido sigiloso desde o momento em que foi colocado e lacrado no envelope.

No contexto de documentos eletrônicos o mesmo procedimento pode ser abordado de duas formas. A primeira se baseia na crença de que a terceira parte confiável, responsável pela guarda do documento, é honesta, e capaz de manter íntegro e inacessível o documento até a solicitação do mesmo por alguma entidade autorizada – um fator de alto custo. A abordagem mais recomendada, e escolhida pela Central Notarial de Serviços Eletrônicos Compartilhados, consiste na cifragem deste documento – este só poderá ser lido por aqueles de posse da chave de decifragem. A chave de decifragem pode ser "quebrada" em diversas partes e estas controladas por grupos de pessoas, entidades ou tabelião, conforme a política previamente estabelecida. Uma possível política é definir que somente um número mínimo de pessoas deve cooperar para poder recuperar a chave e assim abrir o documento sigiloso.

O Depósito Sigiloso tem o propósito de oferecer esta funcionalidade, e igualmente, suprir todas as necessidades relativas, como por exemplo, as políticas e procedimentos necessários em caso de perda das chaves.

5.7.6.2.3 AUTORIDADE CERTIFICADORA TEMPORAL NOTARIAL (ACTEMPON)

Uma das formas de se garantir o sigilo temporal do documento em papel é inserindo o documento em um envelope e depois o lacrando. O envelope pode ser mantido em local seguro e entregue ao destinatário somente na data de abertura. O destinatário pode então, na data previamente estabelecida, romper o lacre e revelar seu conteúdo. Uma vez que o lacre esteja intacto, o destinatário do documento tem a garantia de que o documento foi mantido sigiloso desde o momento em que foi colocado no envelope e inserido o lacre. Cabe ressaltar que neste caso, ninguém, nem mesmo o responsável pelo lacre do envelope pode provar qual o conteúdo do documento sem quebrar o lacre. A quebra do lacre pode ser facilmente identificada.

Como exemplo de aplicações que requerem o armazenamento sigiloso e liberação da informação em um instante de tempo no futuro, pode-se citar as licitações, leilões, acesso a documentos sigilosos e testamentos.

Apesar da ICP-Brasil ter definido dois conjuntos de certificados digitais, um para assi-

natura e outro para sigilo, a quase totalidade das resoluções regulando o assunto tratam exclusivamente da assinatura digital e procedimentos associados tal como a autenticação. Não há qualquer definição de procedimentos ou recomendações para o efetivo uso dos certificados de sigilo. Pode-se constatar que isso não é exclusividade do Brasil. Isso acontece em praticamente todas as nações do mundo, que têm alguma legislação regulando o uso da certificação digital. Acredita-se que, em grande parte, isso é devido à falta de uma infra-estrutura apropriada ao sigilo de documentos eletrônicos.

O objetivo da Autoridade Certificadora Temporal Notarial (ACTempoN) é permitir o gerenciamento do ciclo de vida dos certificados digitais temporais. A ACTempoN é responsável pela geração de um par de chaves criptográficas assimétricas. Um das chaves, denominada chave privada, é mantida em sigilo. O par correspondente é tornado público e por isso é chamado de chave pública. Uma informação cifrada utilizando a chave pública só poderá ser decifrada usando a correspondente chave privada. A chave privada é mantida em sigilo até uma determinada data no futuro quando é publicada. A chave pública correspondente é inserida no chamado certificado digital temporal.

Em conjunto com o Depósito Sigiloso, permite que documentos lá armazenados só possam ter seu conteúdo revelado após uma data e hora pré-estabelecidas.

5.7.6.3 APLICAÇÕES DE CONTROLE

Nesta seção são apresentadas aplicações que realizam controles diversos com o intuito de permitir que a Central Notarial de Serviços Eletrônicos Compartilhados gere evidências que tornem possíveis a auditoria e contabilidade de suas atividades, agregando assim, uma maior credibilidade à estrutura.

As Aplicações de Controle são: (i) Autoridade de Aviso, (ii) Emissor de Selos Digitais de Controle e Autenticidade, (iii) Controladoria Eletrônica e (iv) Corregedoria Eletrônica.

5.7.6.3.1 AUTORIDADE DE AVISO

Uma comunicação que não é executada em tempo real, por exemplo, o e-mail, é passível de negação de recebimento. Se o processo normal de comunicação tiver problemas de recusa de recebimento (repúdio), ou seja, um participante não conseguir uma resposta de outro participante, deverá ser usada uma Autoridade de Aviso. A Autoridade de Aviso tem como objetivo garantir que toda comunicação oficial entre entidades não tenha problemas de repúdio.

A Autoridade de Aviso faz o papel de jornal ou de cartas registradas enviadas pelo correio. Só que neste caso, a Autoridade de Aviso pode ter uma funcionalidade maior. Ela pode, por exemplo, ser responsável por enviar um e-mail, publicar o aviso em jornais on-line, fóruns, ou até mesmo em jornais impressos em papel. Tudo o que é feito pela Autoridade de Aviso é publicado também em um diretório público.

5.7.6.3.2 EMISSOR DE SELOS DIGITAIS DE CONTROLE E AUTENTICIDADE

As corregedorias têm no Selo de Controle dos Atos dos Serviços Notariais e de Registro uma forma de impedir adulterações, imitações, cópias não autorizadas de forma a obter a mais absoluta segurança jurídica na autenticidade dos atos da serventia extrajudicial.

O Emissor de Selos Digitais de Controle e Autenticidade atende às mesmas necessidades das corregedorias dentro da Central Notarial de Serviços Eletrônicos Compartilhados. Todo documento emitido dentro da CNSEC deve apresentar um selo de controle ligado de forma única ao documento, não podendo um selo estar relacionado a mais de um documento.

O selo também é um documento assinado pela corregedoria, contendo o resumo criptográfico do documento a que se refere, uma descrição sucinta do documento, número serial e identificação da serventia que o requisitou e do cliente que solicitou o serviço.

É controlado pelas corregedorias que podem utilizar seus registros de eventos no caso de necessidade de auditorias.

Os mecanismos de controle e garantia da qualidade do serviço prestado são complementados por estes selos, que seriam anexados a todos os documentos emitidos pelas serventias integradas na Central Notarial de Serviços Eletrônicos Compartilhados. Estes selos seriam emitidos eletronicamente, dentro dos padrões de segurança da ICP-Brasil, com a autorização da autoridade competente, e utilizados pelas serventias sempre que necessário.

5.7.6.3.3 CONTROLADORIA ELETRÔNICA

Por ser uma central compartilhada, há um grande fluxo de serviços entre usuários e serventias. Este fluxo gera uma contabilização de valores decorrentes do uso de serviços. Ao final de um determinado período, as partes que forneceram o serviço devem ser devidamente ressarcidas.

Há também a necessidade de controlar os valores a serem direcionados às corregedorias decorrentes de emolumentos recolhidos.

Percebe-se que os valores são recolhidos em diversos prestadores de serviço, fazendo-se necessária a existência de uma aplicação estrutural que garanta a todos os envolvidos o pagamento e recebimento dos valores legalmente previstos.

A Controladoria Eletrônica tem por finalidade automatizar o fluxo contábil, facilitando o fechamento de contas e configurando-se como uma central automática de compensação.

Este serviço desempenha sua funcionalidade de forma transparente, permitindo a todos o acesso aos dados para que não existam dúvidas quanto aos valores envolvidos.

5.7.6.3.4 CORREGEDORIA ELETRÔNICA

Este módulo provê a função correcional das atividades notarias e de registro. O livro de Visitas e Correições pode ser um documento eletrônico assinado pelo magistrado, havendo um para cada unidade notarial e de registro. O visto de correição poderá ser feito através de assinatura digital.

5.7.6.4 CAPACITAÇÃO E SUPORTE

Todo sistema desenvolvido tem, ou pelo menos deveria ter, um espaço onde os principais usuários – neste caso os notários – pudessem requisitar assistência técnica, sugerir um melhoramento ou mesmo assinalar suas reclamações. A CNSEC não será diferente e terá um módulo especialmente desenvolvido para isso, pois, para que as serventias prestem serviços com qualidade, estas precisam de uma estrutura que atenda suas necessidades e anseios.

Outro componente de fundamental importância em um projeto como este, é um módulo que capacite os notários a prestarem seus serviços nesta nova estrutura. Além desta função, a Central de Capacitação tem a finalidade de ser uma porta para a educação a distância, por ser uma idéia inovadora e adequada à realidade das serventias, uma vez que o Brasil é um país extenso e cursos de atualização poderiam ser ministrados a todos os interessados, sem necessidade de deslocamento.

As aplicações que compõem esta seção são: (i) Central de Comunicação e Suporte e (ii) Central de Capacitação.

5.7.6.4.1 CENTRAL DE COMUNICAÇÃO E SUPORTE

A Central de Comunicação e Suporte é responsável pela comunicação das serventias com a administração da CNSEC. Qualquer solicitação de suporte ou pedido de ajuste da estrutura seria realizado através desta aplicação.

É através da análise dos registros da Central de Comunicação e Suporte que se pode avaliar as métricas de efetividade e eficiência deste mecanismo. Estas informações serão coletadas pelo sistema e oferecidas à administração do sistema para acompanhamento das atividades – e esta pode realizar ajustes na estrutura para melhora do desempenho.

5.7.6.4.2 CENTRAL DE CAPACITAÇÃO

A Central de Capacitação busca a educação continuada dos envolvidos na prestação de serviço nas serventias extrajudiciais e no desenvolvimento de novas aplicações. Os objetivos são o aperfeiçoamento dos serviços, harmonização de procedimentos, buscando uma regulação uniforme nas atividades notariais e registrais, visando o aprimoramento técnico dos notários e a reciclagem de prepostos e profissionais que atuam na área.

Frente às enormes distâncias geográficas no Brasil, há a necessidade de uma alternativa para maior acessibilidade a Central de Capacitação, através de um projeto de educação a distância. A Educação a distância é o processo de ensino-aprendizagem, mediado por tecnologias, onde professores e alunos estão separados espacial e/ou temporalmente.

Hoje temos a educação presencial, semipresencial (parte presencial/parte virtual ou a distância) e educação a distância (ou virtual). A presencial é a dos cursos regulares, em qualquer nível, onde professores e alunos se encontram sempre num local físico, chamado sala de aula. É o ensino convencional. A semipresencial acontece em parte na sala de aula e outra parte a distância, através de tecnologias diversas. A educação a distância pode ter ou não momentos presenciais, mas acontece fundamentalmente com professores e alunos separados fisicamente no espaço e/ou no tempo, mas podendo interagir através de tecnologias de comunicação.

Outro conceito importante é o de educação contínua ou continuada, que se dá no processo de formação constante, de aprender sempre, de aprender em serviço, juntando teoria e prática, refletindo sobre a própria experiência, ampliando-a com novas informações e relações – como é proposto.

As tecnologias interativas, sobretudo, vêm evidenciando, na educação a distância, o que deveria ser o cerne de qualquer processo de educação: a interação e a interlocução entre todos

os que estão envolvidos nesse processo.

Na medida em que evoluem, as tecnologias de comunicação virtual, que conectam pessoas que estão distantes fisicamente através de redes de comunicação de dados tal como a Internet modificam o conceito de presencialidade. Poderemos ter professores externos compartilhando determinadas aulas ou mesmo um professor de fora "entrando" com sua imagem e voz na aula de outro professor. Haverá, assim, um intercâmbio maior de saberes, possibilitando que cada professor colabore, com seus conhecimentos específicos, no processo de construção do conhecimento, muitas vezes a distância.

O conceito de curso ou aula também muda. Hoje, ainda entendemos por aula um espaço e um tempo determinados. Mas, esse tempo e esse espaço, cada vez mais, serão flexíveis. O professor continuará "dando aula", e enriquecerá esse processo com as possibilidades que as tecnologias interativas proporcionam: para receber e responder mensagens dos alunos, criar listas de discussão e alimentar continuamente os debates e pesquisas com textos, páginas da Internet, até mesmo fora do horário específico da aula. Há uma possibilidade cada vez mais acentuada de estarmos todos presentes em muitos tempos e espaços diferentes. Assim, tanto professores quanto alunos estarão motivados, entendendo "aula" como pesquisa e intercâmbio. Nesse processo, o papel do professor vem sendo redimensionado e cada vez mais ele se torna um supervisor, um animador, um incentivador dos alunos na instigante aventura do conhecimento.

Podem ser oferecidos cursos predominantemente presenciais e outros predominantemente virtuais. Isso dependerá da área de conhecimento, das necessidades concretas do currículo ou para aproveitar melhor especialistas de outras instituições, que seria difícil contratarem.

Sugere-se a adoção de um sistema de educação continuada a distância. Para isto, há a necessidade de que todo o conteúdo seja preparado minuciosamente, garantindo qualidade e eficácia ao aprendizado.

Estabelecem-se como requisitos os seguintes cursos, além de uma equipe capacitada para desenvolver o material didático:

- capacitação continuada;
- capacitação técnica;
- capacitação aos processos;
- direito notarial e registral;
- gestão de processos de negócio;

- projetos e implementação de sistemas voltados a CNSEC;
- desenvolvimento de aplicativos utilizando as ferramentas disponíveis na CNSEC.

5.7.7 GESTÃO DA CNSEC

Credibilidade é fator chave na CNSEC. Nesse sentido, a estrutura gera evidências de todas as suas atividades, e provê facilidade para a configuração de permissões de acesso de seus integrantes, dentro de seus respectivos papéis. Além disso, permite o monitoramento em tempo-real, assumindo postura pró-ativa para notificação em certas situações.

São, portanto, notáveis as seguintes áreas: (i) Monitoramento e Configuração, (ii) Auditoria e (iii) Administração.

5.7.7.1 MONITORAMENTO E CONFIGURAÇÃO

A Central Notarial de Serviços Eletrônicos Compartilhados é constituída por diversos componentes que cooperam entre si para que o sistema, como um todo, cumpra seu propósito. Estes devem ser corretamente configurados e seu funcionamento deve ser monitorado em tempo real, a fim de que, em caso de falhas, as devidas medidas sejam tomadas o mais prontamente possível. O Monitoramento e Configuração têm por meta oferecer aos administradores um meio de suprir essas necessidades. Seu acesso dá-se através de uma página Web. Quando necessário este componente também pode avisar os administradores, sobre certos eventos, por outros meios (e-mail, SMS, etc).

5.7.7.2 AUDITORIA

Todos os componentes da CNSEC geram registros no decorrer de seu funcionamento. Isso permite a verificação das atividades realizadas, provendo meios de garantir que as mesmas são executadas de forma apropriada e conforme previsto. Tais evidências são periodicamente analisadas por auditores internos e externos.

5.7.7.3 ADMINISTRAÇÃO

No contexto da Central Notarial de Serviços Eletrônicos Compartilhados, existem diversos integrantes que exercem diferentes papéis. Entre eles, aqueles necessários para o devido funcionamento do sistema, como os administradores e auditores, e aqueles que estão vinculados à

CNSEC, como as próprias serventias e órgãos. Este componente oferece, através de uma página Web, as funções necessárias para a devida gerência desses participantes dentro do sistema.

5.8 CENÁRIOS DE INTEGRAÇÃO

Nesse ponto, torna-se perceptível a capacidade da CNSEC de acomodar as mais diferentes necessidades de seus associados no uso de serviços da CNSEC ou na integração de sistemas existentes. Essa gama de opções permite a visualização de diversos cenários de vinculação. Nessa seção, lista-se alguns deles. Nota-se que esta listagem não é exaustiva, e diversos outros cenários podem ocorrer.

É interessante notar que as serventias poderão continuar prestando seus serviços da forma que já o fazem. Sua integração à CNSEC é especificada serviço-a-serviço, ou seja, o cartório tem a possibilidade de integrar cada serviço da forma que desejar, ou mesmo não integrar certos serviços. Desse modo, as serventias podem enquadra-se ao mesmo tempo em mais de um cenário apresentado – seja no modo tradicional, como representado na figura 14, ou em outros cenários possíveis, incluindo aqueles listados nessa seção.

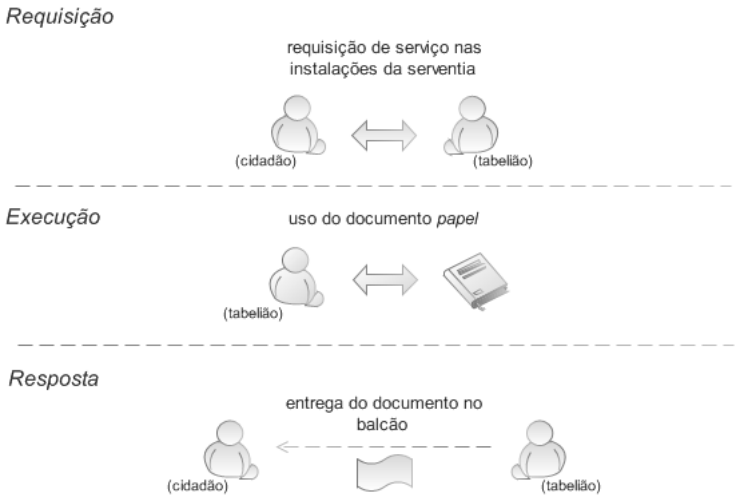

Figura 14: Modo tradicional.

Provavelmente, o cenário mais simples de integração ocorre quando a serventia pretende apenas atender a um número maior de clientes, devido a exposição de seus serviços pela CNSEC – usuários poderão requisitar seus serviços por meio do Portal de Serviços e Informações disponível na Internet. A mesma também não deseja empregar grandes investimentos em TI e, portanto, utiliza o software de gestão Cartórios Digitais, que fica hospedado na CNSEC. Sua autenticação, junto ao sistema, dá-se por meio de smartcard com certificados dig-

itais ICP-Brasil, porém há a possibilidade do uso complementar de identificações biométricas. Por fim, tendo em vista sua disposição de apenas utilizar documento papel, a execução de suas atividades continua baseada em seus livros e outros documentos, e a entrega das respostas aos pedidos de serviço, poderá ser apenas efetuada através do balcão ou pelo correio. Este cenário é ilustrado na figura 15.

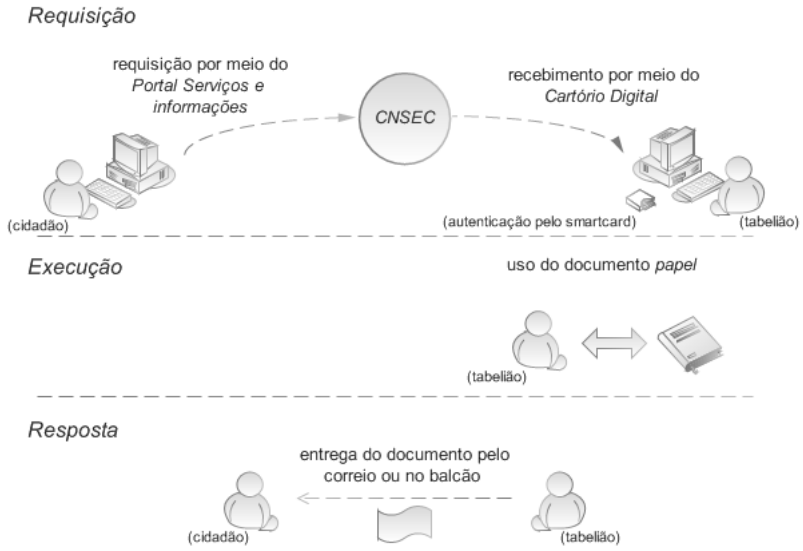

Figura 15: Página na Web.

Uma vez que a serventia deseje também responder por meio eletrônico a pedidos de serviços, oferecendo comodidade aos seus clientes, evitando filas em suas instalações, e diminuindo gastos com papel, o cartório pode passar a digitalizar seus documentos por meio de um scanner no momento da entrega. Esse documento eletrônico é, então, enviado através do Cartório Digital, conforme ilustra a figura 16. Vislumbra-se nesta figura a possibilidade do tabelião pode utilizar ambos os meios de reposta ao cliente: documento papel ou documento eletrônico.

A execução dos serviços pelo tabelião, entretanto, ainda está baseada na lida com documentos em papel – o que implica em diversos problemas, dentre eles uma maior dificuldade na busca de informações e necessidade de um espaço físico adequado, e crescente, para a guarda dos mesmos. Nesse contexto, o cartório pode passar a armazenar seus dados em bancos de dados, o que lhe dará maior segurança, graças a possibilidade da realização de backups (cópias de segurança), maior rapidez na prestação de serviços, tendo em vista, a utilização de ferramentas de Gerência Eletrônica de Documentos, e redução de custos com papel, conforme é ilustrado na figura 17.

Alguns serviços prestados devem, por diversos motivos, ser executados sem poderem ser cobrados e constituem-se em ônus ao cartório. Este é o caso, por exemplo, de algumas solici-

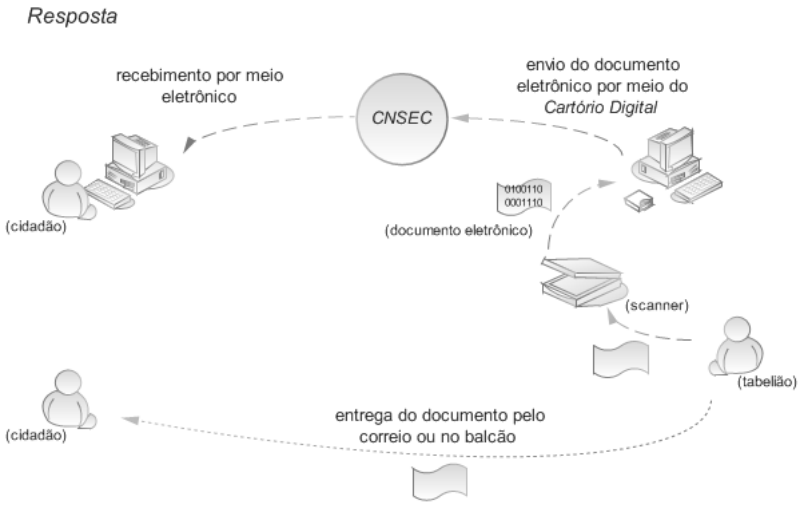

Figura 16: Resposta por meio digital.

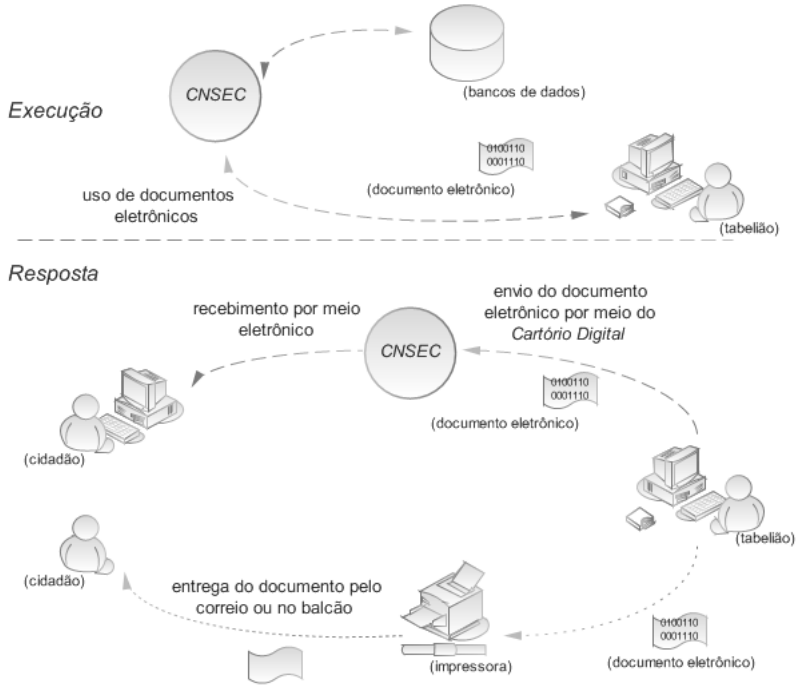

Figura 17: Emprego de bancos de dados.

tações do Estado. É importante minimizar ao máximo a posta de recursos das serventias para o atendimento destas solicitações. Isso permite que os recursos sejam integralmente destinados àqueles serviços que permitem o seu sustento, o que trará benefícios a todo os seus usuários. Para isso existe a possibilidade de delegar a execução de alguns serviços ou parte dos mesmos à CNSEC conforme ilustra a figura 18. Tal medida, contudo, requer que os dados para a execução dos serviços estejam acessíveis – em bancos de dados. O serviço por completo ou parte dele será, então, automatizado pelas aplicações de serviço. As respostas aos pedidos podem ser

diretamente encaminhadas aos requisitantes, ou, podem primeiramente passar pela finalização ou aprovação do tabelião.

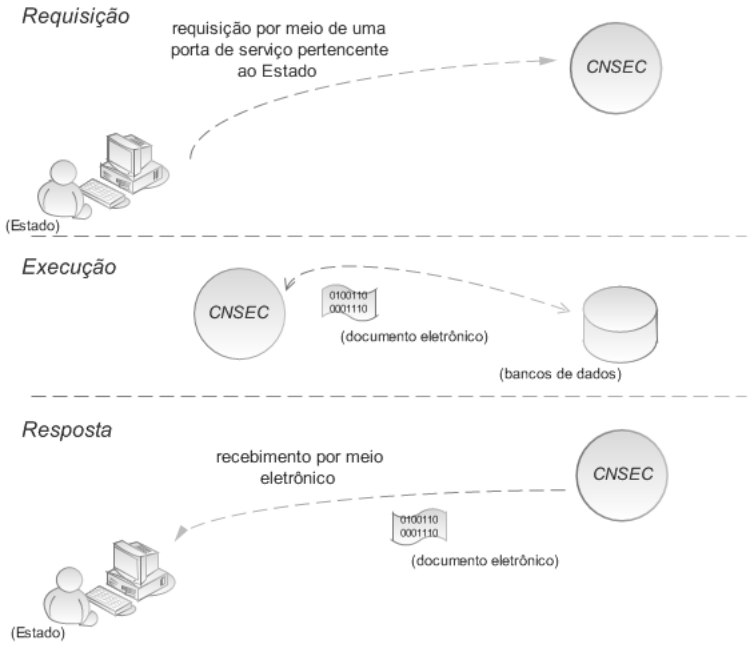

Figura 18: Automatização de processos.

A CNSEC oferece, por padrão, implementações para a gestão da serventia, por meio do Cartório Digital, e a automatização de processos através das aplicações de serviço do Provedor de Aplicações de Serviço. Entretanto, a estrutura permite que as serventias apontem para seus próprios sistemas, desde que estejam dentro dos padrões estabelecidos para a comunicação entre os sistemas por mensagens XML.

5.9 CENÁRIOS DE ACESSO AOS SERVIÇOS

Como visto, a CNSEC contempla as diferentes necessidades e possibilidades dos interessados em serviços, por meio dela providos, através de portas de serviço. Numa determinada porta o usuário especifica quais serviços utilizará, e como.

Nesse contexto, inúmeros são os modos de acesso aos serviços, e novos podem ser criados quando necessários. Essa seção lista alguns deles, entretanto não pretende esgotá-los, e diversos outros cenários de uso são possíveis.

Como já apresentado na seção Cenários de Integração um usuário – dependendo do caráter do serviço e nos interesses e possibilidades das partes – pode ter sua requisição atendida no balcão, via correio, ou em meio eletrônico.

Contudo, essa nova realidade criada pela CNSEC permite a visualização de cenários mais elaborados. Essa estrutura possibilita, por exemplo, a requisição de serviços que envolvam um conjunto de serventias. O usuário do serviço pode, por exemplo, especificar uma dada localidade, e as serventias do local responderão ao pedido. Este cenário é ilustrado na figura 19. O modo como cada serventia responde depende da forma pela qual a mesma integrou-se ao sistema. Esse fator, contudo, é apenas percebido pelo usuário por meio de uma diferença entre o tempo de resposta dos cartórios.

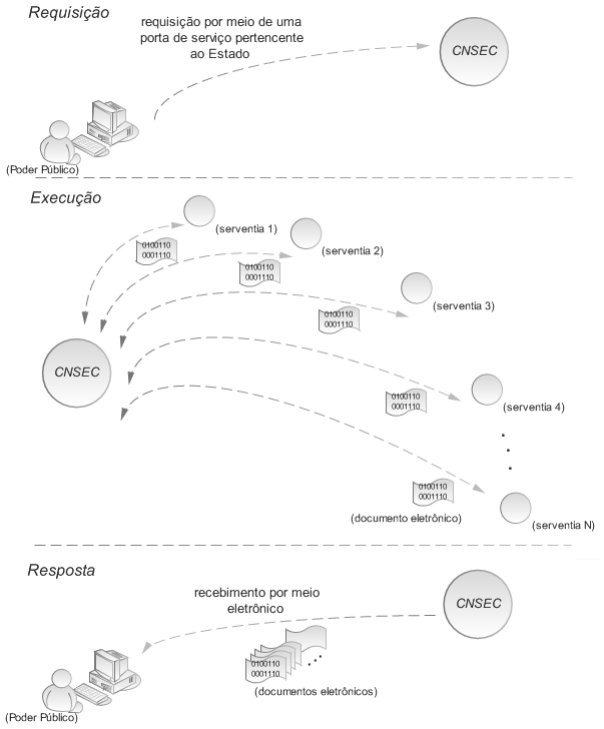

Figura 19: Cenário de acesso 1.

A integração promovida pela CNSEC, do mesmo modo, oferece ao usuário a liberdade de escolher em que serventia deseja receber a informação requisitada. Livrando-o do ônus de deslocar-se até o cartório onde está o documento que procura.

Uma vez que o usuário necessite de algum documento em papel e o mesmo pertença a uma serventia instalada em localidade diferente da qual ele encontra-se, o mesmo pode dirigir-se à serventia mais próxima e requisitar o documento desejado. Essa tratará de contatar a serventia detentora do documento requerido, recebê-lo por meio eletrônico, e materializá-lo – desde que ambos os cartórios estejam integrados à CNSEC, como mostra a imagem 20.

Outro benefício oriundo da integração das serventias à CNSEC, está na possibilidade de criação de aplicativos, por parte dos clientes, para acessar os serviços cartoriais.

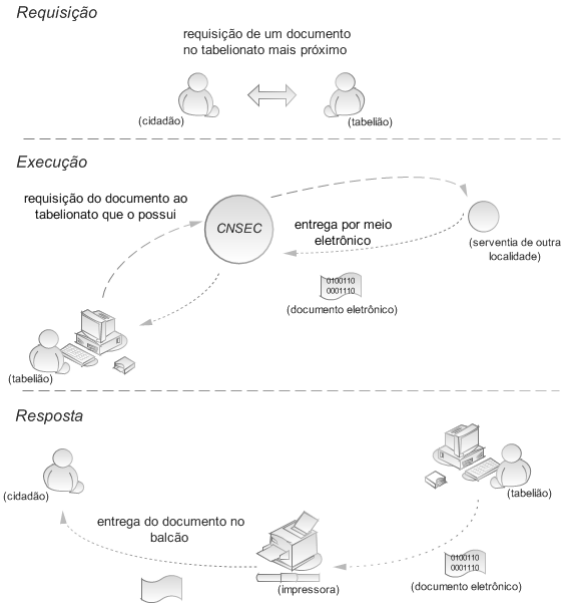

Figura 20: Cenário de acesso 2.

Um banco, por exemplo, pode solicitar a criação de uma porta de serviço a ele dedicada. O mesmo especifica quais serviços deseja, e como quer acessá-los. Um possível meio de acesso seria através de mensagens XML. Nesse sentido, uma vez que as serventias prestadoras do referido serviço concordem, a CNSEC criaria a infra-estrutura necessária para receber essas requisições XML e redirecioná-las às serventias. O tratamento dessas requisições pelas mesmas, obviamente, dependeria da forma pela qual as mesmas se integraram ao sistema.

Uma vez criada a infra-estrutura, será exposta ao banco a definição das mensagens XML de acesso aos serviços. Com base nessas mensagens, o mesmo pode criar, de forma simples, aplicações que façam uso desses serviços. Esta configuração é mostrada na figura 21.

Esse mesmo contexto aplica-se a qualquer usuário dos serviços prestados por meio da CNSEC, e outros meios de acesso são possíveis, como por exemplo, páginas Web.

5.10 INTEGRAÇÃO COM OUTROS SISTEMAS

Nessa seção está descrito como os sistemas já existentes (também conhecidos por sistemas legados), e os sistemas futuramente desenvolvidos poderão ser integrados à Central Notarial de Serviços Eletrônicos Compartilhados. Vale ressaltar que além de uma simples integração – suas funcionalidades podem ser disponibilizadas aos usuários por meio da central – é possível estender ou aperfeiçoar as funcionalidades do sistema existente por meio do uso de serviços oferecidos pela CNSEC.

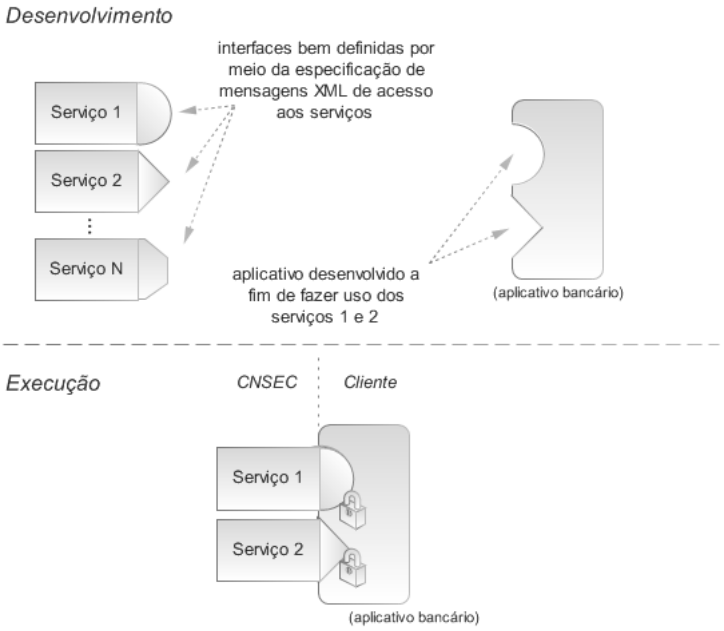

Figura 21: Cenário de acesso 3.

Em geral, esses sistemas têm suas funcionalidades definidas na camada lógica. O acesso a essas funções ocorre por meio da camada de apresentação, através de alguma representação assimilável aos usuários – uma página Web, por exemplo, conforme mostra a figura 22. Assim sendo, sistemas podem, até certo ponto, serem vistos como prestadores de serviços aos usuários e, portanto são integrados à CNSEC por meio de portas de integração. Imagem:Integracao sis legado 1.PNG

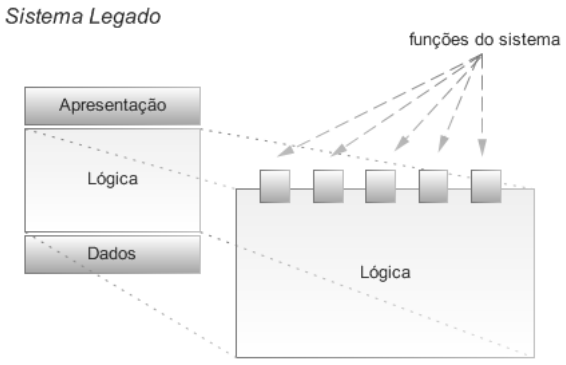

Figura 22: Sistema Legado.

Nesse sentido, o oferecimento das funcionalidades de um sistema por meio da CNSEC envolve a habilitação do mesmo para tal situação. Para tanto, dois passos básicos são necessários:

1. criação de uma porta de integração junto a CNSEC, especificando o modo pela qual as requisições aos serviços serão encaminhadas – especificação das mensagens XML que

serão usadas na comunicação – e, o modo como os serviços deverão ser ofertados pela CNSEC, mais precisamente, através de quais portas de serviço;

2. exposição das funcionalidades do sistema através de componentes Web Service. Esses componentes são responsáveis pela transformação das requisições oriundas da CNSEC, por meio de mensagens XML definidas no passo anterior, em chamadas nativas do sistema. Desse modo, proporciona-se a interoperabilidade entre a CNSEC e qualquer sistema, independentemente da plataforma ou linguagem em que foi desenvolvido. Tais componentes também são responsáveis pelo caminho inverso da comunicação, ou seja, a transformação das respostas do formato nativo do sistema para XML, podendo assim ser recebida pela central.

Tal procedimento é ilustrado na figura 23.

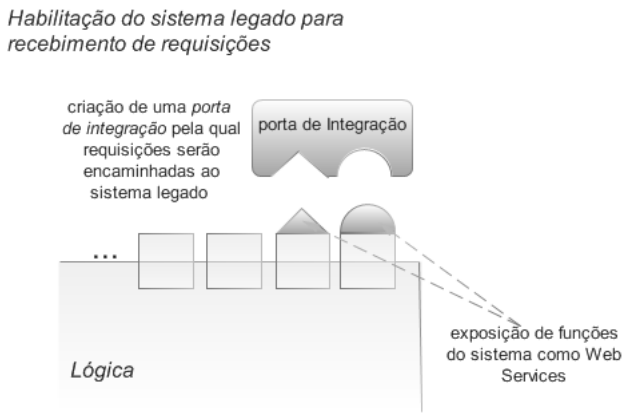

Figura 23: Habilitação para recebimento de requisições.

Uma vez que o sistema esteja apto a receber requisições e responder por elas, portas de serviço podem ser criadas ou adaptadas, sob demanda, para utilizarem esses novos serviços. Desta forma, independentemente do fato de a CNSEC comunicar-se com o sistema por meio de mensagens XML, usuários potencias do serviço podem pedir a exposição dos mesmos através de uma página Web, por exemplo. Tal pedido é então atendido, com a criação ou adaptação de uma porta de serviço destinada ao referido usuário, desde que o provedor do serviço esteja de acordo.

Essa nova realidade é representada na figura 24.

A integração do sistema em questão pode ir além. O mesmo pode beneficiar-se dos serviços ofertados pela CNSEC, tais como a Autoridade Certificadora Temporal Notarial, a Autoridade de Carimbo do Tempo Notarial, entre outros. Dessa forma, tem-se a vantagem das implemen-

Figura 24: Possibilidade de criação/adaptação de portas de serviço.

tações dos serviços serem mantidas e atualizadas pela central, acompanhando as evoluções das tecnologias envolvidas e livrando o responsável pelo sistema de tal ônus.

Essa integração envolve os seguintes passos:

1. definição de uma porta de serviço onde será especificado qual serviço da CNSEC deseja utilizar, e de que forma – conjunto de mensagens XML que será empregado;
2. adaptação do sistema em questão. É necessário adaptar o sistema de modo a utilizar as implementações fornecidas através da porta de serviço criada. Isso envolve a criação de componentes Web Service, que façam a transformação das chamadas nativas do sistema nas mensagens XML definidas anteriormente, podendo assim ser recebidas pela CNSEC.

A figura 25 ilustra essa configuração.

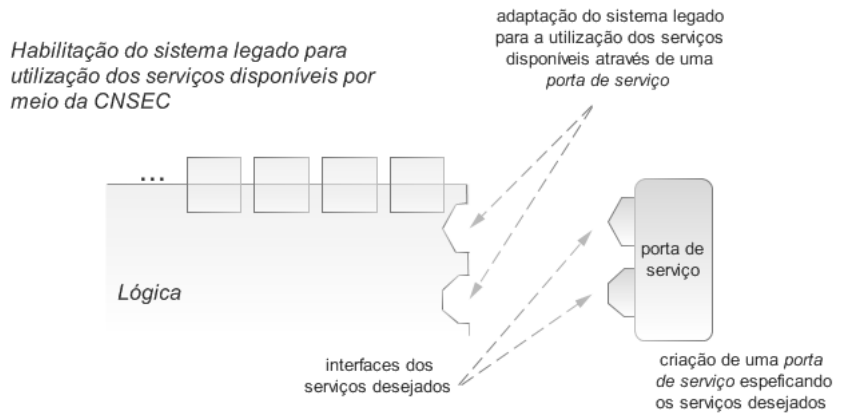

Figura 25: Habilitação para utilização dos serviços da CNSEC.

É interessante notar que após a integração o sistema ainda pode ser utilizado como o era antes de tal procedimento – sem alteração na forma como os usuários acessavam o serviço an-

teriormente, e nem modificação nos dados do sistema. Contudo, o mesmo agora está habilitado a receber requisições por meio da CNSEC, e ainda beneficia-se do uso de serviços mantidos e atualizados pela central, conforme ilustrado na figura 26.

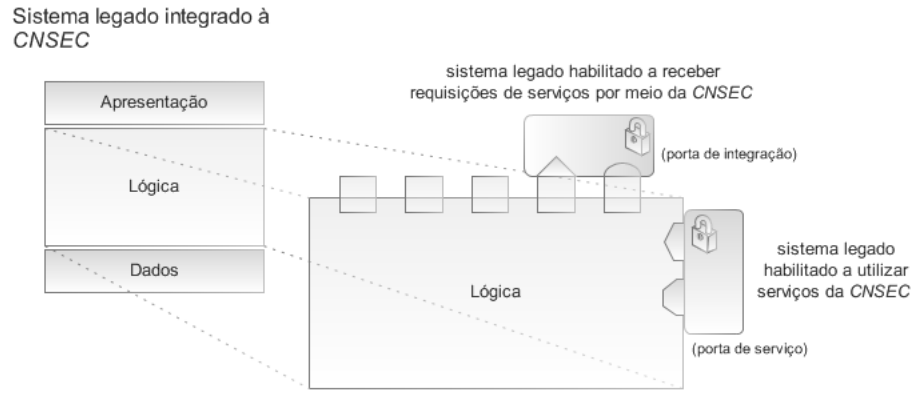

Figura 26: Sistema legado integrado a CNSEC.

Logo, a CNSEC oferece meios de integração de novos sistemas que venham a ser desenvolvidos e, igualmente, provê formas de aproveitar aqueles já existentes, tais como o Registro Central de Testamentos On-line (RCT-O), a Central de Escrituras e Procurações – (CEP), entre outros.

5.11 ACESSO DAS CORREGEDORIAS

As Corregedorias, órgãos do judiciário, são responsáveis pelo controle, fiscalização, orientação e instrução dos serviços jurisdicionais e administrativos da justiça, e em particular pelos serviços prestados pelas serventias extrajudiciais, seja a partir de documentos ou por inspeções e correições in loco. Artifícios tais como livros de correição e selos são utilizados como mecanismos de auxílio a estas inspeções e correições.

As corregedorias poderão se beneficiar da CNSEC seja pela busca de dados relativos aos processos de inspeção e correição previstos nos provimentos, seja através de sistemas de informação dos tribunais que poderão facilmente se integrar à estrutura através das portas de integração e de serviços como visto na seção Integração com Outros Sistemas.

5.12 CONCLUSÃO

Um cartório extrajudicial apresenta um elevado número de processos de negócios de complexidade elevada. Esta complexidade decorre da dependência desta atividade com uma série

de outras atividades econômicas e da regulamentação vigente, que é extensa e requer conhecimento específico de várias áreas.

Evidentemente que o processo de desenvolvimento da sociedade criou novas demandas que não foram correspondidas pelas serventias extrajudiciais. Neste momento são necessárias algumas correções para que as serventias utilizem o desenvolvimento tecnológico e científico para atender as demandas atuais e preparar as bases para novas demandas que com certeza existirão.

A solução para este quadro demanda um esforço cooperado para inserir todas as serventias e apresentar à sociedade uma resposta adequada de modernização. Sem este esforço cooperado, qualquer iniciativa apresentaria um tempo de desenvolvimento extenso e custo proibitivo, inviabilizando a inserção de grande parte das serventias que não apresenta capacidade econômica suficiente para um investimento desta magnitude.

O desenvolvimento da CNSEC é uma iniciativa que visa apresentar uma resposta a todos os usuários das serventias extrajudiciais, mobilizando uma rede de entidades que apresentam competências complementares. O desenvolvimento neste modelo fornecerá as ferramentas adequadas para a prestação de serviço de forma eficiente e com qualidade desejada. Não é objetivo deste projeto a simples informatização ou automação dos processos atuais. Pretende-se neste momento realizar uma ampla discussão com as entidades envolvidas, permitindo a otimização e desenvolvimento de novos processos de negócio de acordo com a necessidade das partes envolvidas.

Este modelo permite uma troca de experiências entre serventias e seus clientes, viabilizando um novo patamar para a prestação dos serviços. A visibilidade resultante deste esforço deve fortalecer as serventias que poderão dedicar-se à execução de suas atividades principais, atendendo às expectativas de todos os usuários.

O planejamento e controle da modernização decorrem da implantação de um modelo de gestão. O modelo de gestão está baseado na cooperação entre organizações com competências complementares. Tal modelo é compatível com a atual dinâmica do ambiente competitivo e abriga todos os envolvidos com as suas diferenças e semelhanças. A CNSEC – Central Notarial de Serviços Compartilhados é a materialização da ação planejada e cooperada de modernização.

6 *ARQUIVO DA CENTRAL NOTARIAL DE SERVIÇOS ELETRÔNICOS COMPARTILHADOS*

6.1 INTRODUÇÃO

As serventias extrajudiciais têm seu valor nos atos e documentos que emana. O aumento na celeridade dos seus serviços passa por sua modernização, e esta tem relação direta com o emprego de documentos eletrônicos frente ao uso dos tradicionais documentos em papel. É fato que muitos desses documentos atualmente já nascem em meio digital. Faz-se razoável, portanto, armazená-los nesse meio. Além disso, documentos em papel, quando armazenados, ocupam grande espaço físico e estão sujeitos a agentes como o tempo e insetos. Sua inconveniência, do mesmo modo, está em sua transmissão.

A microfilmagem de documentos em papel, que já possui suporte legal desde 1968, soluciona alguns desses problemas. Contudo, do mesmo modo carrega seus inconvenientes. Somando-se a isso, é restrito o número de cartórios que hoje em dia utilizam tais serviços.

Nesse sentido, é natural propor um modelo para a armazenagem dos documentos eletrônicos dos serviços delegados, que respeite os princípios junto a eles levantados. Entretanto, muitos desses documentos carecem de armazenagem por longo, ou mesmo indefinido período. E como esclarecido ao longo deste trabalho, esta não é uma tarefa trivial.

Assim, no decorrer deste capítulo é descrito o Arquivo da CNSEC. Uma proposta alinhada ao Modelo de Referência OAIS, que tem por meta possibilitar a preservação por longo prazo dos atributos desejáveis aos documentos eletrônicos no contexto das serventias extrajudiciais.

A fim de facilitar comparação com outros projetos de arquivos, este capítulo segue a estrutura dos anexos do Modelo de Referência OAIS e da norma ABNT NBR 15472: em Domínio, analisa-se o domínio no qual o Arquivo está inserido, e sua relação com os produtores e consumidores de dados; na seção Admissão são descritas os conceitos e procedimentos relacionados à recepção desses documentos e captura de metadados; em Formatos Internos descreve-se a forma como estes são armazenados e os procedimentos necessários a sua manutenção; por fim, em Acesso discorre-se sobre os meios pelos quais essas informações ficam acessíveis aos

tabelionatos.

6.2 DOMÍNIO

Guardiãs da base de dados primária da nação, as serventias extrajudiciais são o foco da CNSEC e do seu Arquivo. Esta seção visa, brevemente, descrever como o Arquivo está inserido nesse contexto, os papéis que os tabeliães exercem nesse ambiente e algumas atribuições dos notários, que permitirão a realização de alguns procedimentos necessários a correta preservação dos documentos eletrônicos em longo prazo, tais como o processo de normalização.

6.2.1 DOMÍNIO E CONSUMIDORES

Notário ou tabelião é um profissional do direito, dotado de fé pública, a quem é delegado o exercício da atividade notarial. Suas atribuições são declaradas na Lei n° 8.935, de 18 de novembro de 1994, que "Regulamenta o art. 236 da Constituição Federal, dispondo sobre serviços notariais e de registro. (Lei dos cartórios)" conhecida como a Lei dos cartórios.

A um notário, por exemplo, compete: formalizar juridicamente a vontade das partes; intervir nos atos e negócios jurídicos a que as partes devam ou queiram dar forma legal ou autenticidade, autorizando a redação ou redigindo os instrumentos adequados, conservando os originais e expedindo cópias fidedignas de seu conteúdo; e autenticar fatos.

São esses os consumidores que o Arquivo da CNSEC visa atender. A eles, além dos documentos eletrônicos preservados aos quais tem acesso, são fornecidas outras informações relacionadas, como, por exemplo, provas de que o documento manteve-se íntegro desde sua armazenagem, informações sobre sua proveniência, cadeia de custódia e histórico de procedimentos aos quais o documento foi submetido.

6.2.2 PRODUTORES DE DADOS

No exercer das atividades que lhe competem, o tabelião dá origem a documentos de naturezas diversas, como, por exemplo, testamentos, procurações e escrituras. Enquanto documentos eletrônicos, estes podem ser frutos de processos de desmaterialização – digitalização de documentos em papel – ou mesmo terem nascido em meio digital.

São estes os documentos alvos de preservação por parte do Arquivo da CNSEC. Para tanto, sofrem processos de normalização, classificação, indexação e inclusão de metadados que buscam torná-los aptos a conservação de longo prazo.

6.3 ADMISSÃO

Uma preservação de longo prazo bem sucedida depende primordialmente de uma correta preparação do documento para a armazenagem. Tal preparação deve tornar o documento o mais apto possível a conservar os atributos que se farão necessários ao longo do tempo. No Arquivo da CNSEC, tal procedimento ocorre junto a entidade funcional Admissão, e está relacionado aos conceitos abaixo detalhados.

6.3.1 ACORDO DE SUBMISSÃO

Os documentos eletrônicos submetidos ao Arquivo devem seguir as políticas definidas no Acordo de Submissão. Estas são fruto de negociações entre os tabelionatos e o Arquivo, e definem os formatos dos dados aceitos (PSI) e como as sessões de submissão ocorrerão. Devem compreender o maior conjunto de informações possível a fim de dar maior celeridade às entregas dos documentos.

Salvo alterações no acordo de submissão, em princípio são emitidas duas confirmações ao tabelionato. A primeira no início do processo de submissão, e a última quando o documento e outras informações a ele vinculadas (PAI) estiverem sob a guarda de todos os locais de armazenamento vinculados ao tabelionato.

6.3.2 NORMALIZAÇÃO

Na microfilmagem, o conteúdo de um documento tradicional é, por meio de reprodução em filme, levado a um suporte mais apto a manter suas propriedades ao longo do tempo. Processo semelhante deve ser adotado na preservação dos documentos eletrônicos.

Obviamente, os atributos de um documento eletrônico, como a sua interpretabilidade, disponibilidade e valor jurídico, estão alicerçados de forma diferente àquela dos documentos tradicionais. Tais particularidades devem, portanto, ser devidamente entendidas e tratadas.

A conservação da interpretabilidade de um documento, ou seja, a possibilidade do mesmo ser compreendido num momento futuro, como visto na seção 4.3, depende de diversos fatores, dentre eles a possibilidade de ser contextualizado ao longo do tempo.

No Arquivo da CNSEC, a contextualização de um documento é alcançada por meio de metadados a ele anexados. Tais metadados seguem um vocabulário pré-definido próprio das serventias extrajudiciais, que tem por objetivo, além da contextualização do documento, dar-lhe maior rastreabilidade, e facilitar a geração de formulários e relatórios.

Outro fator necessário a interpretação do documento, como conceitua o Modelo de Referência OAIS, está na informação de representação, capaz de mapear os bits que o compõem em símbolos assimiláveis pela comunidade alvo – no caso, os tabeliães. Para os documentos eletrônicos, tal informação reside em seu formato.

Atualmente existe uma proliferação desses formatos, tais como o PDF, ODF e o OpenXML, e muitos deles possuem, potencialmente, dependências de software e hardware. Contudo, muitas dessas tecnologias desaparecem conforme as companhias mudam para novas linhas de produtos – sem compatibilidade com as versões antigas – ou até mesmo pela falência dessas companhias, o que constitui um sério problema a sua preservação em longo prazo.

Uma solução para esse problema está na migração na obsolescência – abordagem adotada pelo Arquivo Nacional do Reino Unido. Nesse caso, um formato atualmente adequado é escolhido, e posteriormente, quando o suporte ao mesmo for inviável, migram-se todos os documentos para um novo formato. Por exemplo, poder-se-ia utilizar o formato PDF/A, especialmente criado para esse fim, sendo autocontido, autodocumentado, e independente de dispositivo. Contudo, dada a dinamicidade do mercado, não há maiores garantias que o mesmo será suportado perpetuamente, e então a migração far-se-á necessária.

A natureza da informação das serventias extrajudiciais, entretanto, torna custoso tal procedimento. A eficácia probante que os documentos possuem depende da integridade dos mesmos, e a migração, como visto na seção 4.4.3, altera os bits que os compõem.

Tal fato implica na inutilização dos dados que garantem seu valor jurídico – estes não são válidos para o novo documento, e apesar de ainda o serem para o antigo, o mesmo tende a perder a interpretabilidade com o passar do tempo.

Nesse sentido, uma forma de atribuir eficácia jurídica ao novo documento seria a inclusão de metadados assinados pelo notário, onde seria realizado o ateste da validade de tais dados – como, por exemplo, carimbos do tempo e assinaturas digitais – no momento da conversão e, como defendido pelo projeto TransiDoc, a confirmação da preservação das informações contidas no documento, ou seja, sua continuidade semântica.

Tal abordagem é razoável para poucos documentos, porém, para um crescente e grande volume deles, torna-se inadequada.

Com isso em vista, a emulação surge como melhor alternativa. Tal estratégia baseia-se na imitação em nível de software, sistema operacional, ou hardware, da plataforma em que era possível visualizar um antigo formato. Por não alterar o documento em si, mas apenas o ambiente, tal estratégia é mais adequada à preservação da eficácia probante, uma vez que os

dados que a garantem não são invalidados.

Sabe-se, porém, que a emulação ainda é vista com certo ceticismo na literatura, e apesar de projetos como CAMiLEON e UVC terem produzidos provas de conceito sobre tal abordagem, ainda restam dúvidas sobre sua viabilidade em longo prazo. Este questionamento, por sua vez, origina-se na complexidade de construir tais emuladores, e no fato de que, uma vez construído, o mesmo também se torna objeto de obsolescência – necessitando um processo contínuo.

A escolha de um formato sem dependências arraigadas de sistema operacional e hardware certamente diminui tais esforços. Tomando o PDF/A novamente como exemplo, teoricamente, seria possível emulá-lo em nível de software, conservando a forma e conteúdo dos documentos, através do desenvolvimento continuado de visualizadores.

Contudo, tanto o PDF/A quanto outros formatos dão forma ao conteúdo do documento por meio de procedimentos complexos e que, se mal ou ambiguamente definidos em sua especificação, podem levar ao desenvolvimento de emuladores defeituosos. Defeitos esses que podem passar despercebidos por um longo período de tempo até que documentos específicos, fazendo uso de particularidades do formato, evidenciem-nos. Nesse caso, as informações de representação necessárias para a correção, como visualizadores da época em que o formato era amplamente utilizado, podem não mais existir, ou dependerem de plataformas computacionais ultrapassadas.

Os ganhos com tais procedimentos, em geral, justificam-se no uso diário do documento eletrônico. Entretanto, em longo prazo, tal característica apenas carrega complexidades que podem vir a comprometer a viabilidade de sua preservação de longo prazo.

Nesse sentido, o Arquivo da CNSEC, analogamente ao processo de microfilmagem, transporta conteúdo e forma do documento para um suporte mais adequado a preservação de longo prazo. No caso, imagens de mapas de bits, que se resumem à especificação da tonalidade de cada um dos pixels que as compõem, independentes de dispositivos.

Nesse processo de normalização, ilustrado na figura 27 em (1), cada uma das páginas do documento dá origem à uma imagem de mapa de bits.

A confiança nesse procedimento é alcançada de forma análoga à uma cópia autenticada, onde o notário autentica o novo documento afirmando tratar-se de uma reprodução fiel do documento original. Assim, como representado em (2), são apostos pelo tabelião, metadados onde se atesta:

- a continuidade semântica da conversão e obtenção da qualidade desejada;

Figura 27: Processo de normalização.

- a validade das assinaturas e/ou carimbos do tempo apostos no documento antigo, e a segurança dos algoritmos e parâmetros envolvidos, caso houver. Nesse caso, faz-se ainda necessária à adição de informações complementares, como, por exemplo, dados dos signatários.

Posteriormente, como ilustrado em (3), a fim de concluir o processo de autenticação, o conjunto formado pelas imagens e os atestes é assinado pelo notário. A formação desse conjunto, detalhado na figura 28, é alcançada pelo uso de Árvores de Resumos Criptográficos, já descrita na seção 4.4.

Igualmente, como visto na seção 4.4, nas formas avançadas de assinaturas digitais, ocorre a inclusão e protocolação das informações de validação necessárias a verificação futura da assinatura do notário, tais como os certificados do caminho de certificação, as LCR, e/ou as respostas OCSP. Possibilitando, assim, atribuir confiança em longo prazo no processo de normalização.

Por fim, como representando em (4), todos esses dados são encapsulados em um documento XML.

Além de oferecer suporte mais adequado para preservação de longo prazo da forma e conteúdo do documento original, o documento normalizado, como ilustrado na figura 28, possui as seguintes propriedades:

- é possível provar a autenticidade do documento normalizado como um todo e igualmente para uma página em específico. Tal característica é exemplificada na figura 29 para uma das páginas;
- a remoção, caso necessária, de alguma página do documento normalizado, apesar de

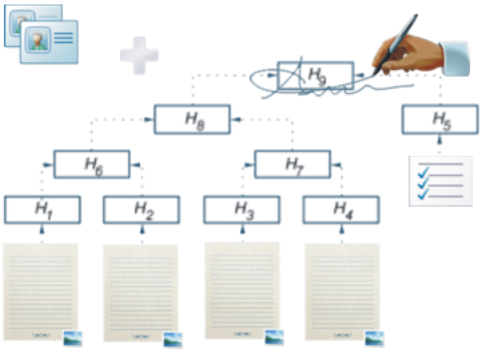

Figura 28: Documento normalizado.

visível, não interfere na possibilidade de comprovação da autenticidade das outras páginas.

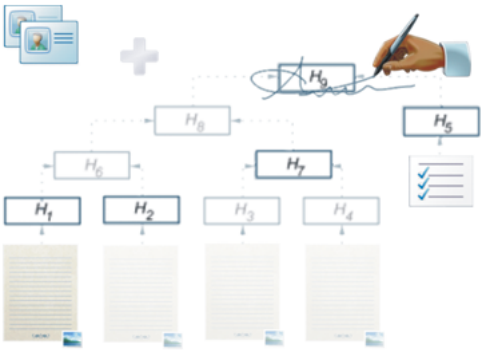

Figura 29: Página normalizada.

Caso seja de interesse do tabelião, o documento original e seus dados vinculados podem, igualmente, ser preservados. É provável que os mesmos percam sua interpretabilidade ao longo do tempo, contudo, em casos atípicos podem vir a servir de base à processos de Arqueologia Digital.

6.3.3 CLASSIFICAÇÃO

Os dados manipulados no ambiente do Arquivo da CNSEC são classificados e registrados junto à entidade funcional de Gerenciamento de Dados antes de serem enviados aos respectivos locais de armazenamento. Essa classificação identifica as tecnologias das quais os dados são dependentes, sejam elas de formato ou criptográficas, de modo a possibilitar a execução das medidas cabíveis a sua conservação.

Do mesmo modo, são registradas as regras de controle de acesso que devem ser aplicadas aos dados e em quais locais de armazenamento do tabelionato o mesmo será guardado.

Opcionalmente, podem ser vinculadas informações, providas pelo tabelião, que ajudem na preservação dos dados, como sua freqüência de uso esperado ou por quanto tempo o documento deve ser armazenado.

Por fim, as informações descritivas do documento, incluindo suas informações de contexto, são registradas seguindo o vocabulário de metadados das serventias, garantindo assim a rastreabilidade dos dados, detalhada na seção 6.5.

6.4 FORMATOS INTERNOS

Após a normalização, extração de metadados e classificação do documento, o pacote de arquivamento de informação (PAI), que cerra tais informações, deve ser armazenado. Nesta seção descreve-se a forma como ocorre a guarda desses dados e os procedimentos necessários a sua manutenção.

6.4.1 MONITORAMENTO TECNOLÓGICO

Os documentos eletrônicos sofrem da obsolescência induzida, fruto dos avanços constantes nas diversas áreas da computação. Tais problemas não se encerram no formato dos documentos, mas igualmente compreendem as tecnologias criptográficas que garantem sua proteção e eficácia probante. Além disso, não só os dados devem sobreviver, mas também o acesso a eles.

A entidade funcional Planejamento de Preservação monitora as tecnologias em uso no Arquivo da CNSEC, recomendando a Administração ações que devem ser tomadas a fim de garantir as propriedades desejadas aos documentos eletrônicos armazenados em longo prazo. Sua participação igualmente se dará em eventuais questões desconsideradas nessa proposta, como a inviabilidade de utilização dos formatos XML e imagens de mapa de bits. Nesse caso, sua colaboração compreende o desenvolvimento de protótipos, estratégias de preservação e planos de migração.

Suas recomendações, uma vez aceitas pela Administração, são publicadas periodicamente em formato XML – sendo processáveis por máquinas. Cada publicação informa o conjunto de tecnologias aceitas naquele momento. Portanto, apenas a última publicação é relevante para determinar se o uso de uma dada tecnologia é atualmente aconselhado. Para inferir a validade de uma tecnologia em uma data no passado, basta encontrá-la na publicação anterior à data. Somente são utilizados formatos e tecnologias criptográficas que já foram avaliadas. É interessante notar que apesar de seu escopo, a princípio, ser o Arquivo CNSEC, tais recomendações

podem ser úteis a toda a CNSEC.

No tocante as tecnologias criptográficas, estas são publicadas seguindo o Data Structure for Security Suitabilities of Cryptographic Algorithms (DSSC), especificado em Kunz, Okunick e Pordesch (2007), e baseiam-se em informações como aquelas disponibilizadas por entidades como NIST, ETSI e Federal Network Agency da Alemanha. No Arquivo são utilizados na avaliação das assinaturas, carimbos do tempo e informações de validação – entregues nas sessões de submissão, além de serem base para a criação de canais seguros de comunicação. Na CNSEC as mesmas informações podem ser utilizadas por aplicações estruturais como o Framework Notarial de Documento Eletrônico Confiável, Autoridade Certificadora Notarial, Autoridade de Carimbo do Tempo Notarial e Autoridade Certificadora Temporal Notarial.

Uma última responsabilidade da entidade Planejamento de Preservação refere-se ao aviso sobre eventos críticos que possam comprometer as funcionalidades esperadas ao Arquivo. Tais eventos serão avaliados pela Administração e poderão dar inicio a processos preventivos como o de Renovação de Tecnologia Criptográfica, detalhado na seção 6.4.2.

6.4.2 RENOVAÇÃO DE TECNOLOGIA CRIPTOGRÁFICA

A eficácia probante de um documento eletrônico, como visto na seção 4.4, baseia-se na garantia de certas propriedades do documento: em geral, a autenticidade e integridade. Ambas podem ser alcançadas por meio da aposição de assinaturas digitais, sendo esse o motivo pelo qual elas têm sido objetos de regulamentação ao redor do mundo – inclusive no Brasil, através da MP 2.200-2 de agosto de 2001. Contudo, diferentemente da assinatura manuscrita, a digital perde sua eficácia probante ao longo do tempo.

Indícios do problema podem ser acompanhados, por exemplo, no Projeto de Lei nº 1.589/99 da OAB/SP, acolhido pelo Substitutivo aprovado pela Comissão Especial de Comércio Eletrônico da Câmara dos Deputados, onde nos artigos 8º e 9º, declara-se:

> Art. 8º O juiz apreciará livremente a fé que deva merecer o documento eletrônico, quando demonstrado ser possível alterá-lo sem invalidar a assinatura, gerar uma assinatura eletrônica idêntica à do titular da chave privada, derivar a chave privada a partir da chave pública, ou pairar razoável dúvida sobre a segurança do sistema criptográfico utilizado para gerar a assinatura.
> Art. 9º Havendo impugnação de documento eletrônico incumbe o ônus da prova:
> I – à parte que produziu a prova documental, quanto à autenticidade da chave pública e quanto à segurança do sistema criptográfico utilizado;
> II – à parte contrária à que produziu a prova documental, quando alegar apropriação e uso da chave privada por terceiro, ou revogação ou suspensão das chaves.

Sabe-se que em longo prazo, os avanços nas áreas da criptografia e no poder computacional tendem a viabilizar a ocorrência de todos os problemas citados no artigo 8º. O primeiro deles, por exemplo, ocorre quando o algoritmo de resumo criptográfico utilizado na assinatura não é mais resistente à colisão; nesse caso seria possível alterar um documento eletrônico *m* para *m'*, onde $h(m) = h(m')$, sem invalidar a assinatura. Já o segundo e terceiro problemas, ocorrem quando o algoritmo de criptografia assimétrica, utilizado no processo de assinatura, não é mais seguro.

Mesmo que carimbos do tempo sejam utilizados para provar que a assinatura foi aposta enquanto as tecnologias criptográficas utilizadas eram válidas, os próprios carimbos, que no fim nada mais são que documentos eletrônicos assinados, também serão objetos dos mesmos problemas. Faz-se necessário um processo contínuo.

Nesse sentido, o Arquivo da CNSEC adota a solução proposta em agosto de 2007, pelo grupo de trabalho Long-Term Archive and Notary Services (LTANS), para não-repúdio da existência e integridade em longo prazo. O modelo, especificado em Gondrom, Brandner e Pordesch (2007) e já abordado na seção 4.4, foi engendrado para a realização de tal procedimento, de forma eficaz, em cenários onde é grande o volume de dados. Surgindo, portanto, como uma estratégia adequada às serventias extrajudiciais.

Assim, a garantia das propriedades das quais depende a eficácia probante de um documento eletrônico, armazenado em longo prazo, esta sujeita a apresentação de Registros de Evidência, cujas operações de Renovação de Carimbo do Tempo, e Renovação da Árvore de Resumo Criptográfico tenham sido realizadas em tempo hábil.

Tal constatação pode ser apoiada, por exemplo, nos documentos XML publicados pela entidade funcional Planejamento de Preservação, onde são expostos os períodos de validade das tecnologias criptográficas passadas ou atualmente recomendadas no Arquivo da CNSEC.

Há uma última questão ligada àqueles eventos cuja ocorrência é imprevisível, como o comprometimento da chave privada da Autoridade de Carimbo do Tempo ou a quebra repentina de algum algoritmo criptográfico utilizado. Nesse caso, não é possível provar que a renovação foi feita a tempo.

Desse modo, o Arquivo CNSEC, utiliza dois ou mais Registros de Evidência por unidade de dado protegido, cada qual com seus algoritmos de função resumo criptográfico, algoritmos de criptografia assimétrica, e Autoridades de Carimbo do Tempo, de forma que um registro garanta a segurança dos dados enquanto o outro é renovado frente a algum evento não previsto.

Em suma, os Registros de Evidência alcançam funcionalidade semelhante aos carimbos do

tempo, atestando a existência de um dado em um determinado momento, e a preservação de sua integridade desde então. Contudo, aqueles o fazem de maneira perpétua, sobrevivendo à inevitável obsolescência das tecnologias criptográficas envolvidas.

No Arquivo da CNSEC os mesmos são empregados para comprovar a validade das tecnologias criptográficas utilizadas na normalização do documento, no momento em que ela se deu. Permitindo, portanto, inferir a validade das assinaturas digitais do documento eletrônico, no momento em estas que foram apostas.

No processo, como visto na seção 4.4, uma Árvore de Resumos Criptográficos é construída e posteriormente reduzida. No caso, como ilustrado na figura 30, tem-se como folhas todos os dados do documento normalizado, descrito na seção 6.3.2, necessários a tal inferência, sendo estes: as imagens de mapas de bits, os atestes de conversão, a assinatura digital do tabelião aposta sobre esses dados, e as informações de validação devidamente protocoladas para a verificação de tal assinatura.

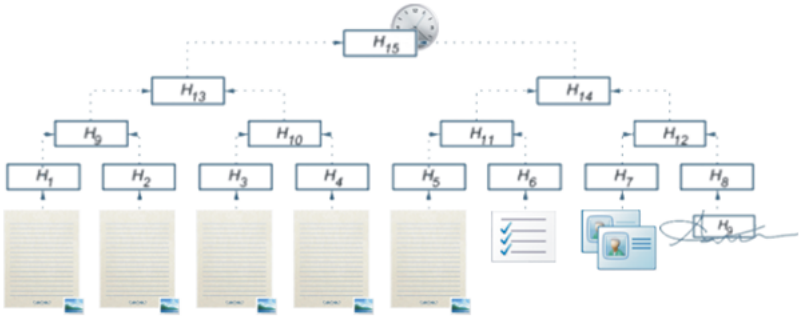

Figura 30: Não-repúdio de existência e integridade do documento em longo prazo.

Tal abordagem permite a redução da árvore para cada um desses dados e, por conseguinte a associação de um Registro de Evidência a cada um deles, possibilitando a sua verificação de forma individual, como exemplificado na figura 31. Uma última questão diz respeito a eliminação de qualquer um desses itens, que apesar de visível, não interfere na capacidade de validação dos outros.

6.4.3 LOCAIS DE ARMAZENAMENTO

Dentre os princípios norteadores da CNSEC, está a autonomia administrativa, onde os dados gerados pelas serventias são de sua propriedade e ficam sob sua responsabilidade. Esses dados são armazenados a critério de cada tabelionato, sendo possível a eles apontar um ou mais locais de guarda dos documentos.

Figura 31: Não-repúdio de existência e integridade da página em longo prazo.

Sendo assim, a manutenção da disponibilidade dos dados não fica a cargo do Arquivo da CNSEC. Contudo, são especificadas funcionalidades mínimas que cada local de armazenamento deve prover, e igualmente, são oferecidas recomendações a fim de facilitar suas operações. Além disso, como detalhado na seção 6.4.4, os PAI são projetados de modo a facilitar o armazenamento e preservação dos dados: atributos, como a freqüência esperada do documento, podem ser informados a cada submissão, facilitando a alocação adequada das mídias.

Essa flexibilidade, entretanto, requer tratamento adequado quanto à forma de referenciar cada PAI – seja para especificação de relacionamentos entre PAIs ou seja para seu registro junto à entidade funcional de Gerenciamento de Dados. Assim, no Arquivo da CNSEC, cada PAI possui uma referência única na sintaxe Uniform Resource Name (URN). Como descrito em Moats (1997): "URNs são concebidos a fim de servir como identificadores, persistentes e independentes de localização". Portanto, caracterizam-se como forma adequada de referência, dentro de um contexto onde a localização dos documentos tende a mudar ao longo do tempo, por fatores como a falência ou descontinuidade dos serviços prestados pelos locais de armazenamento. Esse nível de indireção igualmente faz-se necessário pelo fato de um mesmo arquivo ser replicado em diferentes locais.

Dentre suas responsabilidades, um local de armazenamento deve garantir a disponibilidade e integridade dos dados submetidos, independentemente de seu caráter ou conteúdo, preocupando-se apenas com a preservação dos octetos que o compõem. Igualmente, ao longo do tempo, deve seguir as indicações feitas pela Administração do Arquivo CNSEC, a fim de conservar a eficácia probante dos documentos armazenados, realizando, quando necessário, os processos de renovação de tecnologia criptográfica, detalhados na seção 6.4.2.

Recomenda-se que as entidades funcionais de Armazenamento estejam atentas às questões apontadas na seção 4.2, e realizem a renovação das mídias como detalhado na seção 6.4.4. Além disso, análises de risco, a exemplo da descrita em Constantopoulos, Doerr e Petraki (2005), de-

vem ser realizadas a fim de determinar o número de locais de armazenamento necessários frente à possibilidade de ocorrência de desastres naturais, como incêndios e enchentes. Igualmente, deve ser determinado o número de cópias necessárias de cada documento e o quão freqüente a integridade dessas cópias será checada. Tais esquemas de armazenamento para preservação de longo prazo devem ser periodicamente reavaliados, a fim de garantir a confiabilidade desejada e absorver evoluções tecnológicas na área.

6.4.4 RENOVAÇÃO DE MÍDIA

A ameaça mais fundamental da qual os documentos eletrônicos são alvo refere-se a sua perda ou corrupção, uma vez que os mesmos são armazenados em mídias as quais podem falhar devido à exposição ao calor, umidade, contaminação ou mesmo por falhas nos dispositivos de leitura e escrita. Outro fator relacionado a esse problema está na própria obsolescência desses dispositivos.

A fim de reduzir os riscos de corrupção e perda dos dados armazenados, algumas abordagens, como em Brown (2003a), estudam o controle das condições ambientais dos locais de armazenamentos; outras focam na cópia continuada dos dados para novas mídias antes da ocorrência de falha ou obsolescência das antigas – método conhecido como renovação de mídia (do inglês, refresh). Sua realização pode se dar periodicamente, ou com base em técnicas de detecção de erro.

Obviamente, o arranjo de mídias deve ser escolhido, de forma a suportar tal procedimento. Por exemplo, em uma configuração utilizando dois discos rígidos, onde o segundo mantém copias de todos os dados do primeiro, caso fosse detectada a falha total de um deles, seria possível a cópia dos dados do outro para um terceiro disco. Porém, fatores como o tempo entre a ocorrência da falha e sua detecção e o tempo gasto para a cópia dos dados para um novo disco, são cruciais. Caso não sejam adequados, o disco restante pode falhar antes que a recuperação tenha terminado, levando a perda dos dados.

É recomendável, portanto, que a infra-estrutura dos locais de armazenamento associados aos tabelionatos seja dimensionada levando em conta análises de risco, a exemplo da detalhada em Constantopoulos, Doerr e Petraki (2005), com o intuito de atingir, dentro de custos mínimos, a confiabilidade desejada.

A renovação de mídia, como visto, pode levar a cópia dos dados de uma mídia de tecnologia antiga para uma mais recente. Tal cópia pode, inclusive, envolver sistemas de arquivos diferentes, a exemplo do ISO 9660 para o ReiserFS. Por esse motivo, estruturas baseadas em

diretórios necessitariam migrar de um formato para outro.

Nesse sentido, o Pacote de Arquivamento da Informação (PAI) projetado para o Arquivo da CNSEC, encerra tais informações de estruturação – informação de empacotamento no Modelo de Referência OAIS – em um documento XML, encapsulando os dados necessários juntamente com seus nomes e tipos. Esta estratégia permite o tratamento desse conjunto como um bloco opaco de octetos, facilitando a migração.

6.5 ACESSO

Serviço fundamental a um arquivo, um sistema de busca eficiente é de grande importância em um ambiente onde a quantidade de documentos é substancialmente elevada. No Arquivo da CNSEC, todos os documentos são indexados e informações relevantes são capturadas a fim de facilitar as operações de consulta. Nesta seção são detalhados o sistema de busca e outros conceitos pertinentes à acessibilidade dos documentos eletrônicos nele armazenados.

6.5.1 ACORDO DE PEDIDO

O acesso aos documentos eletrônicos por meio do Arquivo da CNSEC deve seguir as políticas definidas no Acordo de Pedido. Este é fruto de negociações entre o Arquivo e os consumidores – em geral os tabelionatos, definindo assim o formato dos dados recebidos nas requisições e como tais requisições ocorrerão. Deve compreender o maior conjunto de informações possíveis a fim de dar maior celeridade ao recebimento dos documentos.

6.5.2 SISTEMA DE BUSCA

O acesso a um determinado documento ou informação associada no Arquivo da CNSEC dá-se mediante o conhecimento de sua referência URN ou por meio do sistema de busca.

Quanto a sua referência, esta é recebida no ato do depósito do documento, permitindo ao tabelião acompanhar as sucessivas etapas do processo de armazenagem.

O sistema de busca, por sua vez, provê um canal para a recuperação de pacotes de disseminação de informação (PDI), cuja referência do PAI não é conhecida a priori. Por este sistema é possível listar todos os documentos sob a guarda de um tabelião, ou um subconjunto deles, relacionados com determinadas palavras-chave. Tais palavras podem ser igualmente originadas por meio do preenchimento de formulários gerados a partir do vocabulário de metadados próprio das serventias.

Os operadores de busca, a princípio, procuram ocorrências das palavras-chave nas informações de contexto registradas na entidade funcional de Gerenciamento de Dados e provida pelo notário no momento do depósito. Entretanto, essas operações podem incluir a aplicação de tecnologias de reconhecimento óptico de caracteres (Optical Character Recognition – OCR) sobre as imagens, possibilitando a busca sobre seu conteúdo.

Ilustrando, um tabelião que procure um determinado testamento anteriormente armazenado, cujas informações de contexto – como nome completo do testador, números de CPF e RG, espécie e data do ato, livro e folhas em que foi lavrado – tenham sido registradas, poderá recuperá-lo provendo um subconjunto desses dados.

6.5.3 DADOS DISPONÍVEIS

Uma vez encontrado o documento, ou um conjunto deles, o notário determina as informações que lhe são relevantes. O Arquivo da CNSEC então constrói um Pacote de Disseminação da Informação (PDI) contendo os dados pedidos. Dentre as opções estão:

- o documento original, caso o tabelião tenha requisitado sua guarda;
- os Registros de Evidência que comprovam a manutenção da eficácia probante do documento original, caso o tabelião tenha requisitado sua guarda;
- o documento normalizado;
- os Registros de Evidência que comprovam a conservação da eficácia probante do documento normalizado.
- páginas do documento normalizado.
- atestes de conversão que autenticam tais páginas;
- registros de Evidência que comprovam a conservação da eficácia probante de tais páginas;
- outros dados associados ao documento, como informações de proveniência, contexto, referência.

Assim, dando continuação ao exemplo anterior, uma vez determinado o documento que contém a informação em questão, no caso o livro e as páginas em que o ato foi lavrado, o tabelião poderia requisitar tais páginas do documento normalizado, os dados necessários a comprovação de que estas foram autenticadas no processo de conversão e que a eficácia probante

das mesmas foi conservada desde seu depósito, respectivamente, seus atestes de conversão e seus Registros de Evidência.

6.5.4 MIGRAÇÃO NA REQUISIÇÃO

A normalização dos documentos, proposta na seção 6.3.2, possibilita a conservação da interpretabilidade dos documentos eletrônicos no contexto do Arquivo da CNSEC. Mesmo que o formato de imagem de mapas de bits nela utilizado venha a se tornar obsoleto, o desenvolvimento de emuladores para tal formato torna-se trivial.

Certidões e traslados digitais podem ser emitidos com base nessas informações normalizadas. Contudo, caso o usuário do serviço notarial venha a requisitar um documento arquivado em determinado formato, por exemplo, em PDF, é possível ao notário converter o documento normalizado para o formato desejado.

Tal migração deve ser devidamente autenticada, como acontece na normalização, e pode ser realizada por um conversor capaz de encapsular as imagens do documento normalizado no formato em questão.

6.6 CONCLUSÃO

Neste capítulo foi apresentado o Arquivo da Central Notarial de Serviços Eletrônicos Compartilhados. Mostrou-se sua compatibilidade com o modelo de referência OAIS e a distribuição das entidades funcionais seguindo o mesmo modelo.

A primeira seção tratou sobre o domínio, consumidores e produtores de dados. Na segunda seção discorreu-se sobre a entidade Admissão, ressaltando a importância do acordo de submissão e descrevendo os processos de normalização e classificação. A seção seguinte, Formatos Internos, exibiu-se os pontos mais relevantes do Arquivo da CNSEC: monitoramento tecnológico, renovação de tecnologia criptográfica, locais de armazenamento e renovação de mídia. Por último, destacou-se a entidade Acesso, acordo de pedido, sistema de busca, dados disponíveis e migração na requisição.

Percebe-se que a configuração selecionada para o Arquivo da CNSEC tenta ao máximo minimizar os transtornos causados com as mudanças decorrentes do perfil do mercado de TI. Aproveitando-se ao máximo utilizar de modo eficiente e proveitoso as tecnologias existentes a fim de facilitar o uso do sistema pelos tabeliães, que certamente não gostariam de serem incomodados sempre que uma tecnologia expirar, por exemplo, mesmo porque problemas dessa

natureza não fazem parte do seu escopo e deveriam ser tratados o mais automatizadamente possível.

7 CONSIDERAÇÕES FINAIS

Os documentos eletrônicos tiveram e ainda estão tendo seu uso intensificado. São vários os fatores que contribuem para essa expansão, como a popularização de sistemas computadorizados, Internet e demanda por serviços on-line. As serventias extrajudiciais, por se tratarem de serviços públicos, também estão sentindo esta demanda e como resposta, começaram a buscar soluções que as atendessem. A Central Notarial de Serviços Eletrônicos Compartilhados faz parte desta solução, concentrando o melhor em estratégias de negócio, tecnologias e segurança, provendo o ambiente necessário para que os serviços públicos delegados possam ser executados com o mesmo sucesso de hoje, trazendo ainda os benefícios dos documentos eletrônicos, a exemplo da disponibilidade.

Um dos módulos mais importantes, se não o mais, que compõem a central é o Arquivo. Qualquer objeto criado em uma época sofre a ação do tempo; no caso dos digitais essa "erosão" é muito mais rápida devido aos dinamismos do mercado de TI. Essa situação se agrava ainda mais com os documentos assinados, que precisam manter suas propriedades para ter eficácia probante. O Arquivo da CNSEC aparece como a resposta a esses problemas, sendo o suporte necessário para que a manutenção das características necessárias dos documentos eletrônicos.

Ao longo deste trabalho foram relembrados os fundamentos básicos da criptografia que tornaram possível os mecanismos de segurança implantados na CNSEC e seu Arquivo. Outro ponto importante abordado foi em relação a eficácia probante de um documento eletrônico, mostrando uma visão mais jurídica da situação e desfazendo algumas confusões que acontecem com características técnicas e jurídicas, a exemplo do não-repúdio. Em seguida foram vistas as técnicas e estratégias disponíveis na literatura para que as propriedades do documento eletrônico sejam mantidas. Também foram exibidos os potenciais problemas que decorrem do uso de uma técnica ou estratégia de preservação em longo prazo. Como "efeito colateral" pode-se citar a migração de formato de um documento: ao trocá-lo de um formato em obsolescência para outro atual tem-se a invalidação da assinatura digital, em razão de que a mesma é feita sobre o arquivo digital como um todo, carregando junto as informações que compõem o formato.

Um ponto de grande importância deste trabalho está no seu alinhamento, não só as recomendações dos padrões de interoperabilidade de governo eletrônico – o e-PING, mas também ao Modelo de Referência OAIS. Com este modelo tem-se uma arquitetura de alto nível para desenvolver um sistema de arquivamento, dividindo a infra-estrutura do arquivo em entidades funcionais, cada qual com seu respectivo papel associado. Outra contribuição trazida pelo modelo é a questão da nomenclatura, que torna mais fácil a comparação entre as várias implementações existentes, abrindo espaço para que diferentes sistemas arquivísticos troquem informações e melhorem seus serviços.

Um dos focos centrais é a Central Notarial de Serviços Eletrônicos Compartilhados. Elaborada com conceitos modernos que estão transformando o mundo dos negócios, a exemplo das abordagens de Central de Serviços Compartilhados – CSC e software como um serviço (Software as a Service – SaaS). Como sua finalidade é trazer interoperabilidade entre os vários serviços, a central tem como premissa básica as tecnologias relacionadas no e-PING. Além disso, visando dar credibilidade e aceitação ao modelo, foram levantados princípios (listados na tabela 1) junto aos tabeliães, que foram respeitados tanto na CNSEC, quanto em seu Arquivo, a exemplo da autonomia administrativa.

O ponto de convergência do presente trabalho é o Arquivo da Central Notarial de Serviços Eletrônicos Compartilhados, apresentado no capítulo 6. Utilizando-se do modelo de referência OAIS, propôs-se uma infra-estrutura a fim dar suporte ao uso de documentos eletrônicos em longo prazo. O Arquivo, entre outras obrigações, é responsável por receber, normalizar e manter documentos eletrônicos. No recebimento, um documento eletrônico sofre a normalização, sendo extraídas imagens de mapas de bits de cada página do documento que posteriormente são "amarradas" validadas e atestadas pelo notário. Os documentos arquivados sofrem constantes manutenções, por exemplo, renovações de mídia e tecnologias criptográficas. Com relação a estas tecnologias, as informações sobre validade e segurança serão buscadas de órgãos competentes, a exemplo do NIST.

O documento arquivado é encapsulado em um pacote chamado Pacote de Arquivamento de Informação (PAI), contendo o documento em si, metadados, proveniência e outras informações. É neste pacote que ocorrem as manutenções. O ETSI propôs como forma de manter todos os dados encapsulados e para manter suas propriedades o formato XAdES-A, especialmente desenvolvido para este caso. No entanto, o esforço computacional necessário para a manutenção, para cada um dos documentos arquivados, é bastante alto. Uma alternativa para fazer essa manutenção de modo mais eficiente foi proposta pelo grupo de trabalho LTANS – o registro de evidência, consistindo na formação de uma árvore de resumos criptográficos onde

somente a raiz recebe carimbos do tempo. Essa abordagem é bem eficiente, a não ser quando uma função de resumo criptográfico sofre obsolescência e precisa ser substituída. Utilizando-se dessas tecnologias, o Arquivo da CNSEC foi proposto pensando também na eficiência, uma vez que um grande volume de documentos deve circular pela estrutura. Essa eficiência vem do uso de um formato de assinatura avançada que possibilite anexar as informações de validação necessárias à verificação da assinatura ao longo do tempo, a exemplo do XAdES-X-L, combinado ao uso do registro de evidência, garantindo assim a manutenção das propriedades dos documentos eletrônicos para que os mesmos possam manter a eficácia probante.

O modelo do Arquivo da CNSEC, proposto nesse trabalho, preserva sobretudo a interpretabilidade, disponibilidade e eficácia probante do documento eletrônico, servindo bem a documentos públicos. Contudo, outros atributos, como o sigilo por longo prazo, devem ser estudados. Esta, por exemplo, é uma propriedade necessária para documentos que venham a ser guardados em locais de armazenamento não confiáveis. Sua conservação, entretanto, não é trivial, pois como um documento será armazenado por tempo indefinido, o atacante, igualmente, terá esse tempo para decifrá-lo. Outras questões que, do mesmo modo, carecem melhor tratamento, são a autenticação e controle de acesso de longo prazo, uma vez que um mesmo tabelionato é assumido por diferentes notários ao longo do tempo.

Enfim, a CNSEC e seu Arquivo, delineiam um horizonte que pode servir de rumo ao processo de integração e modernização das serventias extrajudiciais, oferecendo uma solução independente que respeita os princípios levantados; capaz de dar maior celeridade à prestação de serviços pelos cartórios, sem, contudo, desconsiderar ou mitigar as particulares dos documentos eletrônicos – seja no seu manuseio diário, seja no seu armazenamento de longo prazo.

REFERÊNCIAS

ADOBE SYSTEMS. *XMP Specification*. 2005. Disponível em: <http://partners.adobe.com/public/developer/en/xmp/sdk/XMPspecification.pdf>. Acesso em: 9 out. 2007.

ADOBE SYSTEMS. *Adobe Acrobat family*. 2007. Disponível em: <http://www.adobe.com/br/products/acrobat/adobepdf.html>. Acesso em: 9 out. 2007.

ANSPER, A. et al. *Efficient long-term validation of digital signatures*. [s.n.], 2001. Disponível em: <http://www.cyber.ee/dokumendid/additional/efficient.pdf>. Acesso em: 14 out. 2007.

BEAGRIE, N.; JONES, M. *Preservation Management of Digital Materials*: a handbook. London, 2002. Disponível em: <http://www.dpconline.org/graphics/handbook>. Acesso em: 19 out. 2007.

BLAZIC, A. J.; SYLVESTER, P.; WALLACE, C. *Long-term Archive Protocol (LTAP)*. 2007. Disponível em: <http://www.ietf.org/internet-drafts/draft-ietf-ltans-ltap-05.txt>. Acesso em: 14 out. 2007.

BORSTEIN, R. *PDF/A*: Pdf for archving. [s.n.], 2007. Disponível em: <http://blogs.adobe.com/acrolaw/2007/01/pdfa_pdf_for_ar.html>. Acesso em: 8 out. 2007.

BRASIL. *Lei nº 8.935, de 18 de novembro de 1994*. Poder Executivo, Brasília, DF, 1994. Disponível em: <http://www.planalto.gov.br/ccivil/leis/L8935.htm>. Acesso em: 25 jun. 2007.

BRASIL. *Medida provisória nº 2.200-2, de 24 de agosto de 2001*. Poder Executivo, Brasília, DF, 2001. 65 p. Disponível em: <http://www.planalto.gov.br/ccivil/mpv/Antigas_2001/2200-2.htm>. Acesso em: 24 jun. 2007.

BRASIL. *Lei nº 11.280, de 16 de fevereiro de 2006*. Poder Executivo, Brasília, DF, 2006. Disponível em: <http://www.planalto.gov.br/ccivil/_Ato2004-2006/2006/Lei/L11280.htm>. Acesso em: 24 jun. 2007.

BRASIL. *Lei nº 11.419, de 19 de dezembro de 2006*. Poder Executivo, Brasília, DF, 2006. Disponível em: <http://www.planalto.gov.br/ccivil/_Ato2004-2006/2006/Lei/L11419.htm>. Acesso em: 24 jun. 2007.

BROWN, A. *Digital Preservation Guidance Note 3*: Care, handling and storage of removable media. [s.n.], 2003. Disponível em: <http://www.nationalarchives.gov.uk/documents/media_care.pdf>. Acesso em: 15 out. 2007.

BROWN, A. *Selecting File Formats for Long-Term Preservation*. [s.n.], 2003. Disponível em: <http://www.nationalarchives.gov.uk/documents/selecting_file_formats.pdf>. Acesso em: 6 out. 2007.

BUENO, F. da S. *Dicionário Escolar da Língua Portuguesa*. 11. ed. Rio de Janeiro: [s.n.], 1992.

CENTRAL de Escrituras e Procurações. [s.n.]. Disponível em: <http://www.notarialnet.org.br/ex_not_pesq.php?codigo=1697>. Acesso em: 30 jun. 2007.

CENTRAL de Sinais Públicos. [s.n.]. Disponível em: <http://www.cartorios.com.br>. Acesso em: 30 jun. 2007.

COMITê EXECUTIVO DE GOVERNO ELETRôNICO. *e-PING*: Padrões de interoperabilidade de governo eletrônico. Disponível em: <https://www.governoeletronico.gov.br/acoes-e-projetos/e-ping-padroes-de-interoperabilidade>. Acesso em: 24 jun. 2007.

CONGRESSO NOTARIAL BRASILEIRO, 14., 2007, São Paulo. *Conclusões do tema 1*: A escritura pública eletrônica.

CONSTANTOPOULOS, P.; DOERR, M.; PETRAKI, M. *Reliability modelling for long term digital preservation*. [s.n.], 2005. Disponível em: <http://www.ics.forth.gr/isl/publications/paperlink/Reliabilityg.pdf>. Acesso em: 14 out. 2007.

COSTA, M. *Validade jurídica e valor probante de documentos eletrônicos*. [s.n.], 2003. Disponível em: <http://www.cic.unb.br/ pedro/trabs/validade.html>. Acesso em: 8 out. 2007.

CUNNINGHAM, A. Recent developments in standards for archival description and metadata. In: INTERNATIONAL SEMINAR ON ARCHIVAL DESCRIPTIVE STANDARDS, UNIVERSITY OF TORONTO, 2001. 2001. Disponível em: <https://archivists.org.au/recent-developments-standards-archival-description-and-metadata>. Acesso em: 20 out. 2007.

CYPHER RESEARCH LABORATORIES. *A Brief History of Cryptography*. Cairns, Australia, 2006. Disponível em: <http://www.cypher.com.au/crypto_history.htm>. Acesso em: 12 out. 2007.

DECLARAçãO sobre Operações Imobiliárias. [s.n.]. Disponível em: <http://www.receita.fazenda.gov.br/principal/Informacoes/InfoDeclara/declaraDOI.htm>. Acesso em: 30 jun. 2007.

DEJANE, L. B. *O documento eletrônico no Ofício de Registro Civil de Pessoas Naturais*. 93 f. Dissertação (Mestrado em Ciência da Computação) — Curso de Pós-Graduação em Ciência da Computação, Universidade Federal de Santa Catarina, Florianópolis, 2002.

DEMéTRIO, D. B. *Infra-estrutura para Protocolização Digital de Documentos Eletrônicos*. 140 f. Dissertação (Mestrado em Ciência da Computação) — Curso de Pós-Graduação em Ciência da Computação, Universidade Federal de Santa Catarina, Florianópolis, 2003.

DIAS, J. S. *Confiança no Documento Eletrônico*. 141 f. Tese (Doutorado em Engenharia de Produção) — Curso de Pós-Graduação em Engenharia de Produção, Universidade Federal de Santa Catarina, Florianópolis, 2004.

DINAMARCO, C. R. *Instituições de Direito Processual Civil*. 2. ed. [S.l.: s.n.].

DOBBERTIN, H. *Cryptanalysis of MD5 Compress*. 1996. Disponível em: <http://www.cs.ucsd.edu/users/bsy/dobbertin.ps>. Acesso em: 14 out. 2007.

EASTLAKE, D.; JONES, P. *US Secure Hash Algorithm 1 (SHA1)*. 2001. Disponível em: <http://www.ietf.org/rfc/rfc3174.txt>. Acesso em: 16 out. 2007.

EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE. *XML Advanced Electronic Signatures (XAdES)*. 2006. Disponível em: <http://pda.etsi.org/pda/home.asp?wki_id=fbH-@i8BNxcedfhfJVWlS>. Acesso em: 15 out. 2007.

EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE. *CMS Advanced Electronic Signatures (CAdES)*. 2007. Disponível em: <http://pda.etsi.org/pda/home.asp?wki_id=o-ZaOAEGBDhjliony'1wX>. Acesso em: 15 out. 2007.

FEDERAL MINISTRY OF ECONOMICS AND TECHNOLOGY. *Transidoc Project*. 2004. Disponível em: <http://www.transidoc.de>. Acesso em: 17 out. 2007.

FEISTEL, H. Cryptography and computer privacy. Scientific American, v. 228, n. 5, p. 15–23, mai. 1973. Disponível em: <http://www.apprendre-en-ligne.net/crypto/bibliotheque/feistel/index.html>. Acesso em: 16 out. 2007.

FILLINGHAM, D. *A Comparison of Digital and Handwritten Signatures*. [s.n.], 1997. Disponível em: <http://www-swiss.ai.mit.edu/6805/student-papers/fall97-papers/fillingham-sig.html>. Acesso em: 30 nov. 2007.

FURRIE, B. *Understanding MARC Bibliographic*: Machine-readable cataloging. [s.n.], 2003. Disponível em: <http://www.loc.gov/marc/umb/>. Acesso em: 9 out. 2007.

GANDINI, J. A. D.; JACOB, C.; SALOMãO, D. P. da S. *A Validade jurídica dos documentos digitais*. Santa Maria - RS, 2001. Disponível em: <http://www.ufsm.br/direito/artigos/informatica/validade.htm>. Acesso em: 8 out. 2007.

GILHEANY, S. Preserving information forever and a call for emulators. In: DIGITAL LIBRARIES ASIA 98: THE DIGITAL ERA: IMPLICATIONS, CHALLENGES & ISSUES, 1998, Singapore. 1998. p. 12. Disponível em: <http://www.archivebuilders.com/pdf/22010v052.pdf>. Acesso em: 17 out. 2007.

GONDROM, T.; BRANDNER, R.; PORDESCH, U. *Evidence Record Syntax (ERS)*. 2007. Disponível em: <http://www.ietf.org/rfc/rfc4998.txt>. Acesso em: 14 out. 2007.

HESLOP, H.; DAVIS, S.; WILSON, A. *An Approach to the Preservation of Digital Records*. 2002. Disponível em: <http://www.naa.gov.au/Images/An-approach-Green-Paper_tcm2-888.pdf>. Acesso em: 5 out. 2007.

HOUSLEY, R. et al. *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. 2002. Disponível em: <http://www.ietf.org/rfc/rfc3280.txt>. Acesso em: 17 out. 2007.

INTERNATIONAL BUSINESS MACHINES. *SOFTWARE as a Service*: A growth opportunity for software providers. 2007. Disponível em: <http://www-304.ibm.com/jct09002c/isv/mem/saas/saas_growth.pdf>. Acesso em: 30 jun. 2007.

JúNIOR, I. T. G. *O Conceito de Documento Eletrônico*. Belo Horizonte, 2000.

KUNZ, T.; OKUNICK, S.; PORDESCH, U. *Data Structure for Security Suitabilities of Cryptographic Algorithms (DSSC)*. 2007. Disponível em: <http://www.ietf.org/internet-drafts/draft-ietf-ltans-dssc-00.txt>. Acesso em: 14 out. 2007.

KUSBICK, L. J. B. *A Desmaterialização do Documento Papel*: Análise do requisito de segurança para a validade legal dos documentos eletrônicos. 26 f. Monografia (Especialização em Redes de Computadores) — Programa de Pós-Graduação em Ciência da Computação, Universidade Federal de Santa Catarina, Foz do Iguaçu, 2002.

LABORATóRIO DE TECNOLOGIAS DE GESTãO. *Central Registral de Serviços Eletrônicos Compartilhados*: O papel dos registradores no século xxi. [S.l.], 2007. 66 p.

LEKKAS, D.; GRITZALIS, D. *Cumulative Notarization for Long-term Preservation of Digital Signatures*. 2004. Disponível em: <http://www.syros.aegean.gr/users/lekkas/pubs/j/2004COMPSEC.pdf>. Acesso em: 14 out. 2007.

LORIE, I. R. *the UVC*: a method for preserving digital documents. 2002. Disponível em: <http://www.kb.nl/hrd/dd/dd_onderzoek/reports/4-uvc.pdf>. Acesso em: 9 out. 2007.

MCLELLAN, E. P. *Selecting Digital File Formats for Long-Term Preservation*. 2006. Disponível em: <http://www.interpares.org/display_file.cfm?doc=ip2_file_formats(complete).pdf>. Acesso em: 6 out. 2007.

MELLOR, P.; WHEATLEY, P.; SERGEANT, D. *Migration on Request*: A pratical technique for preservation. 2002. Disponível em: <http://www.si.umich.edu/CAMILEON/reports/migreq.pdf>. Acesso em: 5 out. 2007.

MERKLE, R. *Protocols for Public Key Cryptosystems*. [S.l.: s.n.], 1980. 122-134 p.

MOATS, R. *URN Syntax*. 1997. Disponível em: <http://www.ietf.org/rfc/rfc2141.txt?number=2141>. Acesso em: 14 out. 2007.

NATIONAL INFORMATION STANDARDS ORGANIZATION. *The Dublin Core Metadata Element Set*. 2007. Disponível em: <http://www.niso.org/standards/standard_detail.cfm?std_id=725>. Acesso em: 9 out. 2007.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *Secure Hashing*. 2007. Disponível em: <http://csrc.nist.gov/groups/ST/toolkit/secure_hashing.html>. Acesso em: 14 out. 2007.

NOTOYA, A. E. *IARSDE*: Infra-estrutura de armazenamento e recuperação segura de documentos eletrônicos. 110 f. Dissertação (Mestrado em Ciência da Computação) — Curso de Pós-Graduação em Ciência da Computação, Universidade Federal de Santa Catarina, Florianópolis, 2002.

ORGANIZATION FOR THE ADVANCEMENT OF STRUCTURED INFORMATION STANDARDS. *The Advantages of the OpenDocument Format (ODF)*. 2006. Disponível em: <http://www.oasis-open.org/committees/download.php/21450/oasis_odf_advantages_10dec2006.pdf>. Acesso em: 9 out. 2007.

PARADIGM PROJECT. *Workbook on Digital Private Papers*. 2007. Disponível em: <http://www.paradigm.ac.uk/workbook/preservation-strategies/08_digital_preservation-20070604.pdf>. Acesso em: 6 out. 2007.

PARENTONI, L. N. *A regulamentação legal do documento eletrônico no Brasil*. Teresina, 2005. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=7154>. Acesso em: 13 out. 2007.

PASQUAL, E. S. *IDDE*. 110 f. Dissertação (Mestrado em Ciência da Computação) — Curso de Pós-Graduação em Ciência da Computação, Universidade Federal de Santa Catarina, Florianópolis, 2002.

REGISTRO Central de Testamentos On-line. [s.n.]. Disponível em: <http://www.notarialnet.org.br/his.htm>. Acesso em: 30 jun. 2007.

SCHWEICKERT, C. L. *Binary Numbers and Their History*. 2000. Disponível em: <http://www.gowcsd.com/master/ghs/math/furman/binary/index.htm>. Acesso em: 9 out. 2007.

SHANNON, C. Communication theory of secrecy systems. Bell Systems Technical Journal, n. 4, 1949. Disponível em: <http://netlab.cs.ucla.edu/wiki/files/shannon1949.pdf>. Acesso em: 16 out. 2007.

STALLINGS, W. *Cryptography and Network Security Principles and Practices*. 4. ed. [S.l.]: Prentice Hall, 2005. 592 p.

THE COMMISSION ON PRESERVATION AND ACCESS AND THE RESEARCH LIBRARIES GROUP. *Preserving Digital Information*: Report of the task force on archiving of digital information. 1996. Disponível em: <http://www.oclc.org/programs/ourwork/past/digpresstudy/final-report.pdf>. Acesso em: 17 out. 2007.

THE LIBRARY OF CONGRESS. *Metadata Object Description Schema (MODS)*. 2007. Disponível em: <http://www.loc.gov/standards/mods/>. Acesso em: 9 out. 2007.

THOMAZ, K. de P. *A Preservação de Documentos Eletrônicos de Caráter Arquivístico*: Novos desafios, velhos problemas. 388 f. Tese (Doutorado em Ciência da Informação) — Programa de Pós-graduação em Ciência da Informação, Escola de Ciência da Informação, Universidade Federal de Minas Gerais, Belo Horizonte, 2004.

WALLACE, C. *Long-Term Archive Service Requirements*. 2007. Disponível em: <http://www.ietf.org/rfc/rfc4810.txt>. Acesso em: 14 out. 2007.

WALLACE, C. *Using SCVP to Convey Long-term Evidence Records*. 2007. Disponível em: <http://www.ietf.org/internet-drafts/draft-ietf-ltans-ers-scvp-03.txt>. Acesso em: 14 out. 2007.

WILSON, A. *Significant Properties Report*. [s.n.], 2007. Disponível em: <http://www.significantproperties.org.uk/documents/wp22_significant_properties.rtf>. Acesso em: 5 out. 2007.

WORLD WIDE WEB CONSORTIUM. *Extensible Markup Language (XML)*. 1998. Disponível em: <http://www.w3.org/XML/>. Acesso em: 9 out. 2007.

WORLD WIDE WEB CONSORTIUM. *Resource Description Framework (RDF)*. 2004. Disponível em: <http://www.w3.org/RDF>. Acesso em: 21 out. 2007.