UNIVERSIDADE FEDERAL DE SANTA CATARINA
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

Vanessa Costa

Um Estudo da Confiabilidade do Sistema de Protocolação Digital de Documentos Eletrônicos

Dissertação submetida à Universidade Federal de Santa Catarina como parte dos requisitos para a obtenção do grau de Mestre em Ciência da Computação.

Prof. Ricardo Felipe Custódio, Dr.
Orientador

Florianópolis, Dezembro de 2003

Um Estudo da Confiabilidade do Sistema de Protocolação Digital de Documentos Eletrônicos

Vanessa Costa

Esta Dissertação foi julgada adequada para a obtenção do título de Mestre em Ciência da Computação, área de concentração Sistemas de Computação e aprovada em sua forma final pelo Programa de Pós-Graduação em Ciência da Computação.

Prof. Raul Sidnei Wazlawick, Dr.
Coordenador do Curso

Banca Examinadora

Prof. Ricardo Felipe Custódio, Dr.
Orientador

Prof. Ricardo Dahab, Dr.

Prof. Daniel Santana de Freitas, Dr.

Prof. Jeroen Antonius Maria van de Graaf, Dr.

Prof. Carlos Roberto De Rolt, Dr.

"Dias de calmaria, noites de ardentia, dedos no leme e olhos no horizonte, descobri a alegria de transformar distâncias em tempo. Um tempo em que aprendi a entender as coisas do mar, a conversar com as grandes ondas e não discutir com o mal tempo. A transformar o medo em respeito, o respeito em confiança. Descobri como é bom chegar quando se tem paciência. E para se chegar, onde quer que seja, aprendi que não é preciso dominar a força, mas a razão. É preciso antes de mais nada, querer."
Amyr Klink

Ofereço à minha família, Márcio, Nazide, Soraya e Rodrigo, e ao meu noivo, Andrei.

Agradecimentos

A Deus, por ter me concedido a vida e por ter permitido que eu conquistasse mais uma vitória.

À minha família, pela educação, pelos princípios e pela formação moral que têm sido a base de todas as minhas conquistas.

Ao meu noivo, Andrei, pelo apoio, pela paciência e pela compreensão.

Aos colegas do LabSEC, especialmente às amigas Debora e Denise.

À secretária do Curso de Pós-Graduação, Verinha.

Aos acadêmicos Cleyton e Marcos, pela cooperação no desenvolvimento do protótipo de auditoria.

À empresa BRy Tecnologia.

Agradeço também ao meu orientador, professor Ricardo Felipe Custódio, por ter me ajudado a vencer este desafio.

E, finalmente, aos membros da banca do Trabalho Individual e da dissertação, pela colaboração.

Sumário

Lista de Figuras

Lista de Siglas

AC	Autoridade Certificadora
AD	Autoridade de Datação
AGDDE	Autoridade de Gerenciamento de Depósitos de Documentos Eletrônicos
AGT	Autoridade de Garantia de Tecnologia
AR	Autoridade de Registro
ATR	Autenticação Temporal Relativa
BIPM	*Bureau International des Poids et Mesures*
CC	Cadeia de Certificação
CSP	*Critical Security Parameter* (Parâmetro de Segurança Crítica)
DPP	Declaração de Práticas de Protocolação
GMT	*Greenwich Mean Time* (Tempo Médio de *Greenwich*)
GPS	*Global Positioning System* (Sistema de Posicionamento Global)
HSM	*Hardware Security Modules* (Módulos Seguros de *Hardware*)
IARSDE	Infra-estrutura de Armazenamento e Recuperação Segura de Documentos Eletrônicos
ICP-Brasil	Infra-estrutura de Chaves Públicas Brasileira
IETF	*Internet Engineering Task Force* (Força Tarefa de Engenharia na *Internet*)
LabSEC	Laboratório de Segurança em Computação
LCR	Lista de Certificados Revogados
MP	Medida Provisória
NIST	*National Institute of Science and Technology* (Instituto Nacional de Ciência e Tecnologia)

NMI	*National Measurement Institutes* (Institutos Nacionais de Medida)
NPL	*National Physical Laboratory* (Laboratório Nacional de Física)
NTP	*Network Time Protocol* (Protocolo de Tempo da Rede)
OAB	Ordem de Advogados do Brasil
ON	Observatório Nacional
PDDE	Protocoladora Digital de Documentos Eletrônicos
PTB	*Physikalisch Technische Bundesanstalt* (Instituto Federal Técnico de Física)
PIN	*Personal Identification Number* (Número de Identificação Pessoal)
PL	Projeto de Lei
PP	Política de Protocolação
RFC	*Request For Comments* (Solicitação de Comentários)
RSA	Rivest-Shamir-Adleman
SSL	*Secure Sockets Layer* (Camada de *Sockets* Seguros)
TSA	*Time-Stamping Authority* (Autoridade de Datação)
TSP	*Time-Stamping Protocol* (Protocolo de Protocolação)
UNCITRAL	Comissão das Nações Unidas para Leis de Comércio Internacional
UFSC	Universidade Federal de Santa Catarina
UTC	*Coordinated Universal Time* (Tempo Universal Coordenado)

Lista de Símbolos

C_i	i-ésimo Ponto de Confiança.
D_i	i-ésimo documento protocolado.
$H(x)$	Resumo criptográfico do documento x.
ID_i	Identificador do documento.
KU_{Alice}	Chave pública de Alice.
L_i	i-ésimo *link* do encadeamento.
n	Número de *links* em um encadeamento.
R_i	i-ésima rodada do encadeamento.
s_i	i-ésimo recibo de protocolação.
S_i	i-ésimo Ponto de Salto.
$sig_{AD}(p)$	Assinatura digital da AD sobre o documento p.
t_i	Data e hora em que o documento foi protocolado.
Z_i	i-ésimo Ponto de Sincronismo.

Resumo

As técnicas utilizadas na protocolação digital de documentos eletrônicos não garantem que o sistema de protocolação seja completamente confiável. Devido a isso, as datas dos documentos protocolados podem ser alteradas, e, conseqüentemente, a tempestividade, um dos requisitos necessários para que um documento eletrônico tenha eficácia jurídica, não é atendida. Com o objetivo de aumentar a confiança provida pelos sistemas de protocolação digital, este trabalho propõe alguns mecanismos, tais como: procedimentos de auditoria, os quais possibilitam a fiscalização do funcionamento da Autoridade de Datação (AD), a elaboração de uma Política de Protocolação, na qual estão apresentados os procedimentos que a AD deve adotar para oferecer um serviço confiável, e a elaboração de um documento chamado Declaração de Práticas de Protocolação, no qual é descrito como a AD executa os procedimentos citados na Política de Protocolação. Utilizando os mecanismos propostos, a AD será mais confiável e, portanto, poderá ser utilizada como componente básico para o atendimento de requisitos de segurança de outros protocolos e aplicações.

Palavras-chaves: confiança, protocolação e documento eletrônico.

Abstract

The techniques used in the digital time-stamping of electronic documents do not assure completely the trust of the system. Due to this, the date in time-stamped documents can be modified, and, consequently, the temporal question, which is one of the requirements to consider in an electronic document legally valid, is not met. In order to improve the trust provided by the digital time-stamping systems, this paper proposes some mechanisms, such as: audit procedures, which inspect the Time-Stamping Authority (TSA) work, the elaboration of a Time-Stamping Policy, in which the procedures that the TSA should adopt to provide a trustworthy service are presented, and the elaboration of a document called Declaration of Practices of Time-Stamping, which describes how the TSA executes the procedures mentioned in the Time-Stamping Policy. By using the mechanisms proposed, the TSA will be more trustworthy and could be used as a basic component to meet the security requirements of other protocols and applications.

Keywords: trust, time-stamping and electronic document.

Capítulo 1

Introdução

O avanço da informática e a disseminação das redes de computadores possibilitaram a realização de transações eletrônicas em larga escala. Tais transações são realizadas através da troca de documentos eletrônicos entre entidades e abrangem diferentes atividades, como, por exemplo, transações comerciais, fechamento de acordos e contratos. Os documentos eletrônicos apresentam uma série de vantagens em relação aos documentos em papel, visto que ocupam pouco espaço, são fáceis de gerir e podem ser copiados e transmitidos quase que instantaneamente, tornando, assim, as transações muito mais ágeis. No entanto, para que sejam legalmente válidos, devem apresentar algumas propriedades, as quais já estão presentes nos documentos em papel:

- **Autenticidade:** correspondência entre o autor indicado e o autor real do documento;
- **Integridade:** possibilidade de verificar se o conteúdo de um documento foi alterado;
- **Tempestividade:** identificação e preservação da data do documento.

Diante disso, faz-se necessária uma mudança no conceito de documento, de forma a adaptá-lo ao meio digital, atribuindo-lhe a mesma confiança já consolidada no meio papel (MARCACINI, 2000). Através da assinatura digital, os requisitos autenticidade e integridade são atendidos. Para obter a tempestividade, os documentos eletrônicos

devem ser protocolados digitalmente. Documentos eletrônicos protocolados e assinados podem ser utilizados em situações de disputa, tais como: na comprovação de que um documento foi assinado antes da revogação do certificado digital ou do comprometimento da chave privada; na comprovação de que uma proposta comercial foi entregue dentro de um prazo definido em um edital de licitação, ou ainda, na resolução de disputas por patente ou propriedade intelectual.

Normalmente, a assinatura digital consiste em uma seqüência de códigos resultante da aplicação de um algoritmo criptográfico sobre o resumo do documento, utilizando a chave privada do assinante. Este é o caso, quando se utiliza o algoritmo RSA e resumos criptográficos MD5 ou SHA-1 (STINSON, 2002; MENEZES; OORSCHOT; VANSTONE, 1999) em protocolos como S/Mime (DUSSE, 1998a, 1998b), IPSec (KENT; ATKINSON, 1998) e SSL (NETSCAPE, 2003; DIERKS; ALLEN, 1999). Percebe-se que a protocolação, nestas aplicações e em muitas outras, é colocada em segundo plano, muitas vezes nem aparecendo como informação no documento assinado. A protocolação, no entanto, é um dos elementos chaves para a validação do documento eletrônico, visto que sem ela, não é possível verificar se um certificado digital estava válido no momento da assinatura digital.

1.1 Definição do Problema

Atualmente existem várias empresas que prestam o serviço de protocolação digital de documentos eletrônicos. Contudo, as técnicas existentes não garantem que o sistema de protocolação seja completamente confiável. Assim, a Autoridade de Datação (AD), entidade responsável pela protocolação do documento eletrônico, poderia agir de maneira maliciosa, protocolando os documentos com datas incorretas ou alterando-as após a protocolação. Porém, a data do documento ou a ordem em que os documentos foram protocolados são informações essenciais em casos como uma disputa por direito autoral, por exemplo. Diante deste problema, novos mecanismos devem ser desenvolvidos para fiscalizar o correto funcionamento da AD, garantindo, assim, a confiança do sistema de protocolação digital.

1.2 Objetivos

1.2.1 Objetivo Geral

Propor procedimentos que proporcionem maior confiança ao sistema de protocolação digital de documentos eletrônicos.

1.2.2 Objetivos Específicos

Entre os objetivos específicos, estão:

- Esclarecer de maneira didática e detalhada o Método da Árvore Sincronizada;
- Identificar os aspectos relevantes da confiança em um sistema de protocolação digital de documentos eletrônicos;
- Definir procedimentos de auditoria que permitam verificar se a AD agiu honestamente durante as protocolações;
- Propor um documento contendo uma Política de Protocolação;
- Analisar a confiabilidade de uma infra-estrutura distribuída de protocolação digital;
- Propor um documento contendo uma Declaração de Práticas de Protocolação.

1.3 Materiais e Métodos

Este trabalho é uma dissertação de mestrado, a qual, segundo o Dicionário Aurélio (1999), "é um trabalho escrito, apresentado a instituição de ensino superior, e defendido, publicamente, por candidato ao grau de mestre".

De acordo com Gil (1988, p.48), pesquisa bibliográfica deve ser "desenvolvida a partir de material já elaborado, constituído principalmente de livros e artigos científicos". Para realizar esta pesquisa, foram utilizados, além de livros e de artigos científicos, outras informações, tais como, dissertações de mestrado, teses de doutorado e leis, com a finalidade de coletar dados que proporcionassem soluções ao problema proposto.

Para complementar o caráter teórico das revisões bibliográficas, foram realizados alguns experimentos práticos de protocolação de documentos eletrônicos. Para tanto, foi utilizado um *software* cliente, disponibilizado pela empresa BRy (BRY, 2003), o qual calcula o resumo de um determinado documento eletrônico e envia uma requisição de protocolação para uma Autoridade de Datação.

Além disso, foram realizadas visitas à seção de protocolo da reitoria da UFSC, para melhor entender o funcionamento de um sistema de protocolação de documentos em papel. Isto forneceu subsídios para comparar a confiança fornecida pela protocolação de documentos em papel com a fornecida pela protocolação de documentos eletrônicos.

1.4 Trabalhos Correlacionados

Há aproximadamente dez anos a única maneira de protocolar documentos eletrônicos era através da utilização de uma Autoridade de Datação - AD, a qual utilizava um método de datação absoluta e precisava ser completamente confiável. Em 1991, Haber e Stornetta publicaram um artigo no qual afirmavam que a necessidade de se confiar na AD poderia ser reduzida através da utilização de um método de datação chamado Encadeamento Linear. A partir daí, vários trabalhos foram publicados, propondo melhorias ao esquema. O trabalho de maior importância na área, no entanto, apareceu somente em 1998 devido a Buldas. Em 2001, foi proposta uma RFC (ADAMS, 2001) que especifica o protocolo de comunicação entre o cliente e a Autoridade de Datação. Em 2002, foi proposto o Método da Árvore Sincronizada (PASQUAL; DIAS; CUSTÓDIO, 2002), além de estabelecer-se os alicerces do sistema de protocolação denominado Protocoladora Digital de Documentos Eletrônicos - PDDE (PASQUAL, 2001). Em 2002, foi proposta uma Infra-estrutura de Armazenamento e Recuperação Segura de Documentos Eletrônicos - IARSDE (NOTOYA, 2002). Tal infra-estrutura torna possível a validade de documentos eletrônicos por tempo indeterminado.

Recentemente, está sendo desenvolvida uma dissertação de mestrado que trata da infra-estrutura da protocolação digital de documentos eletrônicos (DEMÉ-

TRIO, 2003). Este trabalho trata de questões como o sincronismo entre uma fonte de tempo confiável e as ADs. Também encontra-se em fase de desenvolvimento uma proposta de RFC, cujo nome é *Policy Requirements for Time-Stamping Authorities* (PINKAS; POPE; ROSS, 2003). Este documento define os requisitos para uma Política de Protocolação para Autoridades de Datação.

A redução da necessidade de confiança na AD, obtida com os métodos de datação relativa, não elimina, porém, a necessidade de desenvolvimento de outros mecanismos. Até a presente data não se tem conhecimento de pesquisas que tratem especificamente da questão da auditoria da protocolação digital de documentos eletrônicos.

1.5 Justificativa e Motivação

Para que os documentos eletrônicos tenham eficácia jurídica, os mesmos devem ser assinados e protocolados de maneira digital. Desta forma, pode-se provar que um documento existiu em um determinado instante do tempo no passado, não foi alterado desde então e que no momento da assinatura, o certificado digital do assinante estava dentro do seu período de validade.

No Brasil, houve uma iniciativa do governo federal de utilização de tecnologia da informação no âmbito da administração federal. Esta iniciativa resultou em um Plano de Metas (BRASIL, 2000). Entre as tecnologias de informação utilizadas, estão documentos eletrônicos e assinaturas digitais. Para tanto, o governo brasileiro, através da Medida Provisória 2.200-2 de agosto de 2001 (BRASIL, 2001), criou a ICP-Brasil, responsável pela Infra-estrutura de Chaves Públicas brasileira (ICP-BRASIL, 2003).

Recentemente foi assinado um convênio entre o LabSEC (LABSEC, 2003), a BRy (BRY, 2003) e o Observatório Nacional (ON, 2003). O primeiro projeto resultante deste convênio é o desenvolvimento de um sistema de "Sincronização Segura de Relógio para Documentos Eletrônicos". Este projeto tem como principal objetivo desenvolver um sistema para fornecer o serviço de sincronismo de tempo para sistemas de protocolação de documentos eletrônicos e demais possíveis sistemas que necessitem do tempo oficial.

Contudo, para que se possa confiar nos documentos eletrônicos é fundamental que o serviço de protocolação também seja confiável. Assim, este trabalho tem como principal objetivo propor procedimentos que proporcionem maior confiança ao sistema de protocolação digital de documentos eletrônicos.

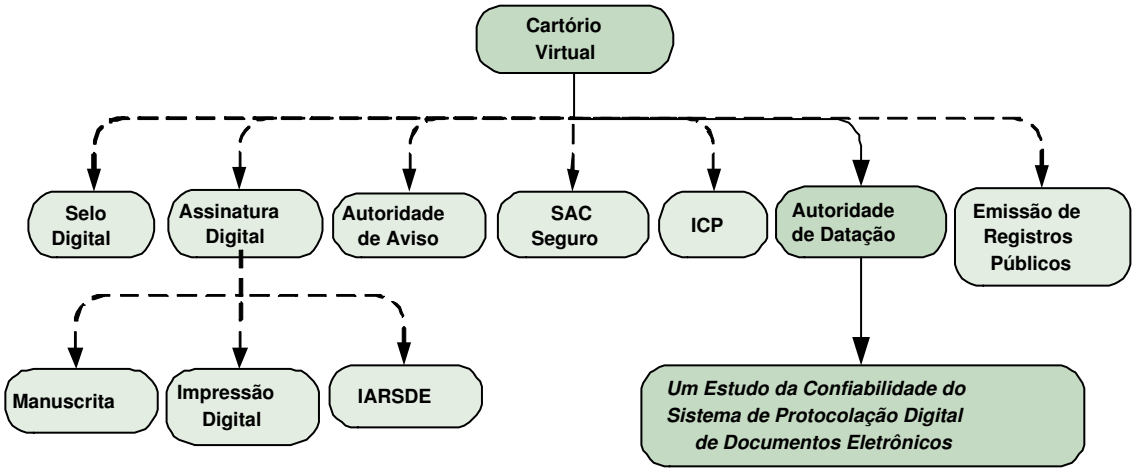


Figura 1.1: Projeto Cartório Virtual

Este trabalho faz parte do projeto Cartório Virtual. Conforme ilustra a Figura 1.1, o Cartório Virtual é o projeto do LabSEC (LABSEC, 2003) que envolve vários subprojetos, tais como: SAC Seguro (GHISLERI, 2002), Autoridade de Aviso, Selo Digital, ICP (IGNACZAK, 2002; MIGNONI, 2002), Assinatura Digital (KAZIENKO, 2003; NOTOYA, 2002), Emissão de Registros Públicos (BORTOLI, 2002), Autoridade de Datação (PASQUAL, 2001), entre outros. O trabalho que está sendo proposto faz parte do subprojeto Autoridade de Datação.

1.6 Organização do Texto

Primeiramente são apresentados alguns conceitos básicos para facilitar o entendimento dos assuntos tratados posteriormente. O capítulo 2 apresenta o conceito de documento e documento eletrônico, suas vantagens e desvantagens. Também trata da questão da eficácia jurídica e legislação referente ao assunto no Brasil e no mundo.

O capítulo 3 apresenta uma explicação geral sobre a protocolação de documentos tradicionais, descreve o funcionamento de um serviço de protocolação de documentos eletrônicos e os principais métodos de datação, além de relacionar algumas soluções de empresas que fornecem o serviço de protocolação digital.

Após a revisão bibliográfica descrita nos capítulos 2 e 3, são apresentadas as contribuições deste trabalho. O capítulo 4 apresenta os aspectos relevantes da confiança em um sistema de protocolação digital. Primeiramente são levantados os elementos que constituem a confiança. Após isso, são apresentadas as questões referentes ao problema, e, finalmente, são propostos alguns mecanismos, os quais visam aumentar a confiança do sistema. Dentre os mecanismos propostos, está a realização de procedimentos de auditoria, a publicação do Ponto de Confiança, a elaboração de uma Política de Protocolação e de uma Declaração de Práticas de Protocolação, além da renovação dos recibos.

O capítulo 5 apresenta os procedimentos de auditoria propostos, os quais podem ser aplicados em sistemas de protocolação digital que utilizem como método de datação o Encadeamento Linear ou a Árvore Sincronizada.

O capítulo 6 propõe uma Política de Protocolação. Este documento tem como objetivo descrever, de maneira sucinta, as práticas da AD, de modo que os usuários possam tomar conhecimento dos procedimentos adotados e avaliar se os mesmos são suficientes para assegurar a confiança do sistema.

O capítulo 7 apresenta uma análise da confiança de um sistema de protocolação digital, no qual várias ADs constituem uma infra-estrutura distribuída. Inicialmente, é descrito o funcionamento do sistema e, após isso, são apresentados os procedimentos adicionais que devem ser executados em uma auditoria, quando houver uma protocolação cruzada.

O capítulo 8 apresenta as considerações finais da dissertação, onde são divulgados os resultados obtidos e as sugestões de trabalhos futuros.

O apêndice A apresenta um glossário.

No apêndice B é apresentada uma proposta de Declaração de Práticas de Protocolação, a qual foi elaborada para o sistema de protocolação digital comercializado

pela BRy (BRY, 2003).

O apêndice C relata um protótipo de um sistema de auditoria desenvolvido para Autoridades de Datação que utilizam o Método do Encadeamento Linear.

O apêndice D apresenta os artigos científicos que foram publicados.

Capítulo 2

Documento

2.1 Introdução

Com o advento da *Internet*, muitas transações, que normalmente eram realizadas utilizando documentos tradicionais[1], passaram a ser realizadas de maneira eletrônica. Contudo, para que um documento eletrônico tenha eficácia jurídica, ele deve apresentar algumas propriedades, tais como, autenticidade, integridade e tempestividade.

Com o surgimento dos documentos eletrônicos, o conceito de documento teve de ser atualizado. Este assunto é tratado na seção 2.2. A seção 2.3 apresenta um breve histórico da evolução do documento ao longo do tempo. Na seção 2.4 são discutidas as vantagens e desvantagens entre os documentos tradicionais e os documentos eletrônicos. Apesar de os documentos eletrônicos não apresentarem naturalmente algumas propriedades necessárias para que tenham eficácia jurídica, algumas técnicas criptográficas podem ser utilizadas para que tais propriedades sejam atendidas. Este assunto é tratado na seção 2.5. A seção 2.6 apresenta algumas leis que regulamentam esta questão no Brasil e no mundo. Por fim, na seção 2.7 são apresentadas as conclusões deste capítulo.

[1] A expressão *documento tradicional* será utilizada neste trabalho no sentido de representar os documentos utilizados antes do advento do computador. Este termo geralmente se refere aos documentos em papel.

2.2 Definição de documento

A palavra documento tem origem no latim, *documentum*, que deriva do verbo *doceo*, que significa ensinar, mostrar, indicar. A definição mais usual do termo documento é "qualquer base de conhecimento, fixada materialmente e disposta de maneira que se possa utilizar para consulta, estudo, prova, etc."(AURÉLIO, 1999).

Sob o ponto de vista jurídico, a palavra documento possui diversas acepções. Para Santos (1982, p. 386), "num sentido amplo, documento é a coisa que representa e presta-se a reproduzir uma manifestação de pensamento, ou seja, uma coisa representativa de idéias ou fatos".

De acordo com Marques (1967, p. 307), "o documento é a prova histórica real, visto que representa fatos e acontecimentos pretéritos em um objeto físico, servindo assim de instrumento de convicção".

Segundo Aurélio (1999), o termo documento também pode ser definido como "escritura destinada a comprovar um fato; declaração escrita, revestida de forma padronizada, sobre fato(s) ou acontecimento(s) de natureza jurídica".

O conceito de documento sempre esteve relacionado com a idéia de um escrito oficial, de uma informação fixada sobre um meio material. Isto porque por muito tempo o papel foi utilizado como o principal meio onde o conhecimento era registrado.

Rover (2002) leciona que o documento tradicional é uma forma de registro sobre papel (suporte físico, confiável e durável) e por meio da escrita (linguagem precisa e imutável). O documento em papel associa uma informação com um suporte material, de maneira que o conteúdo, ou seja, a informação, seja indissociável do suporte. Entretanto, com o advento da informática, criou-se um novo meio de registro de informação. Surge o documento eletrônico e com ele a necessidade de atualizar o conceito de documento, visto que agora, a informação não é mais associada com um suporte material.

2.3 Evolução do documento

Na era primitiva, as expressões de vontade eram marcadas por rituais. Os negócios se realizavam em público, para que o testemunho de uma grande concentração de pessoas fosse a prova daquele ato. Ao longo do tempo esses ritos foram sendo substituídos pela assinatura. Com a popularização dos pergaminhos e, posteriormente, do papel, a materialidade do documento ganhou importância. O documento passou a ser composto também pelo nome do autor e pela data, recebendo, assim, valor probatório.

Com o advento do meio eletrônico, surge a necessidade de ampliar o conceito de manifestação de vontade, suporte e documento. Trata-se do surgimento de um novo suporte, com a provável conseqüência de superar-se, definitivamente, a associação direta entre documento e suporte tangível. O conceito de documento teve que se adaptar, para viabilizar a sua aplicação no meio eletrônico, pois é necessário garantir as mesmas propriedades já consolidadas no meio tradicional. O documento eletrônico se apresenta em um novo suporte, na forma de uma seqüência de *bits* que pode ser traduzida por meio de um programa de computador.

2.4 Documento tradicional *versus* documento eletrônico

A seguir são apresentadas as vantagens da utilização dos documentos eletrônicos em relação aos documentos tradicionais:

- Maior velocidade em sua elaboração;
- Arquivamento de forma simples;
- Facilidade de recuperação dos dados;
- Alta capacidade de armazenamento;
- Duplicação e transmissão imediata;
- Capacidade de resistência ao envelhecimento e deterioração.

Os documentos tradicionais, que utilizam como meio o papel, não mais suprem as necessidades de agilidade na circulação das informações. São evidentes as suas limitações nos dias atuais, seja no que se refere à simples conservação ou transmissão. Em virtude disso, várias instituições passaram a utilizar os documentos eletrônicos, visando tornar os processos mais ágeis. Um exemplo disto, é a proposta apresentada por Bortoli (2002) em sua dissertação de mestrado, na qual sugere que os cartórios, principalmente os Ofícios de Registro Civil de Pessoas Naturais, façam uso do documento eletrônico para emitir e armazenar registros e documentos em geral, visando facilitar e garantir os registros civis aos indivíduos e também melhorar o atendimento aos usuários.

Apesar das vantagens mencionadas anteriormente, os documentos eletrônicos também apresentam algumas desvantagens em relação aos documentos tradicionais, tais como:

- O documento tradicional não exige a utilização de qualquer artifício para sua visualização, enquanto que um documento eletrônico requer a intermediação de um computador e de um *software* para decodificar a seqüência de *bits* do arquivo. Em razão disso, o tempo de vida do documento estaria vinculado ao tempo de vida do *software* utilizado para decodificá-lo;

- Marcas, impressões e formas em alto relevo existentes em documentos em papel garantem o controle das cópias e a origem do emissor, mas não podem ser facilmente transferidos para documentos eletrônicos;

- Por razões culturais, as pessoas podem apresentar resistência para adotar a utilização de documentos eletrônicos.

Apesar das vantagens da utilização dos documentos eletrônicos em relação aos documentos tradicionais, acredita-se que as tecnologias de digitalização dos documentos devam reduzir muito o uso do papel, mas dificilmente irão eliminá-lo. Acredita-se que as duas formas devam permanecer por muito tempo.

2.5 Eficácia jurídica do documento eletrônico

Devido ao fato de o documento eletrônico ser composto por uma seqüência de *bits*, ele apresenta algumas características que o difere de um documento tradicional, como, por exemplo:

- **Mobilidade:** Não está preso ao meio físico;
- **Alterabilidade:** Permite alteração no conteúdo sem deixar vestígios.

Apesar disso, os documentos eletrônicos podem ter eficácia jurídica, desde que apresentem algumas propriedades, que são as mesmas exigidas para os documentos tradicionais:

- **Autenticidade:** correspondência entre o autor indicado e o autor real do documento. Esta propriedade geralmente é comprovada através de uma assinatura;
- **Integridade:** Possibilidade de verificar se o conteúdo de um documento foi modificado;
- **Tempestividade:** identificação e preservação da data em que foram manifestadas as declarações de vontade.

Estas propriedades podem ser atendidas através de técnicas criptográficas. A assinatura digital possibilita detectar se o conteúdo de um documento eletrônico foi alterado, garantindo a integridade, e permite verificar se o autor do documento é quem ele diz ser, assegurando a autenticidade. Para obter a tempestividade, o documento eletrônico deve ser protocolado através de um sistema de protocolação digital.

Existe uma grande discussão a respeito da eficácia jurídica dos documentos eletrônicos. Alguns estudiosos do direito defendem a validade do contrato eletrônico, equiparando-o ao contrato verbal que é aceito desde 1916. Eles defendem a tese de que se o contrato verbal é aceito, o contrato eletrônico também deveria ser.

A falta de regulamentação referente a esta questão representa, atualmente, um dos maiores empecilhos ao desenvolvimento do comércio eletrônico. Em razão disto, alguns países estão adotando legislações sobre este assunto.

2.6 Legislação

Os avanços tecnológicos têm causado forte impacto sobre as mais diversas áreas do conhecimento e das relações humanas. O comércio eletrônico é um dos exemplos mais significativos disso. Devido a estas mudanças, surgiu a necessidade de criar leis que regulamentem a questão da eficácia jurídica dos documentos eletrônicos.

2.6.1 Legislação internacional

Nos últimos anos, vários países criaram leis para regulamentar a eficácia jurídica de documentos eletrônicos. Porém, cada país tratou da questão a sua maneira, visto que alguns países simplesmente criaram mecanismos certificadores das assinaturas digitais, enquanto outros decidiram por subordinar a eficácia jurídica ao consentimento das partes, enquanto outros, ainda, atribuíram a mesma eficácia jurídica dos documentos tradicionais assinados manualmente aos documentos eletrônicos assinados digitalmente.

Estados Unidos: A primeira lei referente a esta questão foi promulgada pelo estado norte-americano de Utah, denominada *Digital Signature Act* (UNIDOS, 1995). Esta lei reconhece o método de certificação digital e considera o documento eletrônico autêntico e de mesma eficácia de um documento tradicional.

Já o estado da Califórnia, através do *California Government Code* (UNIDOS, 1997), subordinou a validade dos documentos eletrônicos à aquiescência daqueles que os produzirem. A lei define que a utilização de uma assinatura digital deve ter o mesmo efeito que uma assinatura manual, desde que atenda os seguintes requisitos:

- Deve ser única para cada pessoa;
- Deve ser possível verificá-la;
- Deve estar sob o controle exclusivo da pessoa que assinou;
- Deve estar ligada aos dados, de tal maneira que se os dados forem alterados, a assinatura digital torna-se inválida;

- Deve estar de acordo com as regulamentações adotadas pela Secretaria do Estado.

Atualmente, os Estados Unidos possuem uma lei federal tratando do assunto (UNIDOS, 2000). A lei estabelece que uma assinatura, um contrato, ou qualquer registro referente a uma transação não pode ter efeito legal ou validade negados, somente porque se encontra em uma forma eletrônica.

Alemanha: A Alemanha já tem a sua lei federal (ALEMANHA, 1997) que estabelece as condições gerais para a utilização de assinaturas digitais. No entanto, a legislação se limitou a definir a estrutura necessária para a utilização de assinaturas digitais, não lhes atribuindo a mesma eficácia jurídica que o documento assinado manualmente.

Portugal: O Decreto-Lei n^o 290-D/99 regula o reconhecimento e a eficácia jurídica dos documentos eletrônicos e das assinaturas digitais, e define os poderes e procedimentos das Autoridades Certificadoras. Conforme esta lei, o documento eletrônico satisfaz o requisito legal de forma escrita quando:

> Artigo 3^o
>
> 1. O documento eletrônico satisfaz o requisito legal de forma escrita quando o seu conteúdo seja suscetível de representação como declaração escrita.
>
> 2. Quando lhe seja aposta uma assinatura digital certificada por uma entidade credenciada e com os requisitos previstos nesta lei, o documento eletrônico com o conteúdo referido no número anterior tem a força probatória de documento particular assinado, nos termos do artigo 376^o do Código Civil.
>
> 3. Quando lhe seja aposta uma assinatura digital certificada por uma entidade credenciada e com os requisitos previstos nesta lei, o documento eletrônico cujo conteúdo não seja suscetível de representação como declaração escrita tem a força probatória prevista no artigo 368^o do Código Civil e no artigo 167^o do Código de Processo Penal.
>
> 4. O disposto nos números anteriores não obsta à utilização de outro meio de comprovação da autoria e integridade de documentos eletrônicos, incluindo a assinatura eletrônica não conforme com os requisitos da presente lei, desde que tal meio seja adotado pelas partes ao abrigo de válida convenção sobre prova ou seja aceite pela pessoa a quem for oposto o documento.
>
> 5. O valor probatório dos documentos eletrônicos aos quais não seja aposta uma assinatura digital certificada por uma entidade credenciada e com os requisitos previstos nesta lei é apreciado nos termos gerais de direito. (PORTUGAL, 1999).

Estônia: A lei *Digital Signature Act* entrou em vigor em 2000 e define as condições necessárias para a utilização de assinaturas digitais, além de estabelecer procedimen-

tos para supervisionar o fornecimento de serviços de certificação e protocolação digital (ESTÔNIA, 2000). Além disso, determina que uma assinatura digital tem as mesmas conseqüências legais de uma assinatura manuscrita se estas conseqüências não forem restritas pela lei e se a assinatura atender a alguns requisitos previamente definidos. Também afirma que a assinatura digital não é legal quando for provado que a chave privada utilizada na assinatura não foi utilizada com o consentimento do dono do certificado digital correspondente.

Comunidade Européia: A Comunidade Européia elaborou a Diretiva 1999/93/CE através do Parlamento Europeu com o objetivo de facilitar a utilização das assinaturas eletrônicas e contribuir para o seu reconhecimento legal. Com relação a eficácia jurídica, a lei determina que:

> Artigo 5^o Efeitos legais das assinaturas eletrônicas
>
> 1. Os Estados-Membros assegurarão que as assinaturas eletrônicas avançadas baseadas num certificado qualificado e criadas através de dispositivos seguros de criação de assinaturas:
>
> a) Obedecem aos requisitos legais de uma assinatura no que se refere aos dados sob forma digital, do mesmo modo que uma assinatura manuscrita obedece àqueles requisitos em relação aos dados escritos; e
>
> b) São admissíveis como meio de prova para efeitos processuais.
>
> 2. Os Estados-Membros assegurarão que não sejam negados a uma assinatura eletrônica os efeitos legais e a admissibilidade como meio de prova para efeitos processuais apenas pelo fato de:
>
> - se apresentar sob forma eletrônica,
>
> - não se basear num certificado qualificado,
>
> - não se basear num certificado qualificado emitido por um prestador de serviços de certificação acreditado,
>
> - não ter sido criada através de um dispositivo seguro de criação de assinaturas. (EUROPÉIA, 1999).

Organização das Nações Unidas: Em 1996, a Organização das Nações Unidas, por intermédio da Comissão das Nações Unidas para Leis de Comércio Internacional (UNCITRAL), elaborou uma lei modelo buscando uma maior uniformização da legislação sobre a matéria no plano internacional. Com relação à eficácia jurídica dos documentos eletrônicos, a lei afirma que:

> Artigo 9^o Admissibilidade e força probante das mensagens de dados

> 1) Em procedimentos judiciais, administrativos ou arbitrais não se aplicará nenhuma norma jurídica que seja óbice à admissibilidade de mensagens eletrônicas como meio de prova
>
> a) Pelo simples fato de serem mensagens eletrônicas; ou,
>
> b) Pela simples razão de não haverem sido apresentadas em sua forma original, sempre que tais mensagens sejam a melhor prova que se possa razoavelmente esperar da pessoa que as apresente.
>
> 2) Toda informação apresentada sob a forma de mensagem eletrônica gozará da devida força probante. Na avaliação da força probante de uma mensagem eletrônica, dar-se-á atenção à confiabilidade da forma em que a mensagem haja sido gerada, armazenada e transmitida, a confiabilidade da forma em que se haja conservado a integridade da informação, a forma pela qual se haja identificado o remetente e a qualquer outro fator pertinente. (UNIDAS, 1996).

Portanto, os requisitos estabelecidos pela lei permitem que um documento eletrônico tenha eficácia jurídica equivalente a um documento escrito, assinado e original. A Lei Modelo também trata do reconhecimento jurídico dos contratos eletrônicos, não negando a sua validade e força obrigatória, como um contrato firmado na forma tradicional. A lei também discorre a respeito da necessidade do documento eletrônico se apresentar na forma escrita, quando a lei exigir.

2.6.2 Legislação brasileira

A seguir é apresentada a legislação que regulamenta o assunto no Brasil.

Projeto de Lei n^o 1.483/99, do Senado Federal: Institui a fatura eletrônica e a assinatura digital nas transações de comércio eletrônico. Este Projeto de Lei (PL) define que:

> Art. 1^o Fica instituída a fatura eletrônica assim como a assinatura digital, nas transações comerciais eletrônicas realizadas em todo o território nacional.
>
> Art. 2^o A assinatura digital terá sua autenticação e reconhecimento certificado por órgão público que será regulamentado para este fim. (BRASIL, 1999a).

Projeto de Lei n^o 672/99, do Senado Federal: Regula o comércio eletrônico em todo o território nacional, aplica-se a qualquer tipo de informação na forma de mensagem de dados usada no contexto de atividades comerciais. Em relação à eficácia jurídica das mensagens de dados, este PL define que:

> Art. 5^o Serão reconhecidos os efeitos jurídicos, validade ou eficácia à informação sob a forma de mensagem eletrônica e àquela a que se faça remissão mediante a utilização dessa espécie de mensagem.
>
> Art. 6^o Quando a lei determinar que uma informação conste por escrito, este requisito considerar-se-á preenchido por uma mensagem eletrônica, desde que a informação nela contida seja acessível para consulta posterior.
>
> Art. 7^o No caso de a lei exigir a assinatura de uma pessoa, este requisito considerar-se-á preenchido por uma mensagem eletrônica, desde que seja utilizado algum método para identificar a pessoa e indicar sua aprovação para a informação contida na mensagem. (BRASIL, 1999c).

Projeto de Lei n^o 1.589/99, da Ordem de Advogados do Brasil (OAB) de São Paulo: Dispõe sobre o comércio eletrônico, a eficácia jurídica do documento eletrônico e a assinatura digital. Este PL segue algumas regras da Lei Modelo da UNCITRAL, adota o sistema de criptografia assimétrica como base para a assinatura digital e reserva papel preponderante para os notários. Estabelece que a certificação da chave pública por tabelião faz presumir a sua autenticidade, enquanto aquela feita por particular não gera o mesmo efeito. Com relação a eficácia jurídica dos documentos eletrônicos, este Projeto de Lei afirma que:

> Art. 14 Considera-se original o documento eletrônico assinado pelo seu autor mediante sistema criptográfico de chave pública.
>
> §1^o Considera-se cópia o documento eletrônico resultante da digitalização de documento físico, bem como a materialização física de documento eletrônico original.
>
> §2^o Presumem-se conformes ao original, as cópias mencionadas no parágrafo anterior, quando autenticados pelo escrivão na forma dos arts. 33 e 34 desta lei.
>
> §3^o A cópia não autenticada terá o mesmo valor probante do original, se a parte contra quem for produzida não negar sua conformidade.
>
> Art. 15 As declarações constantes do documento eletrônico, digitalmente assinado, presumir-se-ão verdadeiras em relação ao signatário, desde que sejam observados os seguintes requisitos no tocante a própria assinatura digital:
>
> a) seja única e exclusiva para o documento assinado;
>
> b) seja passível de verificação;
>
> c) seja gerada sob o exclusivo controle do signatário;
>
> d) esteja de tal modo vinculada ao documento, em caso de posterior alteração, seja invalidada, e,
>
> e) não tenha sido gerada em momento posterior á expiração, revogação ou suspensão das chaves. (BRASIL, 1999b).

Medida Provisória n^o 2.200: Em 28 de junho de 2001 foi a editada a Medida Provisória (MP) de n^o 2.200, a qual institui a Infra-estrutura de Chaves Públicas Brasileira

(ICP-Brasil) e dá outras providências. Em 27 de julho de 2001, o Presidente da República reeditou a MP com algumas alterações (MP 2.200-1), numa tentativa de modificar alguns pontos criticados pela OAB/SP. Em 24 de agosto de 2001, o Comitê Gestor de Infra-estrutura de Chaves Públicas editou a resolução n^o 2 (MP 2.200-2), que aprova a Política de Segurança da ICP-Brasil. A MP 2.200-2 define em seu primeiro artigo que:

> Art. 1^o Fica instituída a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras. (BRASIL, 2001)

Também é definida a competência do Comitê Gestor, bem como as funções das AC (Autoridades Certificadoras) e das AR (Autoridades de Registro). Além disso, discorre sobre documentos públicos e particulares.

> Art. 10 Consideram-se documentos públicos ou particulares, para todos os fins legais, os documentos eletrônicos de que trata esta Medida Provisória.
>
> §1^o As declarações constantes dos documentos em forma eletrônica produzidos com a utilização de processo de certificação disponibilizado pela ICP-Brasil presumem-se verdadeiros em relação aos signatários, na forma do art. 131 da Lei no 3.071, de 1o de janeiro de 1916 - Código Civil.
>
> §2^o O disposto nesta Medida Provisória não obsta a utilização de outro meio de comprovação da autoria e integridade de documentos em forma eletrônica, inclusive os que utilizem certificados não emitidos pela ICP-Brasil, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento. (BRASIL, 2001).

Lei n^o 12.137/02, do Estado de Santa Catarina: Dispõe sobre a protocolação digital de informações no âmbito da administração pública estadual e adota outras providências. Esta Lei define que:

> Art. 1^o Será materializada em documento eletrônico a informação relativa a pedido de providência ou procedimento, independentemente da existência de prazo para atendimento, atribuído a órgão da administração pública direta, indireta, fundacional e à empresa pública.
>
> [...]
>
> §2^o Considera-se informação a mensagem, a solicitação, a notificação, a intimação, recebida através de qualquer meio de comunicação, que possa ser convertida em linguagem escrita brasileira.

> §3^o Quando recebida através de meio eletrônico, a conversão corresponderá à integridade da informação, ou um resumo contendo a sua essência.
>
> Art. 2^o O disposto nesta Lei não se aplica à informação:
>
> I - contida em documento onde tenha sido aposto recibo ou número de protocolo;
>
> II - que deva ser protocolada no prazo e forma prevista em Lei ou em outro instrumento normativo; e
>
> III - cuja providência a ela relacionada deva ser objeto de divulgação através de órgão oficial de imprensa.
>
> Art. 3^o Será transmitida ao interessado na informação uma resposta comprovando o seu recebimento, a qual receberá um número de registro, com data e hora obtidas por protocolação digital, e que ficará disponível em página da *Internet* do órgão, empresa ou entidade transmitente.
>
> [...]
>
> §5^o O sistema de protocolação deverá ter data e hora sincronizadas com um sistema público, operar como servidor para outros sistemas, estar protegido da ação externa sobre as suas bases de dados e algoritmos e permitir a auditoria sobre as suas operações. (CATARINA, 2002)

2.7 Conclusão

Embora os documentos eletrônicos apresentem uma série de vantagens em relação aos documentos em papel, acredita-se que as tecnologias de digitalização de documentos reduzirão muito a utilização do papel, mas dificilmente irão eliminá-la. A tendência é que as duas formas permaneçam por muito tempo.

Nota-se que vários países já criaram ou estão criando leis para regular a questão da eficácia jurídica dos documentos eletrônicos, no entanto, é necessário que estas leis sejam colocadas em prática o mais rápido possível, visto que todos os países possuem interesse em que as transações internacionais sejam regulamentadas por uma legislação.

Capítulo 3

Sistemas de Protocolação de Documentos

3.1 Introdução

Antes do surgimento dos documentos eletrônicos, os documentos tradicionais já eram protocolados. Atualmente, este tipo de protocolação ainda é muito utilizada, principalmente em instituições públicas, com o objetivo de registrar as datas referentes ao trâmite dos processos. Antes de tratar da protocolação digital, o sistema tradicional de protocolação será abordado na seção 3.2. O funcionamento de um sistema de protocolação digital será apresentado na seção 3.3. Os sistemas de protocolação digital podem utilizar métodos de datação absoluta, que se baseia somente no tempo fornecido por uma fonte confiável, métodos de datação relativa, que encadeiam os documentos pela ordem de chegada, ou ambos. A seção 3.4 apresenta dois métodos de datação relativa: Método do Encadeamento Linear e Método da Árvore Sincronizada. Já a seção 3.5 descreve os módulos criptográficos de *hardware*, os quais são utilizados em alguns equipamentos de protocolação, com o intuito de prover maior segurança física e lógica. Na seção 3.6 são apresentadas algumas empresas que prestam o serviço de protocolação digital, bem como os métodos de datação por elas utilizados. Finalmente, a seção 3.7 apresenta as conclusões deste capítulo.

3.2 Sistema de Protocolação de Documentos Tradicionais

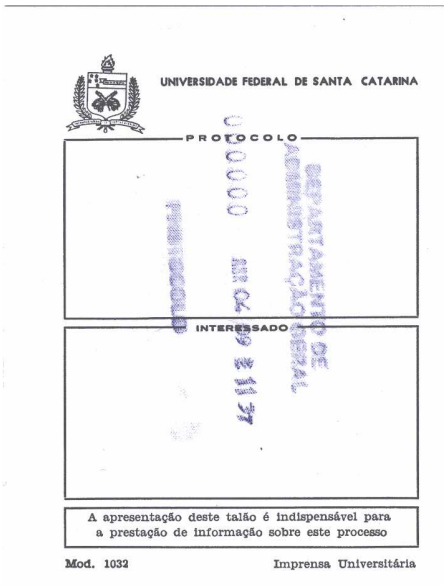
A necessidade de protocolar documentos existe principalmente em instituições onde é importante ter um controle da tramitação dos processos. Para entender melhor o funcionamento de um sistema de protocolação de documentos tradicionais, foi realizada uma visita à seção de Protocolo Geral da UFSC. Nesta visita os funcionários explicaram o funcionamento do processo de protocolação por eles utilizados.

O sistema de protocolação de documentos utilizado na seção de Protocolo Geral da UFSC é composto por um relógio datador, alguns funcionários e pelos usuários. O relógio datador é o equipamento responsável por carimbar os documentos. No carimbo impresso pelo relógio, constam a data e a hora em que o documento foi protocolado. A Figura 3.1 ilustra o relógio datador.

Figura 3.1: Relógio datador

Após a protocolação do documento, o funcionário emite um recibo para o usuário, o qual possui um carimbo contendo a data e a hora da protocolação. A Figura 3.2 ilustra um recibo.

O sistema de protocolação utilizado na Reitoria da UFSC não é inspecionado por nenhum tipo de procedimento de auditoria. Constatou-se, inclusive, que o relógio interno pode ser alterado manualmente, não existindo nenhuma proteção do equipamento no sentido de impedir o acesso aos seus componentes internos. Para aumentar a confiança do sistema, poderiam ser adotadas algumas medidas, tais como: a utilização de lacres no equipamento, realização de auditorias no relógio datador e proteção do


UNIVERSIDADE FEDERAL DE SANTA CATARINA

PROTOCOLO

INTERESSADO

A apresentação deste talão é indispensável para a prestação de informação sobre este processo

Mod. 1032 Imprensa Universitária

Figura 3.2: Recibo de protocolação do Protocolo Geral da UFSC

equipamento contra riscos do ambiente e de pessoas não autorizadas.

Estas medidas implicam custos, pois a realização de auditoria requer um funcionário treinado que realize inspeções freqüentes. Isto é necessário, pois no caso de rompimento do lacre, por exemplo, a invasão é detectada, porém não existem provas ou indícios de quando ou quem violou o equipamento. Assim, não se pode confiar nos documentos protocolados desde a última auditoria. Portanto, quanto maior for a freqüência com que as auditorias são realizadas, menor será o número de protocolações comprometidas no caso de fraude.

3.3 Sistema de Protocolação de Documentos Eletrônicos

A protocolação digital tem como objetivo assegurar a existência de um documento eletrônico em uma determinada data e hora (LIPMAA, 1999; SCHNEIER, 1996). A data e a hora anexadas ao documento devem condizer com a data e a hora em que o documento foi submetido ao processo de protocolação, de modo a garantir que o documento existiu em um determinado momento no tempo. Muitos sistemas de protocolação utilizam uma entidade chamada Autoridade de Datação - AD. A AD é a

entidade responsável por disponibilizar um serviço de protocolação confiável. Em muitos países o relógio da AD deve estar sincronizado de forma segura com o provedor de hora legal. No Brasil, o Observatório Nacional (ON, 2003) é a entidade que fornece a hora oficial. Existem muitos protocolos de comunicação que permitem realizar este sincronismo (SILVA DIAS; CUSTÓDIO; DEMÉTRIO, 2003).

A importância da protocolação de documentos se torna evidente quando existe a necessidade de utilizar documentos eletrônicos por um longo período de tempo. Sem a protocolação não se pode confiar em documentos eletrônicos assinados, pois não se sabe se o documento foi assinado antes da revogação ou da expiração da chave privada.

Um sistema de protocolação digital de documentos eletrônicos pode ser estruturado através da confiança distribuída entre os usuários do serviço ou através de uma Autoridade de Datação (AD), sendo este último, o modelo mais utilizado. Serviços baseados em confiança distribuída são utilizados entre grupos de datadores. Neste modelo, vários integrantes do grupo datam e assinam digitalmente o documento, e, ao término deste processo, o documento é considerado protocolado. Este modelo possui desvantagens em relação à sua eficiência, pois o documento deve ser protocolado por todos os datadores. Já os serviços baseados na Autoridade de Datação, partem do pressuposto de que a Autoridade de Datação é uma entidade confiável e que toda uma comunidade de usuários do serviço compartilha esta confiança.

A Figura 3.3 ilustra um equipamento de protocolação digital de documentos eletrônicos. Um sistema de protocolação digital geralmente é composto por: uma plataforma computacional; identidade digital; Módulo de Hardware Seguro - HSM, para armazenar a chave privada da AD; e um *software* para receber as requisições e gerar o recibo.

Figura 3.3: Protocoladora Digital de Documentos Eletrônicos - Fonte: BRy Tecnologia

3.3.1 Requisitos de Segurança

Um sistema de protocolação digital deve atender aos seguintes requisitos de segurança:

- **Privacidade:** o conteúdo do documento deve ser de conhecimento exclusivo do cliente;
- **Canal de comunicação e armazenamento:** o tamanho do documento não deve afetar o desempenho do serviço de protocolação;
- **Integridade:** deve ser possível detectar se o documento ou o recibo foram alterados;
- **Anonimato:** o cliente deve ter sua identidade mantida em sigilo;
- **Tempestividade:** o documento deve ser protocolado com data/hora corretas e esta informação deve ser preservada;

A Figura 3.4 ilustra um sistema de protocolação que atende alguns destes requisitos:

- **Privacidade:** a AD tem acesso apenas ao resumo do documento e não ao documento;
- **Facilidade de comunicação e armazenamento:** o resumo do documento tem tamanho fixo e é pequeno, normalmente menor do que o documento;
- **Integridade:** de posse do recibo, o cliente pode verificar a assinatura da AD e, desta forma, verificar se o resumo enviado foi alterado durante a comunicação;
- **Anonimato:** não é assegurado neste esquema de protocolação. Este requisito não é necessário em muitas situações, e, portanto, pode ser visto como uma característica desejável, porém não obrigatória;

- **Tempestividade:** pode ser atendido desde que o equipamento de protocolação seja lacrado e adote padrões de segurança física e lógica, como por exemplo, os descritos na FIPS-140 (NIST, 2002). Além disso, devem existir procedimentos de auditoria para inspecionar as operações realizadas pela AD.

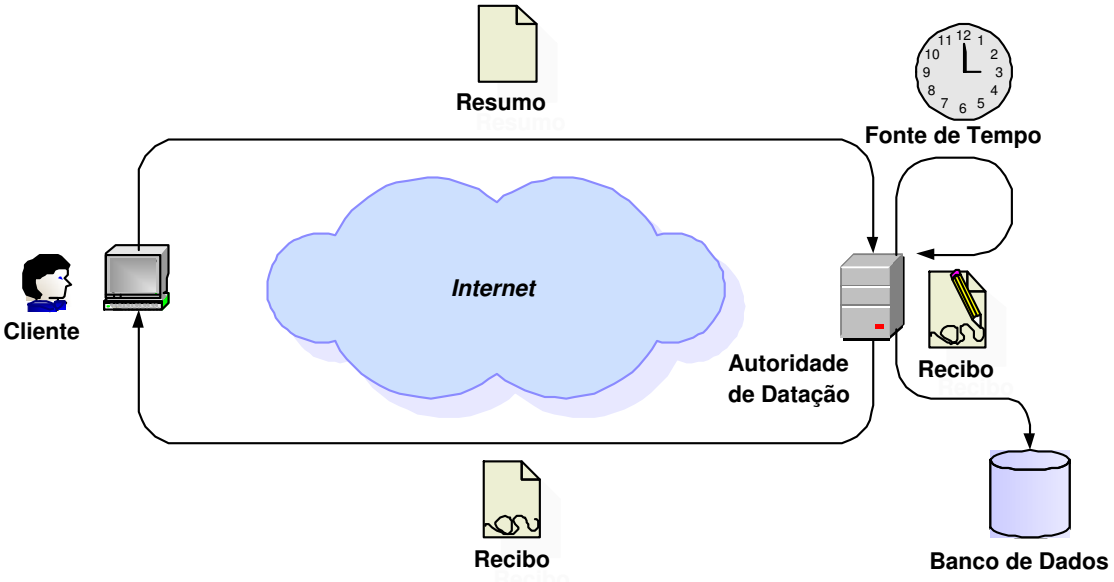


Figura 3.4: No processo de protocolação digital de documentos eletrônicos o cliente envia para a AD o resumo do documento a ser protocolado. A AD anexa a data e a hora ao resumo, assina essas informações e gera um recibo. O recibo é armazenado em seu banco de dados e uma cópia é enviada para o cliente.

Atualmente existe uma RFC que tem como objetivo padronizar o protocolo de requisição de protocolação de um documento. A RFC 3161 (ADAMS, 2001) descreve o formato de uma requisição enviada a uma AD e da resposta que é retornada para o cliente. Esta RFC também estabelece vários requisitos de segurança para a operação da AD, considerando o processamento das requisições e a geração das respostas.

3.3.2 Tipos de Autenticação Temporal

Adicionar data e hora corretas a um documento eletrônico não é trivial. A associação de um documento eletrônico com um determinado momento no tempo é algo muito complicado, visto que a informação de data/hora deve ser confiável e deve

existir uma sincronização entre as fontes de tempo. O processo de anexar uma data a um documento pode ser classificado em (JUST, 1998):

Datação absoluta: Consiste em adicionar ao documento a data e a hora em que o mesmo foi submetido a protocolação. Esta informação deve ser provida por uma fonte de tempo confiável. Uma primeira dificuldade deste tipo de datação é a impossibilidade prática de implementar um ponto central, com um único relógio para protocolar os documentos. Outra dificuldade é a necessidade da rastreabilidade das informações de data e hora inseridas no documento em relação à hora provida pela entidade legal. Isso se deve ao caráter absoluto do processo de datação. Neste tipo de datação se alguém desejar trocar a ordem temporal entre dois documentos, isto não seria facilmente detectado, visto que não existe nenhuma relação de dependência entre os documentos. Além disso, documentos protocolados por ADs diferentes só podem ser comparados se os relógios das ADs estiverem sincronizados no momento da protocolação;

Datação relativa: este tipo de datação não se baseia na data e hora corrente, mas na ordem em que os documentos são enviados para a AD. Sua implementação se baseia na teoria da complexidade de funções de sentido único. Neste tipo de datação não se sabe em que momento do tempo um documento foi protocolado, mas é possível verificar entre dois documentos, qual foi protocolado primeiro (BULDAS, 1998). Se alguém desejar trocar a ordem temporal entre dois documentos, isto seria facilmente detectado, pois os documentos subseqüentes ao que teve sua data alterada não seriam mais dependentes dos anteriores no encadeamento. Por outro lado, não é possível saber com precisão o momento exato em que determinado documento foi protocolado;

Híbrida: consiste na adoção dos dois tipos de datação descritos: datação absoluta e relativa simultaneamente.

Visto que um sistema de protocolação digital deve ser o mais confiável possível, é interessante que a datação híbrida seja adotada.

3.4 Métodos de Datação Relativa

Esta seção descreve alguns métodos de datação que utilizam autenticação temporal relativa. Estes métodos, por encadearem os recibos de acordo com a ordem de chegada dos resumos, facilitam a realização de uma auditoria, pois fornecem informações de dependência temporal entre os documentos protocolados.

3.4.1 Encadeamento Linear

Com o objetivo de diminuir a necessidade de se confiar na AD, os recibos são unidos formando um encadeamento, utilizando para isso uma função de sentido único *H*, resistente à colisão, tal como um *hash* como foi proposto por Haber e Stornetta (1991). O encadeamento é mantido em um banco de dados interno para posterior auditoria.

O encadeamento é formado por *links*, sendo que o primeiro *link* da cadeia pode ser gerado de maneira randômica, formando o L_0. Em seguida, o segundo *link* L_1 é gerado utilizando o *link* anterior, no caso, L_0, e o resumo do documento enviado pelo cliente. De forma genérica, temos:

$$L_n = (t_{n-1}, ID_{n-1}, H_{n-1}, H(L_{n-1})) \tag{3.1}$$

onde t_{n-1} é a data e hora em que o documento anterior foi protocolado, ID_{n-1} é um identificador do documento anterior, H_{n-1} é o resumo do documento anterior e $H(L_{n-1})$ é o resumo do *link* anterior. Após o cálculo do *link*, a AD gera o recibo que será enviado para o cliente que será:

$$s = Sig_{AD}(n, t_n, ID_n, H_n, L_n) \tag{3.2}$$

A Figura 3.5 ilustra o encadeamento no Método do Encadeamento Linear. Os resumos dos documentos que foram enviados pelos clientes ficam ordenados obedecendo à ordem de chegada. Uma desvantagem deste método é o tempo necessário para verificar o relacionamento entre dois documentos, o qual é diretamente proporcional

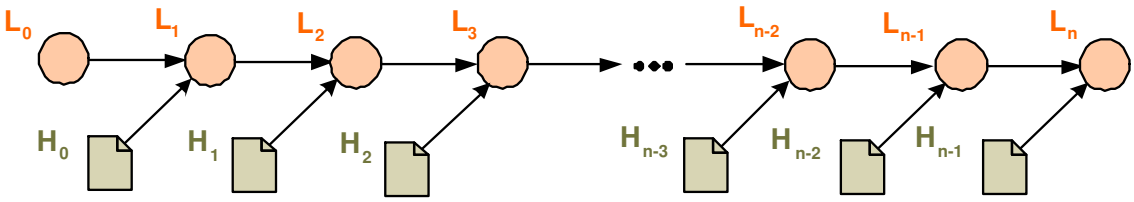


Figura 3.5: Método do Encadeamento Linear

ao número de resumos encadeados. Além disso, é necessário armazenar todo o encadeamento para possibilitar a comparação entre os documentos.

3.4.2 Árvore Sincronizada

O Método da Árvore Sincronizada também utiliza um esquema de protocolação relativa e, portanto, existe um encadeamento dos documentos em uma ordem temporal. No entanto, ele utiliza o conceito de saltos, que tem como objetivo diminuir o tempo de comparação da precedência entre dois documentos (PASQUAL; DIAS; CUSTÓDIO, 2002).

Este método foi proposto por Pasqual (2001) em sua dissertação de mestrado, porém não apresenta de forma detalhada como são são gerados os saltos. Com o objetivo de facilitar o entendimento, esta subseção descreve de forma didática e detalhada o Método da Árvore Sincronizada.

Antes de prosseguir, é necessário definir alguns conceitos utilizados:

- **Rodada**: Período de tempo ou quantidade máxima de resumos necessária para a emissão de um recibo;

- **Ponto de Confiança**: São os pontos tornados públicos da cadeia de protocolação. Após a publicação, o encadeamento anterior ao ponto publicado pode ser exportado para um meio de armazenamento externo, para uma eventual auditoria. A base de dados passa a ter apenas o último *link* do encadeamento como o novo Ponto de Confiança. Os pontos de confiança são representados por C_i;

- **Ponto de Salto**[1]: São os pontos que criam saltos e permitem diminuir o caminho entre uma rodada de protocolação e o Ponto de Confiança. Os pontos de salto são representados por S_i;

- **Recibo**: Contém o encadeamento de sua rodada, bem como o encadeamento das rodadas anteriores até o Ponto de Confiança mais próximo.

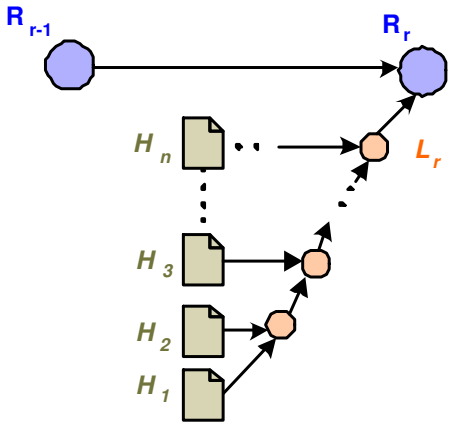


Figura 3.6: Rodada no Método da Árvore Sincronizada

A Figura 3.6 ilustra uma rodada no Método da Árvore Sincronizada. Os resumos dos documentos enviados para a AD para serem protocolados são representados por H_i. Os dois primeiros resumos, H_1 e H_2 são submetidos a uma função F, de sentido único, como um *hash*, por exemplo. O resultado desta função será um *link* intermediário, que, por sua vez, será submetido à função F juntamente com o resumo H_3. Este encadeamento será realizado sucessivamente, até que o último resumo H_n seja encadeado com o último *link* intermediário. Desta forma, os resumos enviados em uma dada rodada constituem uma árvore, onde as folhas são os resumos H_i e a raiz é o *link* L_r, o qual depende de todos os resumos da rodada. Ao final da rodada, a função F será aplicada sobre o *link* L_r e o *link* R_{r-1}, que representa a rodada anterior. O resultado desta função constitui o *link* R_r, que representa a rodada atual.

[1]Quando o Método da Árvore Sincronizada foi proposto, o termo "Ponto de Sincronismo"foi originalmente utilizado para representar o ponto onde ocorreu o salto. Contudo, após uma análise da semântica do termo, decidiu-se adotar a expressão Ponto de Salto, visto que o termo Ponto de Sincronismo é mais apropriado para designar o ponto criado em uma protocolação cruzada.

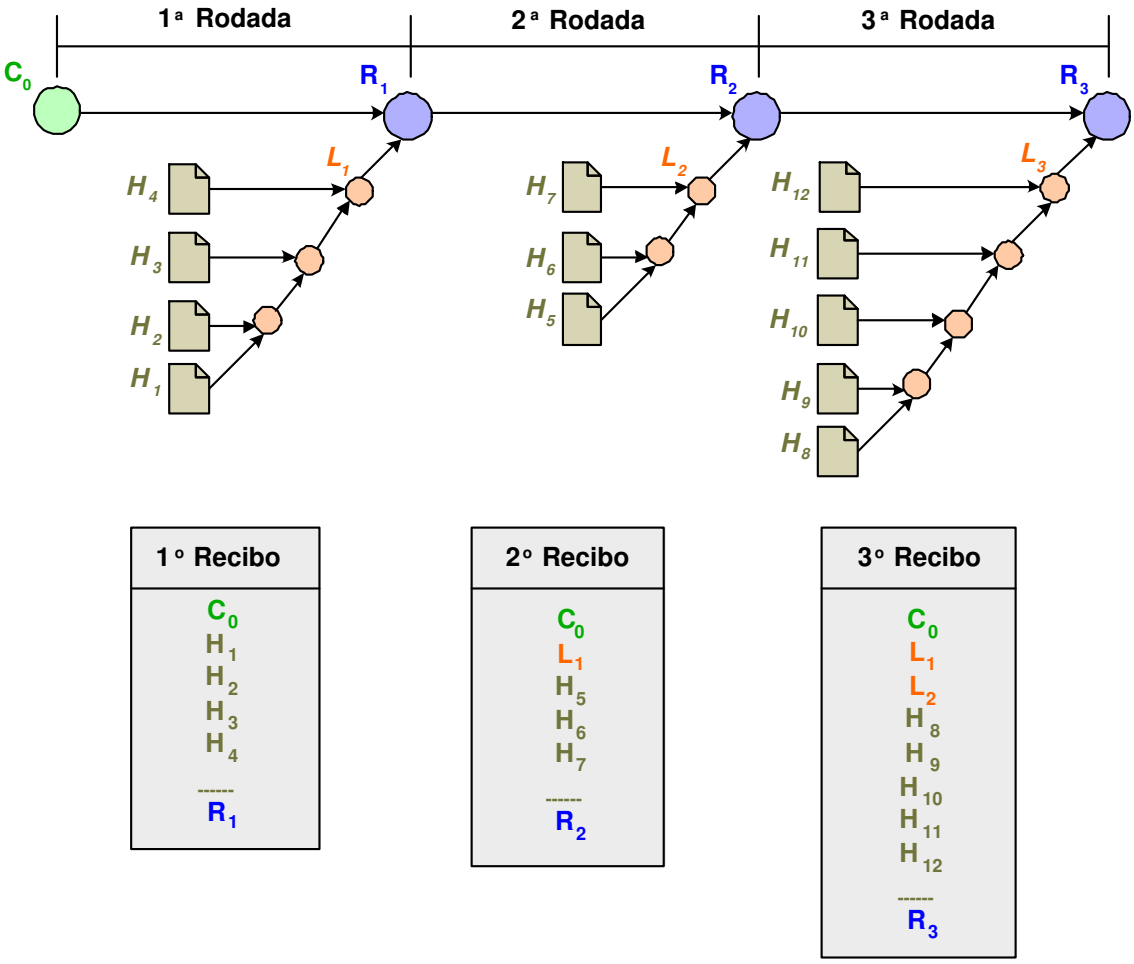


Figura 3.7: Método da Árvore Sincronizada com três rodadas

A Figura 3.7 ilustra um exemplo de encadeamento com três rodadas. Observando a figura, percebe-se que o número de resumos em cada rodada é variável, visto que depende do número de requisições enviadas pelos usuários. Abaixo de cada rodada, a figura ilustra o recibo que é gerado e emitido para os usuários que enviaram um resumo na mesma rodada. Nota-se que todos os recibos contêm o Ponto de Confiança C_0, os resumos H_i enviados na rodada, além dos *links* L_i das rodadas anteriores. A partir destas informações, o usuário pode verificar a validade do recibo. Esse assunto será tratado com mais detalhes no capítulo 5.

Nota-se que o tamanho do recibo é proporcional ao tamanho do encadeamento. Por conseguinte, o tempo necessário para pesquisar um resumo no encadeamento

tende a ser muito grande. Com o objetivo de diminuir o tamanho do recibo, e conseqüentemente, o tempo de busca por um resumo, o Método da Árvore Sincronizada propõe o conceito de saltos.

A Figura 3.8 ilustra um exemplo de encadeamento com saltos. O primeiro *link* do encadeamento é o Ponto de Confiança C_0. O primeiro salto é representado pelo arco que parte de C_0 e vai até R_3. Para criar este salto sobre as três primeiras rodadas, um Ponto de Salto é gerado, o qual é representado por S_1. Este ponto é calculado da seguinte maneira:

$$S_1 = F(C_0, R_3) \tag{3.3}$$

Desta forma, o Ponto de Salto S_1 depende de todos os resumos das rodadas sob o salto. A partir da terceira rodada, os resumos serão encadeados diretamente com o Ponto de Salto S_1, já que ele representa todas as rodadas sob o salto. Os saltos são utilizados para diminuir a distância entre a rodada atual e o Ponto de Confiança, por isso, sempre que houver um salto de nível mais alto, o mesmo será utilizado.

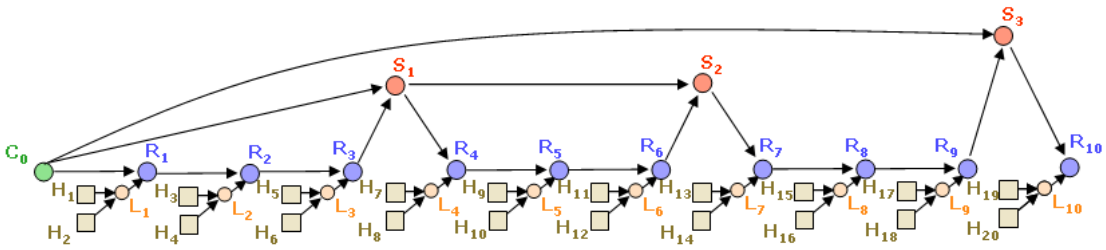


Figura 3.8: Saltos no Método da Árvore Sincronizada

A Figura 3.9 ilustra o conteúdo dos recibos correspondentes a cada rodada do encadeamento.

O segundo salto é representado pelo arco que parte do Ponto de Salto S_1 e vai até R_6. O novo Ponto de Salto S_2 é gerado através do cálculo:

$$S_2 = F(S_1, R_6) \tag{3.4}$$

Recibo correspondente à rodada									
1ª	2ª	3ª	4ª	5ª	6ª	7ª	8ª	9ª	10ª
C_0	C_0	C_0	C_0	C_0	C_0	C_0	C_0	C_0	C_0
H_1	L_1	L_1	R_3	R_3	R_3	R_3	R_3	R_3	R_9
H_2	H_3	L_2	H_7	L_4	L_4	R_6	R_6	R_6	H_{19}
---	H_4	H_5	H_8	H_9	L_5	H_{13}	L_7	L_7	H_{20}
R_1	---	H_6	---	H_{10}	H_{11}	H_{14}	H_{15}	L_8	---
	R_2	---	R_4	---	H_{12}	---	H_{16}	H_{17}	R_{10}
		R_3		R_5	---	R_7	---	H_{18}	
					R_6		R_8	---	
								R_9	

Figura 3.9: Recibos no Método da Árvore Sincronizada

A partir da próxima rodada, os resumos serão encadeados diretamente com S_2. Os saltos podem ser de vários níveis, visto que podem haver saltos sobre outros saltos. Para gerenciá-los, a AD utiliza algumas listas que armazenam os *links* que geram os saltos. Existe uma lista para gerenciar cada nível. A lista de nível 0 contém os *links* L_i das rodadas onde não ocorre salto, a lista de nível 1 contém os *links* R_i que compõem os saltos de nível 1, a lista de nível 2 contém os *links* R_i que compõem os saltos de nível 2 e assim por diante.

Enquanto não ocorre nenhum salto, os *links* L_i são armazenados na lista de nível 0. O primeiro salto ocorre quando a lista de nível 0 atinge o seu tamanho máximo. Neste momento, ela é zerada e a lista de nível 1 passa a conter o R_i que originou o salto. Após isto, a lista de nível 0 passa a armazenar os próximos *links* L_i até atingir o seu tamanho máximo novamente. Quando isso ocorrer, um novo salto de nível 1 é gerado a partir do primeiro Ponto de Salto S_i e do R_i atual. A lista de nível 0 é zerada e o R_i que originou o salto é adicionado na lista de nível 1. Este procedimento continuará até que a lista de nível 1 também alcance o seu tamanho máximo. Quando isso ocorrer, a lista de nível 0 e a lista de nível 1 serão zeradas e o R_i que gerou o salto será adicionado à lista de nível 2.

Estas operações de preencher as listas de nível menor até que atinjam seu tamanho máximo, adicionar o R_i que gerou o salto à lista superior e zerar todas as

listas inferiores, ocorre até que todas as listas estejam completas. Quando isso acontecer, a AD deverá exportar seu encadeamento para um meio de armazenamento externo e publicar um Ponto de Confiança.

Rodada									
1ª		2ª		3ª		4ª		5ª	
N_0		N_0	L_1	N_0	L_1 - L_2	N_0		N_0	L_4
N_1		N_1		N_1		N_1	R_3	N_1	R_3
N_2		N_2		N_2		N_2		N_2	
Rodada									
6ª		7ª		8ª		9ª		10ª	
N_0	L_4 - L_5	N_0		N_0	L_7	N_0	L_7 - L_8	N_0	
N_1	R_3	N_1	R_3 - R_6	N_1	R_3 - R_6	N_1	R_3 - R_6	N_1	
N_2		N_2		N_2		N_2		N_2	R_9

Figura 3.10: Listas de gerência de saltos

A Figura 3.10 ilustra a configuração das listas utilizadas pela AD para gerenciar os saltos para o caso do encadeamento apresentado na Figura 3.8. Neste exemplo didático, para efeito de simplificação, adotou-se que o tamanho máximo das listas é de 2 (dois) *links* e que o número de níveis de saltos suportado é 2 (dois). A cada rodada o conteúdo das listas de nível 0, 1 e 2 (N0, N1 e N2, respectivamente) é alterado. A partir destas listas, a AD consegue administrar o momento em que um salto deve ser gerado.

3.5 Módulos Criptográficos de *Hardware*

Módulos criptográficos de *hardware* são mecanismos que executam serviços específicos de criptografia, como cifragem de dados, autenticação, assinatura digital e gerenciamento de chaves criptográficas (NIST, 2002). Estes módulos podem ser compostos de *hardware*, *software*, e *firmware*[2], ou pela combinação destes elementos.

[2] *Firmware*: programas e dados que são armazenados em *hardware*, por exemplo, ROM, PROM, EPROM, EEPROM e FLASH, e não podem ser dinamicamente modificados durante a execução.

O Instituto Nacional de Padrões e Tecnologia americano (NIST) estabelece, através do padrão FIPS PUB 140-2 (NIST, 2002), os requisitos de segurança para módulos criptográficos utilizados em sistemas de segurança, para proteger informações sensíveis em sistemas computacionais ou de telecomunicação. Este padrão especifica quatro níveis de segurança:

Nível 1: Provê o menor nível de segurança. São especificados requisitos de segurança básicos para módulos criptográficos. Neste nível, nenhum mecanismo de segurança física é especificado. Um exemplo de módulo criptográfico que se enquadra neste nível é uma placa de cifragem em um computador pessoal;

Nível 2: Melhora os mecanismos de segurança física dos módulos criptográficos que se encontram no nível 1, através da adição de lacres. Para se ter acesso físico ao equipamento é necessário quebrar estes lacres, o que seria facilmente detectado. Este nível requer uma autenticação baseada em papéis, em que o módulo criptográfico autentica o usuário, e este possui um papel específico, o qual autoriza a execução de determinado conjunto de ações.

Nível 3: Em adição aos mecanismos de segurança física utilizados no nível 2. O nível 3 tenta prevenir que um intruso acesse o CSP[3]. Estes mecanismos de segurança física tem como objetivo obter uma alta probabilidade de detecção e reação a tentativas de acesso físico, uso ou modificação do módulo criptográfico. Estes mecanismos de segurança física podem incluir o uso de circuitos que, ao detectar alguma tentativa de acesso, zeram todas as informações que estão contidas no CSP e que não estão cifradas. Esta ação pode ser executada, quando, por exemplo, a cobertura de um módulo criptográfico é aberta. Este nível requer mecanismos de autenticação baseados em identidade, melhorando a segurança provida pelos mecanismos de autenticação baseados em papéis especificados para o nível 2. O módulo criptográfico autentica a identidade de um operador e verifica se o mesmo está autorizado a assumir um papel específico, o qual lhe permite executar um conjunto de ações. O nível

[3]*Critical Security Parameter:* informações relacionadas a segurança, tais como, chaves criptográficas, dados de autenticação, como senhas, cuja descoberta ou modificação pode comprometer a segurança de um módulo criptográfico.

3 requer que as entradas ou saídas de informações não cifradas que se encontram no CSP sejam manipuladas através de portas separadas fisicamente, ou interfaces que estejam logicamente separadas, utilizando para isso, caminhos confiáveis de outras interfaces. Tais informações devem ser introduzidas no módulo criptográfico e extraídas do mesmo de forma cifrada.

Nível 4: Provê o mais alto nível de segurança definido no padrão. Neste nível, os mecanismos de segurança física provém um "envelope"completo de proteção ao redor do módulo criptográfico, com o objetivo de detectar e responder a qualquer tentativa de acesso físico não autorizado. Intrusões possuem uma probabilidade muito alta de detecção, e como conseqüência, todos as informações não cifradas contidas no CSP são zeradas imediatamente. Módulos criptográficos que se encontram no nível 4 são úteis para operações em ambientes desprotegidos fisicamente. Este nível também protege o módulo criptográfico contra flutuações da temperatura ou da tensão do ambiente.

3.6 Empresas que oferecem soluções de protocolação digital

Atualmente existem várias empresas que oferecem o serviço de protocolação digital. A seguir são apresentados os produtos oferecidos por algumas empresas.

3.6.1 *BRy*

A BRy (2003) é uma empresa brasileira que oferece um produto de protocolação digital chamado Servidor de Confiança *BRy* PDDE (Protocoladora Digital de Documentos Eletrônicos). A empresa oferece três modelos:

- ***BRy* PDDE 200:** Utiliza o Método da Árvore Sincronizada, oferece segurança BSM, relógio *BRy* e possui capacidade de gerar até 6.000 protocolos/hora;

- ***BRy* PDDE 300:** Utiliza o Método da Árvore Sincronizada, oferece segurança BSM, relógio *BRy*, sincronismo com o Observatório Nacional, possui capacidade para gerar até 15.000 protocolos/hora e possui módulos de administração de usuários, contabilidade e auditoria do encadeamento;

- ***BRy* PDDE 400:** Utiliza o Método da Árvore Sincronizada, oferece segurança *HSM nCipher* ou *Rainbow*, sincronismo com o Observatório Nacional, possui capacidade para gerar até 15.000 protocolos/hora, possui módulos de administração de usuários, contabilidade e auditoria, placa de relógio (rubídio) e um kit SDK com transferência de tecnologia.

Os produtos oferecidos utilizam um método de datação híbrida, composto pelos métodos Absoluto e Árvore Sincronizada, sendo que as informações de data e hora são fornecidas por servidores externos de tempo. A empresa fornece um *software* cliente chamado *BRyX* que gera requisições de protocolação e verifica a assinatura digital da AD sobre o recibo. A PDDE também oferece mecanismos para integrar outros sistemas[4] ao serviço de protocolação. Esta integração pode ser feita através de um *Kit* de desenvolvimento.

3.6.2 *Cybernetica*

O sistema de protocolação digital oferecido pela Cybernetica (2002) utiliza um método de datação híbrida, o qual é composto pelos métodos: Absoluto e Encadeamento em Árvore. O equipamento utilizado para prover o serviço consiste de um servidor de protocolação, um módulo seguro de *hardware* certificado com o nível 4 da FIPS 140-1 e um dispositivo GPS para sincronização com o relógio do servidor. O servidor de protocolação assina todos os recibos emitidos com uma chave privada RSA. A chave é utilizada e armazenada em um módulo seguro de *hardware* certificado com o nível 4 da FIPS 140-1. Também é fornecido um serviço de renovação de recibos. Entretanto, o serviço de protocolação somente renova os recibos por ele emitidos, evitando, assim, aceitar recibos falsos.

[4]Como por exemplo EDI (*Enterprise Data Interchange*), serviço de *e-mail*, etc.

O sistema de protocolação digital oferecido pela empresa provê auditoria. Para realizá-la, são necessários três componentes:

- Serviço de protocolação;
- Verificador;
- Jornal de grande divulgação.

A *Cybernetica* utiliza uma tecnologia de protocolação baseada em encadeamento, a qual vincula, de maneira criptográfica, recibos publicados aos recibos emitidos previamente. O resumo do último recibo emitido é publicado semanalmente no jornal *Ametlikud Teadaanded*. A associação criptográfica entre os recibos corretos é facilmente verificável, já que os recibos falsos não possuem esta associação. A empresa afirma realizar procedimentos de auditoria, porém não os apresenta detalhadamente.

O formato e a definição das requisições de protocolação, bem como os protocolos para verificar e renovar recibos, estão especificados no documento "*Protocols and Data Formats for Timestamping Service*"(CYBERNETICA, 2002).

3.6.3 *DigiStamp*

A DigiStamp (2003) provê o serviço de protocolação digital combinado com a utilização de assinaturas digitais. A seguir são apresentados os dois produtos oferecidos pela empresa:

- ***IP ProtectorTM* :** *Software* livre, encontrado no *site* da empresa (DIGISTAMP, 2003), o qual cria e armazena assinaturas digitais e recibos.;
- ***SecureTimeTM API Toolkit*:** Permite que os clientes integrem seus *softwares* existentes com o serviço de protocolação. O conjunto de ferramentas permite que o programador da aplicação crie e gerencie a interface da aplicação, incluindo geração de resumos, serviço de formatação de mensagens, análise de respostas, seleção de servidor de protocolação e funções de comunicação.

O sistema de protocolação digital utiliza um método de datação absoluta e um *hardware* especializado para cifragem, o qual é certificado pelo NIST e provê detecção contra ataques físicos e eletrônicos, garantindo a integridade da chave privada utilizada para assinar os recibos. O *hardware* seguro também contém um relógio, o qual, segundo a empresa, não pode ser ajustado para criar recibos inválidos e é seguramente sincronizado com um relógio atômico externo.

A empresa afirma que o recibo gerado pode ser utilizado posteriormente para verificar que o conteúdo de um determinado documento existiu em um momento do tempo, porém, não informa se algum tipo de auditoria é realizada.

3.6.4 *Surety*

A Surety (2003) oferece dois produtos de protocolação digital:

- ***AbsoluteProof Data Integrity Service*:** Permite verificar quando uma informação digital foi criada e se foi alterada desde então. Também provê *logs* de auditoria de todos os registros eletrônicos, o que permite detectar se a informação ou a data foram alteradas. Este serviço inclui:
  - Geração de evidência de que determinado registro eletrônico foi criado e quando isso ocorreu;
  - Solução de integridade de dados por tempo indefinido, a qual é construída através de tecnologia patenteada e de algoritmos seguros de *hash*;
  - Protocolação e validação virtual de qualquer registro eletrônico.
- ***Digital Notary Engine*:** Permite que o usuário certifique o conteúdo de um documento eletrônico e a data em que este foi criado. Este serviço permite afirmar que:
  - Um determinado registro foi criado em uma determinada data e hora;
  - Este registro não foi alterado desde então.

O serviço de protocolação digital utiliza duas técnicas criptográficas: funções *hash* e o esquema de Encadeamento em Árvore. A *Surety* atualmente utiliza uma combinação da função *hash* MD5 com SHA-1 (SURETY, 2003). O método de datação utilizado é híbrido, visto que combina o Encadeamento em Árvore com a datação absoluta.

O recibo gerado contém informações como data e hora em que ocorreu a protocolação, além dos resumos de níveis intermediários da árvore. Dessa forma, o usuário pode validar seu recibo no futuro, através do re-cálculo dos resumos até a raiz da árvore.

Uma vez por semana, a *Surety* publica um valor na seção de Notícias Comerciais da edição nacional do *New York Times*. Este valor representa as impressões digitais combinadas dos documentos protocolados durante os sete dias anteriores. Desta forma, diminui-se a probabilidade de que alguém consiga protocolar documentos com datas retroativas. Além disso, a empresa afirma realizar auditoria sobre o sistema, porém não descreve como é realizada.

3.6.5 *Symmetricom*

A Symmetricom (2003) oferece um produto chamado *Trusted Time StampServers*, o qual é um sistema de protocolação digital que adota os padrões de segurança da FIPS 140-1 nível 3 e é passível de auditoria. O produto utiliza um método de datação absoluta e provê canais seguros e rastreáveis com fontes oficiais de tempo.

As operações são executadas dentro de um HSM[5]. Além disso, existe um serviço de certificação de tempo, chamado *Sovereign Time StampServer* que garante que os recibos são precisos e passíveis de auditoria. Os *StampServers* são calibrados por uma terceira parte confiável e independente via uma conexão de rede segura. Uma vez calibrado, o *StampServer* está pronto para realizar protocolações para qualquer requisição que siga o padrão RFC 3161 (ADAMS, 2001).

O recibo gerado é composto pela data e hora da protocolação, o resumo

[5]HSM - *Hardware Secure Mode*: conjunto de *hardware*, *software* ou *firmware* que implementa funções de segurança, tais como, algoritmos criptográficos e geração de chaves.

do documento e um ponteiro para um certificado de calibragem do tempo. Este ponteiro provê a informação necessária para confirmar que o recibo é preciso, válido e provê rastreabilidade até a autoridade oficial de tempo.

A empresa oferece *StampServers* com dois tipos diferentes de proteção criptográfica:

- **StampServer^{TM} SA100:** Provê mais de 50 protocolações por segundo, utilizando 1024 *bits*. Utiliza o co-processador criptográfico IBM 4758 e Arquitetura Criptográfica Comum da IBM para garantir a integridade das operações de protocolação;
- **StampServer^{TM} SA200n:** Provê mais de 125 protocolações por segundo, utilizando 1024 *bits*. Utiliza HSM *nShield^{TM}* da *nCipher* e utiliza tecnologia SEE (*Secure Execution Engine^{TM}*) para proteger todas as operações de protocolação.

O *Sovereign Time^{TM}* é um *software* independente da AD. Este serviço inclui:

- Calibragem e certificação do tempo do *StampServer* SA100;
- Validação e garantia dos recibos emitidos;
- Verificação das assinaturas digitais e dos formatos;
- Validação dos *logs* de auditoria e da cadeia de certificação;
- Provê rastreabilidade com a fonte oficial de tempo;
- Documentação assinada da informação de auditoria.

3.6.6 *TimeProof*

A TimeProof (2003) desenvolve sistemas de assinaturas temporais e fabrica um *hardware* capaz de protocolar documentos eletrônicos. Esta *Trust Box*, como eles definem, funciona em parceria com o *software* que é instalado no servidor, o qual tem as funções de conectar o *hardware* à rede e registrar em um *log* todos os eventos de protocolação. A *TimeProof* disponibiliza três tipos de *hardware*:

- **TSS 380:** Foi desenvolvido para serviços comerciais. Este sistema disponibiliza um serviço de protocolação digital para os usuários que desejam autenticar suas transações eletrônicas na *Internet*;

- **TSS 400:** Foi desenvolvido para Autoridades de Datação que desejam prover um serviço de protocolação digital;

- **TSS 80:** Foi desenvolvido para empresas que almejam prover autenticação temporal para todos os documentos e processos.

A assinatura temporal da *TimeProof* utiliza função resumo do tipo SHA-1, além do formato PKCS#7 para a assinatura digital. A protocolação segue o padrão estabelecido na RFC 3161 (ADAMS, 2001) e um formato derivado do PKCS#7 (KALISKI, 1998). A *TimeProof* recebe a hora oficial (UTC) de um sinal GPS (*Global Positioning System*) ou da estação de rádio oficial alemã DCF-77 AM. A estação de rádio tem como fonte de tempo o PTB (*Physikalisch Technische Bundesanstalt*), que é responsável por gerar a hora oficial.

O servidor de protocolação é composto por uma *trustbox*, que contém um receptor do sinal de tempo, e por um conjunto de *smartcards* que manipulam e respondem as requisições dos clientes. O sistema inclui um relógio interno preciso, o qual é continuamente comparado com o sinal externo. No caso de pequenos desvios, o relógio interno é ajustado. Já no caso de grandes desvios, o sistema de supervisão emite um alarme.

Cada evento do sistema é registrado na *trustbox* através de um *log*. Segundo a empresa, o tempo não pode ser alterado dentro da *trustbox*, pois este equipamento possui funções de supervisão que monitoram a correta operação e informam o administrador por *e-mail*. Além disso, a empresa afirma oferecer alguns serviços de auditoria, porém, não descreve com detalhes o funcionamento de tais serviços.

3.7 Conclusão

Neste capítulo foram apresentados os sistemas de protocolação de documentos tradicionais e de documentos eletrônicos, bem como alguns métodos de datação relativa. Também foram descritas as características de um módulo criptográfico de *hardware*. Por fim, foram apresentadas as soluções de protocolação digital oferecidas por algumas empresas.

Dentre os métodos de datação existentes, sugere-se que a AD opte por um método de datação híbrida. Dessa forma, o sistema poderá oferecer documentos protocolados com precisão e confiança. A precisão é assegurada através da sincronização com uma fonte de tempo confiável e a confiança é obtida através da realização de auditorias sobre o encadeamento.

Capítulo 4

Aspectos relevantes da confiança na protocolação digital

4.1 Introdução

Antes do surgimento dos métodos de datação relativa, para que um sistema de protocolação digital fosse considerado confiável, era necessário confiar na AD, ou seja, acreditar que ela estava protocolando corretamente os documentos. Atualmente, já existem alguns mecanismos que ajudam a reduzir a necessidade de se confiar na AD. Dessa forma, se a AD agir de maneira maliciosa, existem meios de descobrir a fraude. Porém, o sistema de protocolação digital ainda não é completamente confiável. Portanto, é necessário criar outros mecanismos que reduzam ainda mais a necessidade de confiar na AD.

A seção 4.2 descreve os elementos que constituem a confiança do sistema de protocolação digital. Na seção 4.3 são apresentados os mecanismos já existentes que ajudam a reduzir a necessidade de se confiar na AD. Na seção 4.4 são levantadas algumas questões referentes à confiança da protocolação digital e a seção 4.5 apresenta algumas propostas de melhorias que visam aumentar a confiança do sistema. Na seção 4.6 serão apresentadas as considerações finais.

4.2 Tripé de Confiança

Como ilustra a Figura 4.1, a questão da confiança do sistema digital de documentos eletrônicos está vinculada a três elementos:

- **Tempo:** Necessidade de saber quando determinada protocolação foi realizada. A questão não é simplesmente ter uma fonte de tempo que forneça data e hora no momento da protocolação, mas sim, saber se esta informação é confiável e se não será alterada posteriormente;

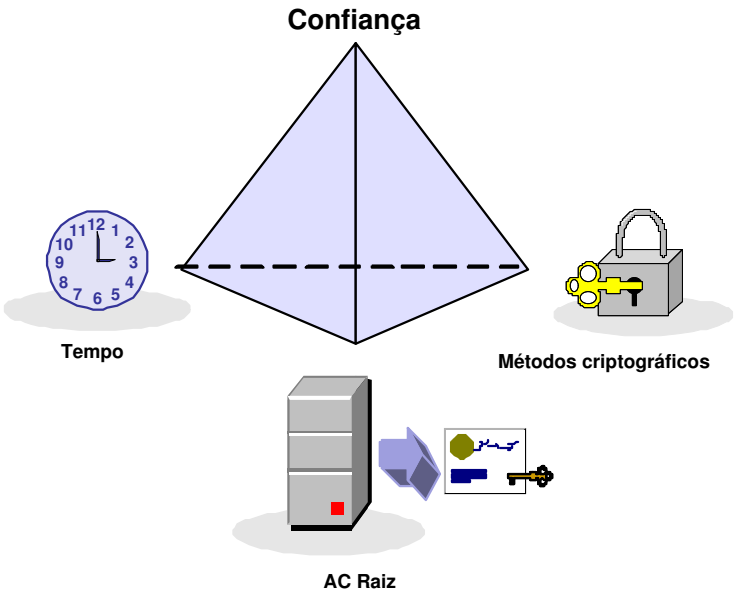


Figura 4.1: Tripé de Confiança

- **Métodos criptográficos:** Não deve ser computacionalmente possível quebrar os algoritmos criptográficos utilizados;
- **AC-Raiz:** Para que um certificado digital seja válido, é necessário confiar na Autoridade Certificadora (AC) que o emitiu e em sua Cadeia de Certificação (CC).

Caso algum dos elementos citados anteriormente seja comprometido, a confiança, como um todo, será afetada. Portanto, para garantir a confiabilidade de um sistema de protocolação digital, é necessário utilizar mecanismos que assegurem cada um dos elementos que constituem o tripé de confiança.

4.2.1 Confiança no tempo

Em sistemas que utilizam métodos de datação absoluta, o tempo só poderá ser considerado confiável, se a fonte responsável por emitir esta informação também for confiável. No Brasil, o governo estabeleceu que o Observatório Nacional (ON, 2003) é a entidade responsável por oferecer a hora oficial. Assim, o tempo fornecido pelo ON é considerado confiável.

Já os sistemas que utilizam métodos de datação relativa não possuem a informação do momento exato em que um documento foi protocolado, mas sim, a ordem temporal entre os documentos. Neste tipo de sistema, a confiança não está relacionada com uma fonte de tempo confiável, mas sim com o encadeamento armazenado no banco de dados interno da AD. Para confiar na ordem dos documentos protocolados, é necessário ter certeza de que o encadeamento não poderá ser alterado. Isto pode ser obtido através de mecanismos como a publicação dos Pontos de Confiança. Desta forma, se a ordem entre os documentos for alterada, isto pode ser detectado através da verificação do encadeamento a partir do Ponto de Confiança até o documento. Em caso de fraude, os *links* calculados não corresponderão com os armazenados no banco de dados.

4.2.2 Confiança nos métodos criptográficos

Os métodos criptográficos são utilizados no cálculo do resumo dos documento, na assinatura digital dos recibos e no cálculo do encadeamento (no caso de sistemas que utilizem um método de datação relativa). Os algoritmos criptográficos utilizados são considerados "seguros", quando a única alternativa que resta é um ataque por força bruta. Para tornar este tipo de ataque quase impossível, alguns artifícios são utilizados, como utilizar um tamanho de chave muito grande, por exemplo. Dessa forma, o tempo necessário para executar o ataque, o tornaria inviável na prática. Entretanto, com o avanço da tecnologia, este tempo pode ser reduzido e, em razão disso, os algoritmos criptográficos devem passar por revisões periódicas, com o objetivo de avaliar se não foram comprometidos.

4.2.3 Confiança na AC-Raiz

Os certificados digitais utilizados no processo de protocolação digital também devem ser confiáveis. Para tanto, é necessário verificar a sua validade, antes de utilizá-lo. Esta verificação envolve:

- Verificar se o certificado digital é apresentado em um formato válido;
- Verificar se a data atual não é maior do que a data de validade do certificado para averiguar se ele expirou;
- Verificar se o certificado não foi revogado. Para tanto, deve-se consultar a Lista de Certificado Revogados (LCR) e verificar se o certificado consta na lista;
- Para confiar na AC que emitiu o certificado, é necessário confiar na outra AC que emitiu o seu certificado e, assim, sucessivamente. Logo, é necessário confiar em toda a Cadeia de Certificação (CC), desde o certificado digital até a AC-Raiz, a qual deve ser uma AC confiável.

4.3 Mecanismos existentes

Atualmente existem alguns mecanismos que ajudam a aumentar a confiança do sistema de protocolação digital de documentos eletrônicos. Entre eles, podem-se citar:

- Adoção de um método de datação que utilize autenticação temporal relativa, pois cria e armazena um encadeamento dos documentos protocolados, o que permite uma posterior verificação da ordem temporal entre eles;
- Adoção de recomendações de segurança física e lógica, como por exemplo, FIPS 140-2 (NIST, 2002). Estas recomendações prevêem utilização de lacres, entre outros mecanismos, com o objetivo de detectar a violação da AD;

- Publicação do Ponto de Confiança, pois cria uma âncora de confiança, permitindo que alterações na ordem temporal entre os documentos protocolados sejam identificadas.

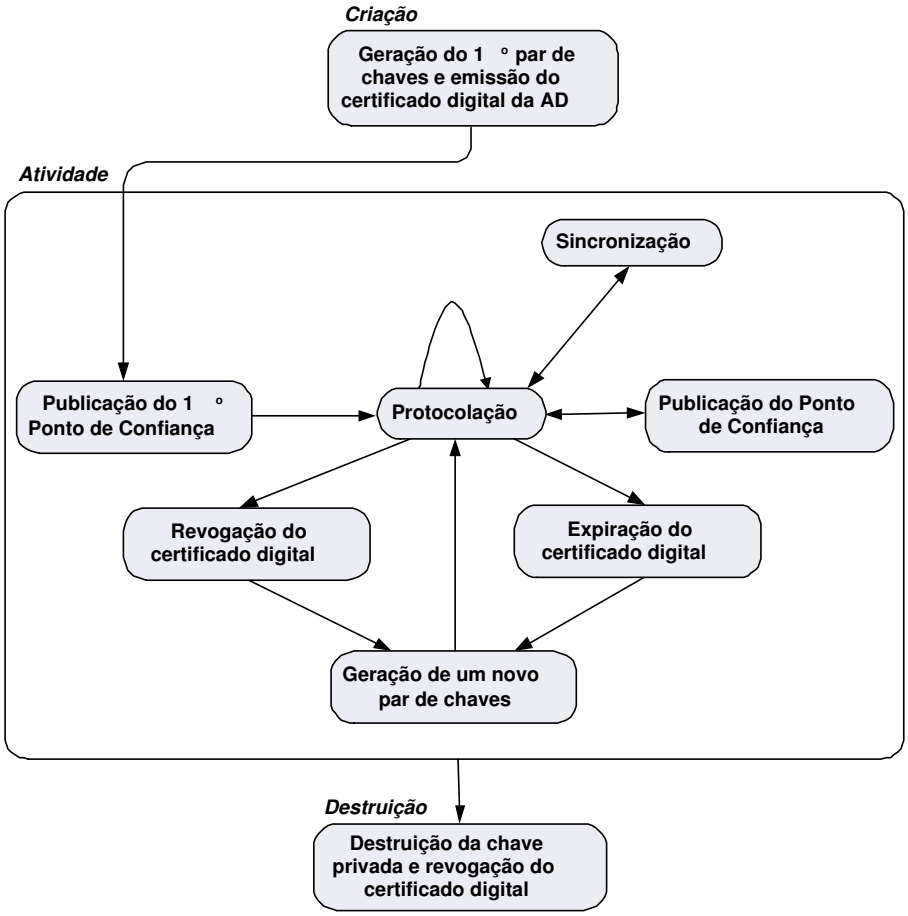


Figura 4.2: Ciclo de vida de uma AD

Apesar da existência destes mecanismos, é necessária a adoção de outros procedimentos para que o processo de protocolação seja mais confiável.

4.4 Questões referentes à confiança na protocolação digital

A Figura 4.2 ilustra as fases do ciclo de vida de uma AD. Quando a AD é criada, um par de chaves é criado e o certificado digital correspondente é emitido em seu nome. Antes de começar a protocolar os documentos, a AD publica o primeiro Ponto de Confiança do encadeamento, o qual pode ser um número randômico, por exemplo. A partir disso, a AD está preparada para receber requisições. Durante sua operação, a AD publica Pontos de Confiança intermediários com o objetivo de facilitar a verificação do encadeamento. Durante o período em que a AD está em operação, seu certificado digital pode expirar ou ser revogado. Nesse caso, um novo par de chaves é gerado e a AD reinicia suas atividades. Além disso, a AD pode sincronizar periodicamente seu relógio interno com uma fonte de tempo confiável. Finalmente, quando a AD é destruída, sua chave privada é destruída e seu certificado digital é revogado.

Existem várias questões relacionadas à confiança em cada etapa do ciclo de vida de uma AD:

- Como garantir a integridade do encadeamento armazenado no banco de dados da AD?

- Como, onde e com que freqüência serão publicados os Pontos de Confiança?

- Por quanto tempo pode-se confiar em um recibo de protocolação? O que acontece quando a tecnologia utilizada no momento da assinatura digital da AD não for mais considerada segura?

- Como garantir ao usuário do sistema de protocolação digital que o serviço é confiável?

4.5 Propostas para aumentar a confiança da protocolação digital

A seguir são apresentadas algumas propostas que visam aumentar a confiança do sistema de protocolação digital. Tais propostas visam solucionar as questões levantadas anteriormente.

4.5.1 Auditoria

Como garantir a integridade do encadeamento armazenado no banco de dados da AD?

Propõe-se a realização de procedimentos de auditoria para inspecionar as atividades desenvolvidas pela AD. Entre os procedimentos propostos estão: verificação da validade dos recibos, verificação da precedência entre dois documentos protocolados e verificação da integridade do encadeamento armazenado no banco de dados da AD. Os procedimentos propostos podem ser aplicados em uma AD que utilize o Método do Encadeamento Linear ou o Método da Árvore Sincronizada. Estes procedimentos são apresentados com mais detalhes no capítulo 5.

4.5.2 Publicação do Ponto de Confiança

Como, onde e com que freqüência serão publicados os Pontos de Confiança?

Periodicamente a AD publica um *link* do seu encadeamento. Estes *links* são chamados de Pontos de Confiança, pois vinculam um ponto do encadeamento com um momento do tempo. Dessa forma, se a data de um documento protocolado após a publicação for alterada, ao re-calcular o encadeamento a fraude será constatada, já que o *link* correspondente ao documento não dependerá mais do Ponto de Confiança. A Figura 4.3 ilustra como é realizada a publicação.

Inicialmente, o banco de dados interno da AD armazena um encadeamento com n rodadas e o atual Ponto de Confiança é representado por C_0. No momento da publicação, o último *link* do encadeamento, no caso R_n, é encadeado com o resumo

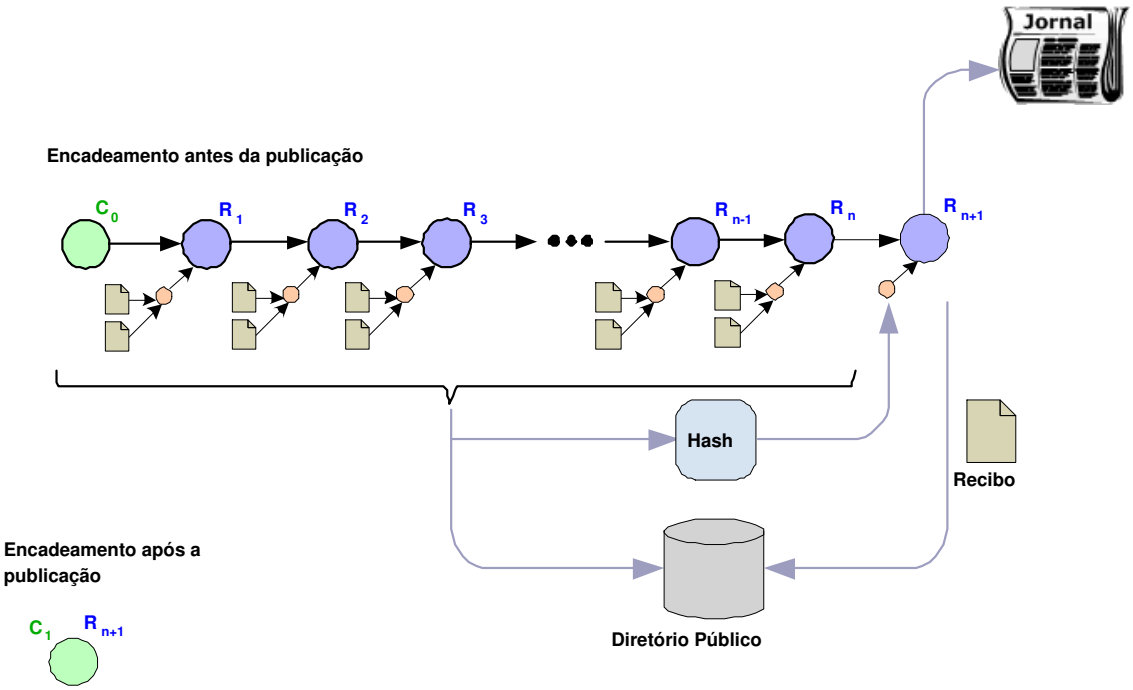


Figura 4.3: Publicação do Ponto de Confiança

de todo o encadeamento, gerando, assim, R_{n+1}. Este *link* é publicado em um meio de grande circulação. A seguir, os *links* são exportados para um meio de armazenamento externo, o qual pode ser um banco de dados, um disco rígido, um CD, etc. Após a exportação, o banco de dados interno da AD conterá apenas um único *link*, R_{n+1}. A partir deste momento, R_{n+1} é o novo Ponto de Confiança e é representado por C_1. Dessa forma, a publicação poderá ser verificada posteriormente, visto que o recibo referente à rodada R_{n+1} conterá o resumo do encadeamento e o momento em que a publicação ocorreu. Além disso, todas estas informações estarão assinadas pela AD, o que permite verificar a integridade dessas informações.

Os Pontos de Confiança devem ser publicados em um jornal nacional de grande circulação, como já ocorre em muitos países, como nos Estados Unidos, por exemplo.

Quanto a freqüência das publicações, isto varia de acordo com a demanda de requisições de protocolação de cada AD. Entretanto, é preciso ter um cuidado, pois um período muito grande sem publicação pode ocasionar lentidão no processo de

verificação do encadeamento, visto que a cadeia de protocolação armazenada no banco de dados tende a ficar muito extensa.

4.5.3 Renovação de recibos

Por quanto tempo pode-se confiar em um recibo de protocolação? O que acontece quando a tecnologia utilizada no momento da assinatura digital da AD não for mais considerada segura?

Os algoritmos criptográficos utilizados durante a protocolação digital são considerados seguros quando os artifícios utilizados, como um tamanho grande de chave, por exemplo, são suficientes para assegurar que o tempo necessário para realizar um ataque por força bruta é realmente muito grande. Porém, com a evolução da tecnologia, o poder de processamento dos computadores aumenta e pode tornar possível a quebra de um algoritmo em um tempo razoável. Se isto acontecer, os recibos de protocolação não podem mais ser considerados válidos, pois eles podem ser facilmente forjados.

Para evitar que isso ocorra, é necessário criar um processo de renovação dos recibos. Para tanto, o sistema de protocolação deve suportar, além das mensagens de requisição de protocolação, mensagens de requisição de renovação de recibos antigos. Notoya (2002) propõe, em sua dissertação de mestrado, uma Infra-estrutura de Armazenamento e Recuperação Segura de Documentos Eletrônicos (IARSDE). A IARSDE propõe um esquema de renovação de assinaturas digitais que poderia ser adaptado para o caso da renovação dos recibos.

> A IARSDE proporciona o armazenamento e recuperação segura de documentos eletrônicos provendo o controle da expiração da validade da tecnologia utilizada para assinatura e protocolação, renovação automática antes da expiração da segurança oferecida pela tecnologia utilizada de modo a manter valor legal do documento e/ou autoria por tempo indeterminado, de forma transparente ao proprietário do documento. (NOTOYA, 2002).

A IARSDE é composta por três autoridades:

- **Autoridade de Datação (AD):** realiza as protocolações normalmente, porém oferece um serviço adicional: informar a previsão da garantia máxima da tecnologia

utilizada na assinatura do documento e do recibo por ela emitido. Esta informação é obtida através de consultas às listas de previsão de comprometimento da tecnologia mantidas pela Autoridade de Garantia de Tecnologia (AGT);

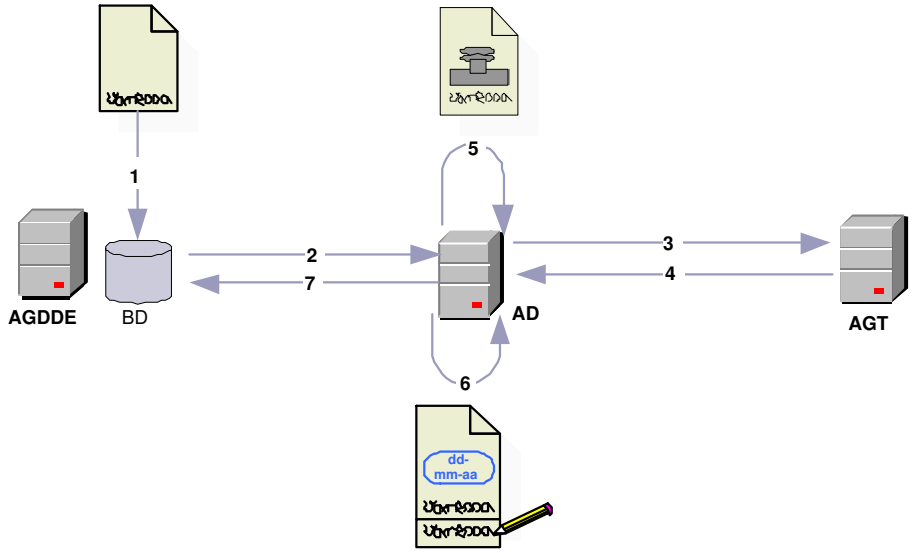


Figura 4.4: Visão geral do funcionamento da IARSDE: 1. A AGDDE recebe o documento, o organiza e armazena. 2. No prazo de validade da tecnologia, a AGDDE o envia para a AD para renová-lo. 3. A AD consulta as datas da tecnologia utilizada na reassinatura. 4. A AGT responde a solicitação da AD. 5. A AD anexa a data ao documento. 6. A AD reassina o documento. Agora o documento passa a ter uma nova assinatura através do encapsulamento da assinatura anterior. 7. A AD reenvia o documento para a AGDDE, que o armazena novamente até o próximo vencimento da validade da tecnologia.

- **Autoridade de Gerenciamento de Depósitos de Documentos Eletrônicos (AGDDE):** responsável por distribuir e recuperar informação na rede, garantindo a integridade do documento, mesmo no caso de tentativas maliciosas de subversão da informação mantida nos servidores. Também é responsável por gerenciar e agrupar os documentos de acordo com a ordem cronológica da validade da tecnologia para o controle da expiração da mesma, ou seja, a reassinatura. Também cabe a AGDDE garantir de forma segura o documento de acordo com o modo de armazenamento selecionado para quem submeteu o documento.

- **Autoridade de Garantia de Tecnologia (AGT):** autoridade responsável por man-

ter as datas relacionadas às expectativas de comprometimento da tecnologia. Para obter estas datas, são realizados vários cálculos sobre diferentes tecnologias existentes para definir o grau de dificuldade de quebra dos algoritmos em conjunto com o tamanho da chave e estimar um tempo de confiabilidade.

A Figura 4.4 ilustra o funcionamento da IARSDE. Na prática, a AGT deve ser um serviço distribuído operado por órgãos do governo e os algoritmos devem ser padronizados. Para adaptar esta idéia para a renovação dos recibos de protocolação, o recibo deve incluir uma informação adicional, que é a expectativa de tempo pelo qual os algoritmos criptográficos utilizados permanecerão seguros.

4.5.4 Política de Protocolação

Como garantir ao usuário do sistema de protocolação digital que o serviço é confiável?

A Política de Protocolação (PP) é um documento que tem como objetivo descrever, de maneira sucinta, o papel dos componentes do sistema de protocolação, bem como suas responsabilidades, práticas, obrigações e direitos. Além disso, este documento proporciona aos usuários um melhor entendimento sobre o funcionamento do sistema. Com base na PP, os usuários podem avaliar o grau de confiança do serviço provido pela AD. Por isso, recomenda-se que a AD elabore um documento contendo a sua Política de Protocolação e o disponibilize aos seus usuários. Este trabalho propõe uma Política de Protocolação, a qual é apresentada com mais detalhes no capítulo 6. Esta PP é baseada em um *Draft* de uma recomendação internacional (PINKAS; POPE; ROSS, 2003), no qual são apresentados os requisitos mínimos de uma Política de Protocolação.

4.5.5 Declaração de Práticas de Protocolação

Como garantir ao usuário do sistema de protocolação digital que o serviço é confiável?

A Declaração de Práticas de Protocolação (DPP) é um documento que tem como objetivo descrever, de maneira detalhada, como a AD implementa os procedimentos descritos na PP. Além disso, este documento proporciona aos usuários um melhor

entendimento sobre o funcionamento do sistema. Com base na DPP, os usuários podem avaliar o grau de confiança do serviço provido pela AD. Por isso, recomenda-se que a AD também elabore um documento contendo a sua Declaração de Práticas de Protocolação e o disponibilize aos seus usuários. Este trabalho propõe uma proposta de Declaração de Práticas de Protocolação, a qual é apresentada com mais detalhes no Apêndice B. Esta DPP foi elaborada para o sistema de protocolação da BRy (2003) e tem como referência a Política de Protocolação proposta neste trabalho. Além disso, esse documento pode servir de exemplo para outras ADs que desejem elaborar sua própria DPP.

4.6 Conclusão

Embora já existam alguns mecanismos que ajudam a diminuir a necessidade de confiança na AD, ainda existem várias questões relacionadas à confiança do sistema de protocolação digital. Neste capítulo foram apresentadas algumas propostas que visam aumentar a confiança do sistema.

Capítulo 5

Auditoria

5.1 Introdução

Os registros de auditoria são amplamente utilizados em administração e manutenção de sistemas no caso de falhas de *software* ou de equipamentos (LANDWEHR, 2001). Entretanto, os registros também podem ser utilizados para detectar a ocorrência de uma fraude no sistema.

Para comprovar que não houve nenhuma fraude em um sistema de protocolação digital, deve ser permitido ao usuário verificar se um determinado recibo é válido. O simples fato de possuir dois documentos com os seus correspondentes recibos não é suficiente para comprovar a autenticação temporal relativa entre os documentos, visto que qualquer pessoa pode produzir falsas cadeias de protocolação (BULDAS, 1998).

> Para aumentar a confiança dos serviços de protocolação, deveria ser possível que os clientes inspecionassem a AD periodicamente. Mesmo no caso em que a AD não agiu de forma desonesta, deveria haver um mecanismo para provar a sua inocência. Além disso, a AD deve publicar seus recibos regularmente. (BULDAS, 1998).

Para aumentar a confiança dos sistemas de protocolação digital foram elaborados procedimentos de auditoria que permitem que o cliente inspecione a AD periodicamente.

Este capítulo apresentará os procedimentos de auditoria propostos. Inicialmente, a seção 5.2 apresenta o conceito de auditoria, bem como os tipos de auditoria

que podem ser realizadas. Se a AD utiliza apenas o Método de Datação Absoluta, a auditoria sobre o encadeamento não pode ser realizada, porém a AD pode ser inspecionada de outra maneira. Esse assunto é tratado na seção 5.3. Os procedimentos para os Métodos de Datação Relativa são apresentados na seção 5.4 e podem ser aplicados em ADs que utilizam o Método do Encadeamento Linear ou o Método da Árvore Sincronizada. Finalmente, na seção 5.5 é apresentada a conclusão do capítulo.

5.2 Auditoria da protocolação digital

O ato de auditar se refere a uma revisão das atividades e dos registros de um sistema, de maneira independente (CENTER, 1998). O auditor é a entidade responsável por selecionar os eventos do sistema que serão auditados, configurar e analisar os registros que armazenarão os resultados de tais eventos.

A auditoria proposta tem como objetivo:

1. Verificar a validade de um recibo de protocolação;
2. Verificar a precedência entre dois documentos protocolados;
3. Verificar a integridade do encadeamento armazenado no banco de dados da AD;

A auditoria pode ser realizada de duas maneiras:

- **Auditoria sobre os recibos**: Utiliza as informações contidas nos recibos, bem como o Ponto de Confiança publicado pela AD em um diretório público. Neste tipo de auditoria, não é necessário consultar o encadeamento armazenado pela AD;
- **Auditoria sobre o encadeamento**: utiliza informações armazenadas internamente na AD como os *logs* e o próprio encadeamento. Devido a isto, a AD deve ser protegida com lacres de segurança para impedir o acesso de entidades não autorizadas aos componentes internos.

Os sistemas de protocolação digital que utilizam apenas um método de datação absoluta, não armazenam o encadeamento dos documentos protocolados. Em

virtude disso, a auditoria só pode ser realizada através de inspeções no equipamento ou através da análise dos registros do sistema.

No Método do Encadeamento Linear, o recibo de protocolação não contém todos os *links* que constituem o encadeamento desde o documento até o Ponto de Confiança. Portanto, em ADs que utilizam o Método do Encadeamento Linear para realizar auditoria é necessário ter acesso não só aos recibos, mas também ao encadeamento.

Como o Método da Árvore Sincronizada utiliza o conceito de saltos, o encadeamento tem o seu tamanho reduzido, o que possibilita que seja incluído nos recibos. Logo, a auditoria pode ser realizada tanto sobre o recibo como sobre o encadeamento.

5.3 Auditoria para o Método de Datação Absoluta

No método de datação absoluta, o processo de protocolar um documento consiste em anexar data e hora ao documento, sem nenhum cálculo que o vincule aos documentos protocolados anteriormente. Sem este encadeamento, a única maneira de fiscalizar o funcionamento da AD é através de inspeções no equipamento e da análise dos registros de *log* do sistema.

Neste caso, o equipamento da AD deve utilizar padrões de segurança física e lógica, como FIPS 140-2 (NIST, 2002), para possibilitar a detecção de violações físicas. Para isso, são utilizados lacres de segurança e dispositivos eletrônicos que podem, por exemplo, destruir a chave privada da AD, quando uma violação for detectada. A seção 3.5 do capítulo 3 descreve os níveis de segurança do padrão FIPS 140-2.

Além disso, a sincronização que ocorre entre a AD e a fonte de tempo pode ser fiscalizada. Esse assunto é abordado com mais detalhes por Demétrio (2003).

5.4 Auditoria para os Métodos de Datação Relativa

Um método de datação relativa não armazena o momento exato em que um documento foi protocolado, mas sim, a ordem temporal entre os documentos. Dentre os métodos de datação relativa existentes na literatura, os procedimentos de auditoria

propostos consideram os métodos: Encadeamento Linear e Árvore Sincronizada.

5.4.1 Auditoria para o Método do Encadeamento Linear

Propõe-se os seguintes procedimentos de auditoria para o Método do Encadeamento Linear:

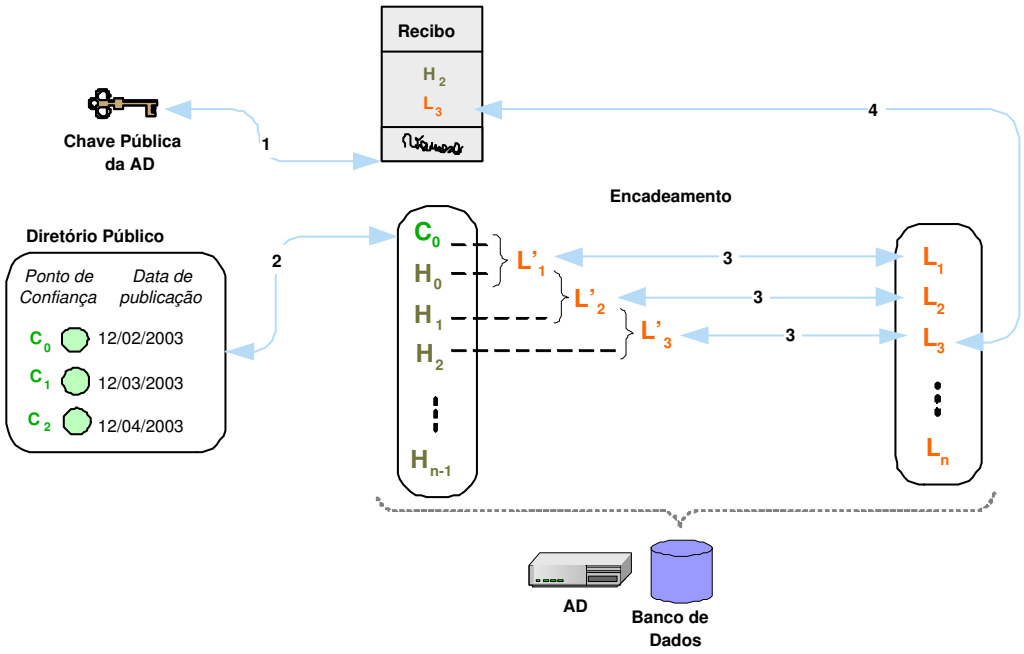


Figura 5.1: Auditoria - Verificação da validade de um recibo no Método do Encadeamento Linear: 1. Verificação da assinatura digital da AD sobre o recibo. 2. Comparação entre o Ponto de Confiança contido no encadeamento com o publicado no Diretório Público. 3. Verificação do encadeamento através do re-cálculo dos *links* desde L_1 até L_3. 4. Comparação do *link* L_3 do encadeamento com o L_3 contido no recibo.

Verificação da validade de um recibo: Seja L_k o *link* correspondente ao k-ésimo documento protocolado e n o número de *links* que constituem o encadeamento. A auditoria consiste das seguintes verificações:

- Verificar a assinatura digital da AD sobre o recibo[1];

[1]Verificar a assinatura digital da AD sobre o recibo envolve verificar se o certificado digital da AD é válido (se não expirou, não foi revogado e respeita as políticas da Cadeia de Certificação) e verificar a Cadeia de Certificação do certificado, desde de a Autoridade Certificadora que o emitiu até a AC-Raiz, a qual deve ser confiável.

- Averiguar se o Ponto de Confiança contido no encadeamento confere com o publicado pela AD em um Diretório Público;
- Re-calcular os *links* que constituem o encadeamento. Para isso, deve-se percorrer os *links* L_i, variando-se i de 1 a k, utilizando a Equação 3.1 da página 28. Ao final do cálculo, L_k deve ser obtido;
- Comparar o *link* L_k contido no encadeamento com o *link* L_k contido no recibo.

A Figura 5.1 ilustra um exemplo de auditoria em que a validade de um recibo é verificada.

Verificação da precedência entre dois documentos protocolados pela mesma AD: Consiste em verificar entre dois documentos, qual foi protocolado primeiro. Seja L_p e L_q os *links* correspondentes aos dois documentos. Os resumos dos documentos podem estar no mesmo intervalo do encadeamento ou em intervalos diferentes. Dependendo da situação, diferentes procedimentos devem ser adotados:

- **Os dois resumos estão em intervalos diferentes:** isto ocorre quando o primeiro resumo faz parte de um encadeamento, que depois de algum tempo foi exportado para um meio de armazenamento externo. Após isso, um novo Ponto de Confiança foi gerado. O segundo resumo foi protocolado após a publicação do Ponto de Confiança. Neste caso, os seguintes passos devem ser executados:
  - Verificar a assinatura digital da AD sobre os dois recibos;
  - Verificar a quais encadeamentos cada um dos *links* pertence;
  - Verificar se o Ponto de Confiança contido nos encadeamentos conferem com os publicados no Diretório Público;
  - Verificar o encadeamento percorrendo os *links* L_i, variando-se i de 1 a p, e depois de 1 a q, utilizando a Equação 3.1 da página 28. Ao final do cálculo, L_p e L_q devem ser obtidos;
  - Verificar a data da publicação dos Pontos de Confiança para identificar qual documento foi protocolado primeiro.

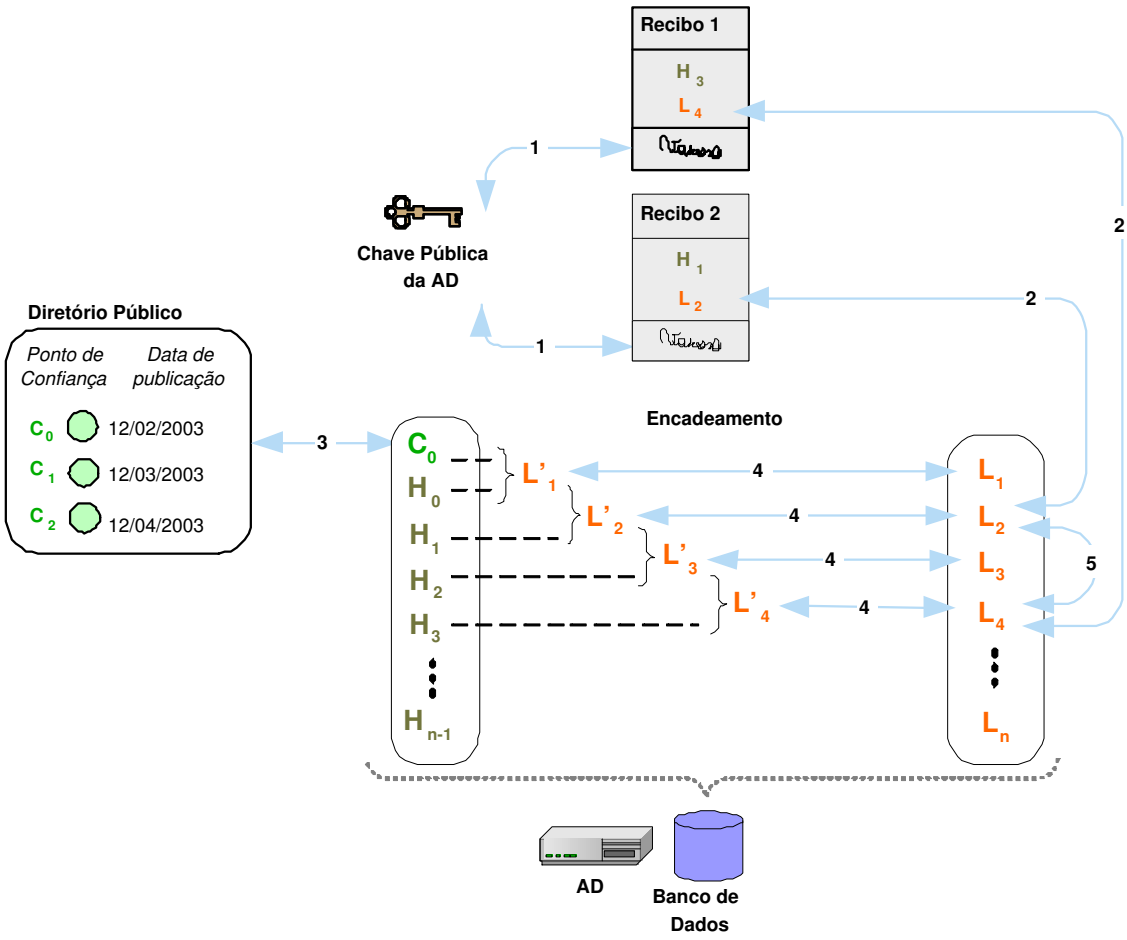


Figura 5.2: Auditoria - Verificação da precedência entre dois documentos no Método do Encadeamento Linear: 1. Verificação da assinatura digital da AD sobre os recibos. 2. Identificação do encadeamento ao qual os *links* pertencem. 3. Comparação entre o Ponto de Confiança contido no encadeamento com o publicado no Diretório Público. 4. Verificação do encadeamento através do re-cálculo dos *links* desde L_1 até L_2, e depois desde L_1 até L_4. 5. Constatação de que L_2 ocorre antes de L_4. Logo, o documento correspondente ao "Recibo 2"foi protocolado antes do documento referente ao "Recibo 1".

- **Os dois resumos estão no mesmo intervalo do encadeamento:** neste caso, os seguintes passos devem ser executados:
  - Verificar a assinatura digital da AD sobre os dois recibos;
  - Identificar a qual encadeamento os *links* pertencem;
  - Averiguar se o Ponto de Confiança contido no encadeamento confere com o publicado pela AD em um Diretório Público;
  - Re-calcular os *links* que constituem o encadeamento percorrendo L_i, variando-se i de 1 a p, e depois de 1 a q, utilizando a Equação 3.1 da página 28. Ao final do cálculo, L_p e L_q devem ser obtidos.
  - Identificar qual dos dois *links* L_p ou L_q ocorreu primeiro no encadeamento.

A Figura 5.2 ilustra um exemplo de auditoria em que é verificada a precedência entre dois documentos que se encontram no mesmo intervalo de encadeamento.

Verificação da integridade do encadeamento armazenado no banco de dados da AD: os seguintes procedimentos devem ser executados:

- Verificar a validade do certificado digital da AD, bem como a Cadeia de Certificação desde a Autoridade Certificadora que o emitiu até a AC-Raiz, a qual deve ser confiável;
- Caso o encadeamento já tenha sido exportado para um meio de armazenamento externo, é necessário verificar a assinatura digital do encadeamento para garantir a integridade do mesmo;
- Averiguar se o Ponto de Confiança contido no encadeamento confere com o publicado pela AD em um Diretório Público;
- Re-calcular os *links* contidos no banco de dados da AD, desde L_1 até L_n, verificando-se se os *links* calculados são equivalentes aos contidos no banco de dados da AD.

A Figura 5.3 ilustra um exemplo de verificação da integridade do encadeamento.

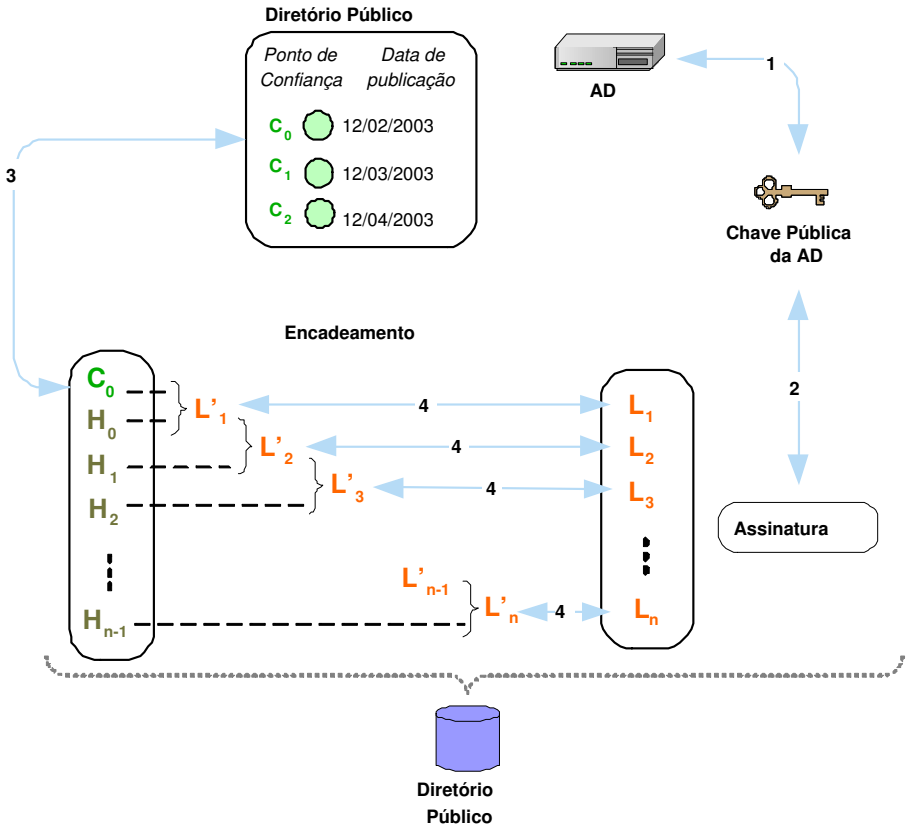


Figura 5.3: Auditoria - Verificação da integridade do encadeamento no Método do Encadeamento Linear: 1. Verificação da validade do certificado digital da AD. 2. Verificação da assinatura digital do encadamento. 3. Comparação do Ponto de Confiança contido no encadeamento com o que se encontra no Diretório Público. 4. Verificação do encadeamento através do re-cálculo dos *links* desde L_1 até L_n.

5.4.2 Auditoria para o Método da Árvore Sincronizada

Propõe-se os seguintes procedimentos de auditoria para o Método da Árvore Sincronizada:

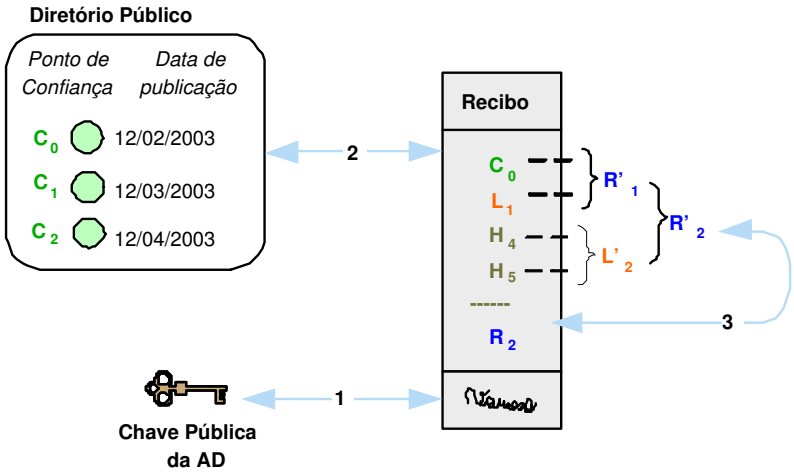


Figura 5.4: Auditoria - Verificação da validade de um recibo no Método da Árvore Sincronizada: 1. Verificação da assinatura digital da AD sobre o recibo. 2. Comparação entre o Ponto de Confiança contido no recibo com o publicado no Diretório Público. 3. Verificação do encadeamento através do re-cálculo dos *links* desde C_0 até R_2. O último *link* obtido, R'_2, é comparado com o *link* R_2 do encadeamento.

Verificação da validade de um recibo: Seja C_i o Ponto de Confiança contido no recibo, L_i e R_i os *links* correspondentes às rodadas e R_k o *link* que representa a rodada em que o documento foi protocolado.

- Verificar a assinatura da AD sobre o recibo;
- Averiguar se o Ponto de Confiança C_i contido no recibo confere com o publicado pela AD em um Diretório Público;
- Re-calcular os *links* que constituem o encadeamento contido no recibo. Para isso, deve-se percorrer os *links* L_i e R_i, desde de o Ponto de Confiança até o recibo em questão. Ao final do cálculo, o *link* R_k deve ser obtido.

A Figura 5.4 ilustra um exemplo de verificação de recibo.

Verificação da precedência entre dois documentos protocolados pela mesma AD: Consiste em verificar entre dois documentos, qual foi protocolado primeiro. Seja R_p e R_q os *links* que representam as rodadas em que os documentos foram protocolados.

- **Os dois resumos estão em intervalos diferentes:** isto ocorre quando o primeiro resumo faz parte de um encadeamento, que depois de algum tempo foi exportado para um meio de armazenamento externo. Após isso, um novo Ponto de Confiança foi gerado. O segundo resumo foi protocolado após a publicação do Ponto de Confiança. Neste caso, os seguintes passos devem ser executados:
  - Verificar a assinatura digital da AD sobre os dois recibos;
  - Averiguar se os Pontos de Confiança contidos nos dois recibos conferem com os publicados pela AD em um Diretório Público;
  - Verificar o encadeamento contido nos recibos, percorrendo os *links* R_i, variando-se i de 1 a p, e depois de 1 a q. Ao final do cálculo, R_p e R_q devem ser obtidos;
  - Verificar a data da publicação dos Pontos de Confiança para identificar qual documento foi protocolado primeiro.
- **Os resumos estão no mesmo intervalo do encadeamento:** quando os resumos estão no mesmo intervalo, eles podem pertencer a mesma rodada ou a rodadas diferentes. Dependendo da situação, diferentes procedimentos devem ser executados:
  - **Os resumos pertencem a mesma rodada:** neste caso $R_p = R_q$ e como os resumos foram protocolados na mesma rodada, a AD considera que eles foram protocolados no mesmo momento. Logo não é possível afirmar qual documento foi protocolado primeiro. É possível apenas verificar a validade do recibos através das verificações a seguir:
    * Verificar a assinatura digital da AD sobre os dois recibos;

* Averiguar se o Ponto de Confiança contido nos dois recibos confere com o publicado pela AD em um Diretório Público;
* Verificar o encadeamento contido nos recibos, percorrendo os *links* R_i, variando-se i de 1 a p, e depois de 1 a q. Ao final do cálculo, R_p e R_q devem ser obtidos.

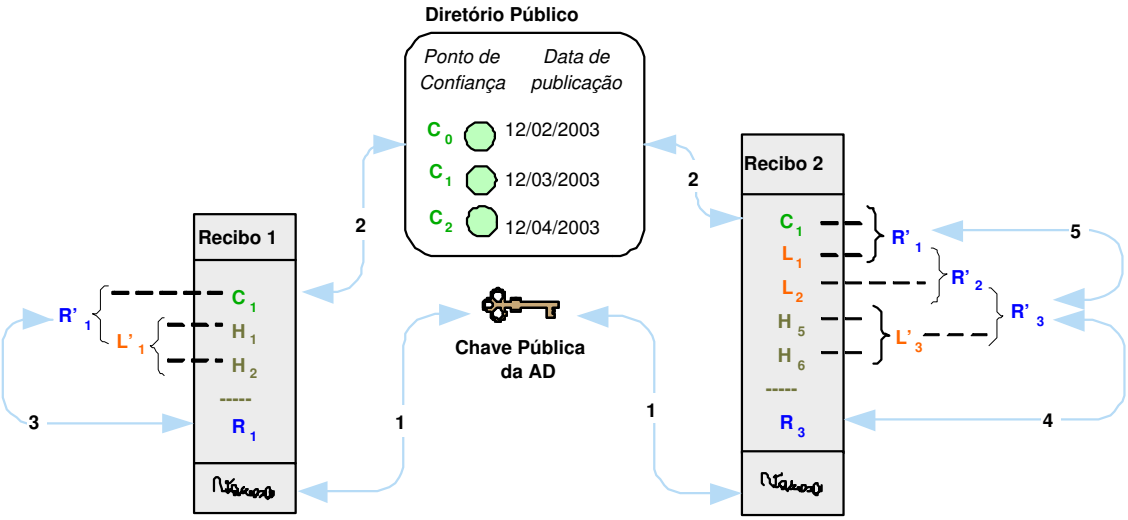


Figura 5.5: Auditoria - Verificação da precedência entre dois documentos no Método da Árvore Sincronizada: 1. Verificação da assinatura digital da AD sobre os recibos. 2. Comparação entre os Pontos de Confiança contidos nos recibos com o publicado pela AD no Diretório Público. 3. Verificação do encadeamento contido no primeiro recibo através do re-cálculo dos *links* desde C_1 até o *link* R_1. O último *link* obtido, R'_1, é comparado com o *link* R_1 contido no recibo. 4. Verificação do encadeamento contido no segundo recibo através do re-cálculo dos *links* desde C_1 até o *link* R_3. O último *link* obtido, R'_3, é comparado com o *link* R_3 contido no recibo. 5. Constatação de que o *link* R_1 ocorre antes do *link* R_3. Logo, os documentos referentes ao "Recibo 1"foram protocolados antes dos documentos referentes ao "Recibo 2".

– **Os resumos estão em rodadas diferentes:**

* Verificar a assinatura digital da AD sobre os dois recibos;
* Averiguar se o Ponto de Confiança contido nos dois recibos confere com o publicado pela AD em um Diretório Público;
* Verificar o encadeamento contido nos recibos, percorrendo os *links* R_i, variando-se i de 1 a p, e depois de 1 a q. Ao final do cálculo, R_p e R_q devem ser obtidos;

  - Identificar qual dos dois *links* R_p ou R_q ocorreu primeiro no encadeamento.

  A Figura 5.5 ilustra um exemplo de verificação da precedência entre dois documentos em que os resumos estão no mesmo intervalo do encadeamento e em rodadas diferentes.

- **Um dos recibos está sob um salto ou ambos estão sob saltos diferentes:** neste caso, para identificar qual dos dois *links* R_p ou R_q ocorreu primeiro é necessário realizar uma consulta ao Diretório Público e solicitar a cadeia de protocolação entre os dois documentos. Isto porque quando há o salto, as informações referentes às rodadas sob o salto são substituídas pelo *link* que o gerou. Assim, o encadeamento contido no recibo não incluirá o *link* R_p ou R_q. Nesse caso, as seguintes verificações devem ser realizadas:

  - Verificar a assinatura digital da AD sobre os dois recibos;
  - Averiguar se o Ponto de Confiança contido nos dois recibos confere com o publicado pela AD em um Diretório Público;
  - Verificar o encadeamento contido no Diretório Público, percorrendo os *links* R_i, variando-se i de 1 a p, e depois de 1 a q. Ao final do cálculo, R_p e R_q devem ser obtidos;
  - Identificar qual dos dois *links* R_p ou R_q ocorreu primeiro no encadeamento.

  A Figura 5.6 ilustra um exemplo de verificação de precedência entre dois documentos em que os resumos estão no mesmo intervalo do encadeamento, em rodadas diferentes e um dos recibos está sob um salto. Os dois recibos referem-se, respectivamente, as rodadas 2 e 5 da figura 3.8 da página 32.

Verificação da integridade do encadeamento armazenado no banco de dados da AD: os seguintes passos devem ser executados:

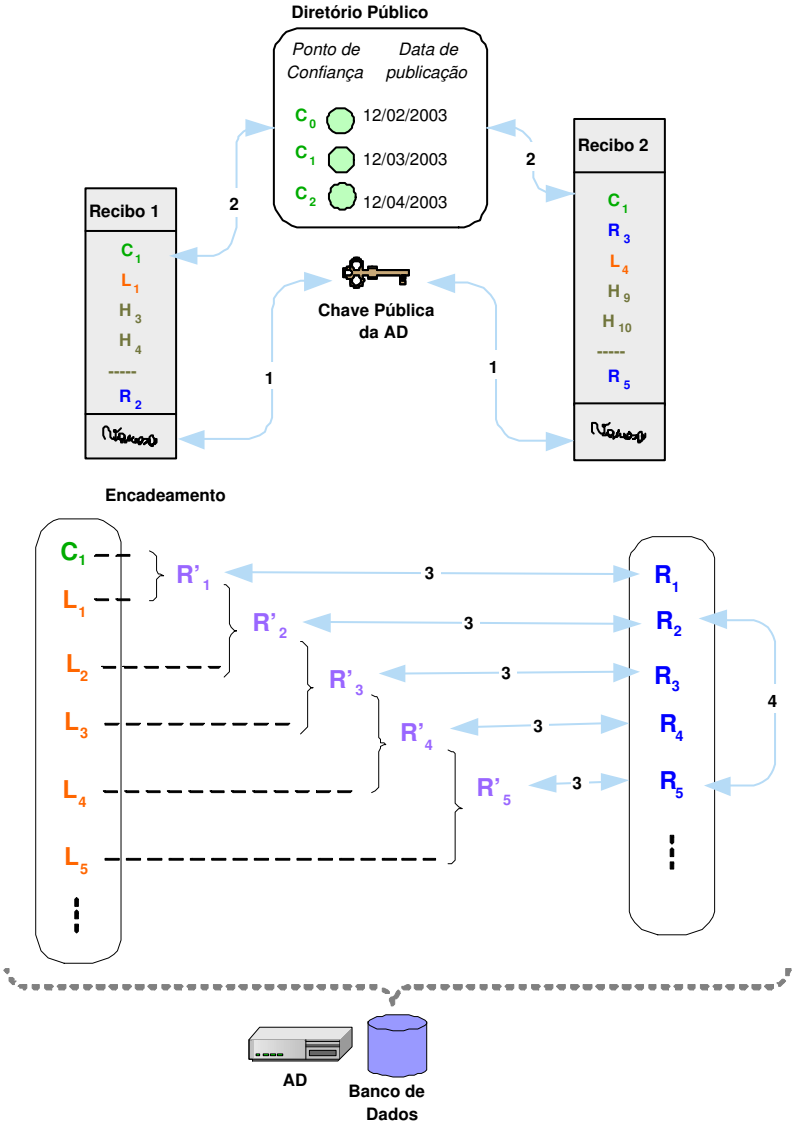


Figura 5.6: Auditoria - Verificação da precedência entre dois documentos no Método da Árvore Sincronizada com Saltos: 1. Verificação da assinatura digital da AD sobre os recibos. 2. Comparação entre os Pontos de Confiança contidos nos recibos com o publicado pela AD no Diretório Público. 3. Verificação do encadeamento contido no banco de dados da AD através do re-cálculo dos *links* R_i desde R_1 até R_5. 4. Constatação de que o *link* R_2 ocorre antes do *link* R_5. Logo, os documentos referentes ao "Recibo 1"foram protocolados antes dos documentos referentes ao "Recibo 2".

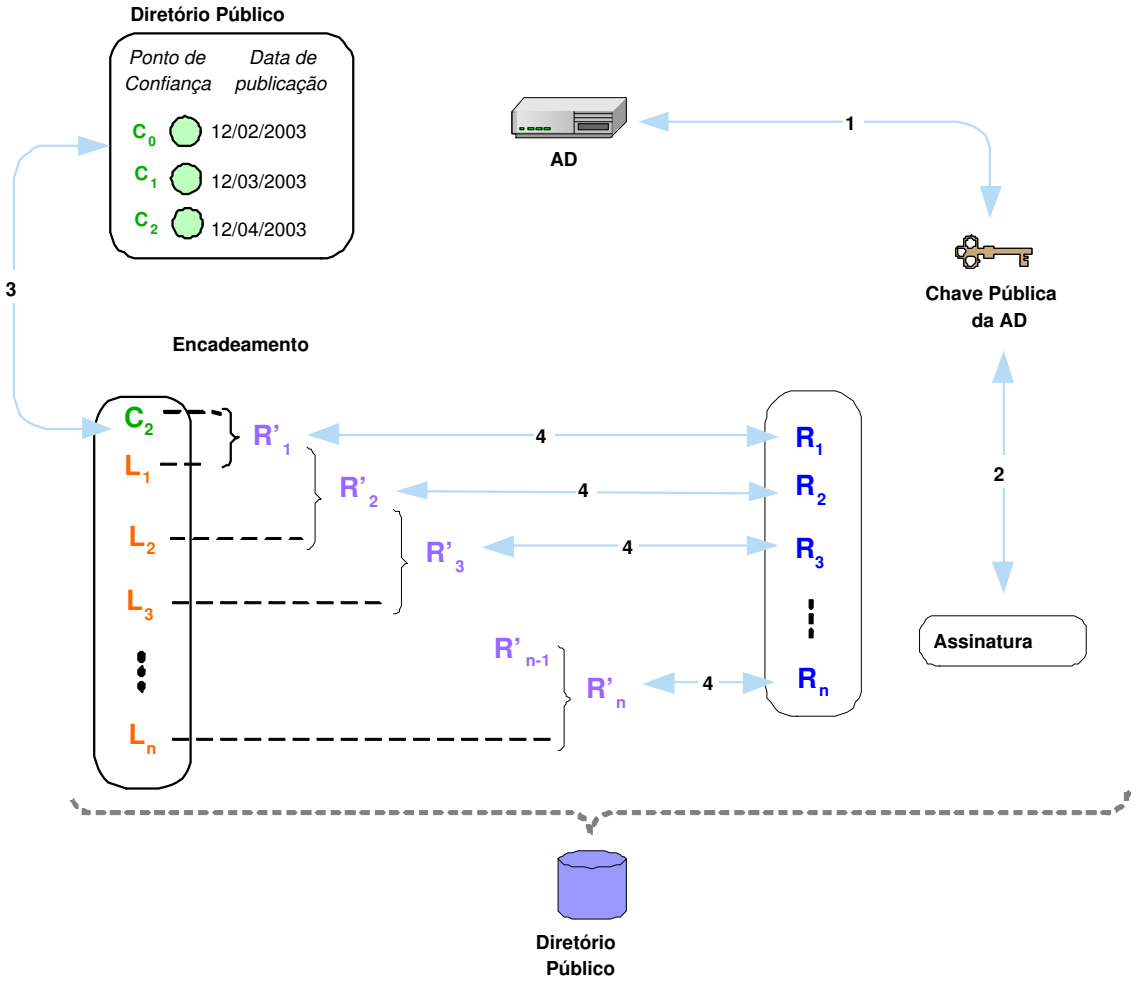


Figura 5.7: Auditoria - Verificação da integridade do encadeamento no Método da Árvore Sincronizada: 1. Verificação da validade do certificado digital da AD. 2. Verificação da assinatura digital do encadeamento. 3. Comparação do Ponto de Confiança contido no encadeamento com o que se encontra no Diretório Público. 4. Re-cálculo dos *links* R_i desde C_3 até o *link* R_n. Os *links* calculados, R'_i, são comparados com os contidos no encadeamento, R_i.

- Verificar a validade do certificado digital da AD, bem como a Cadeia de Certificação desde a Autoridade Certificadora que emitiu o certificado até a AC-Raiz, a qual deve ser confiável;
- Caso o encadeamento já tenha sido exportado para um meio de armazenamento externo, é necessário verificar a assinatura digital do encadeamento para garantir a integridade do mesmo;
- Averiguar se o Ponto de Confiança contido nos dois recibos confere com o publicado pela AD em um Diretório Público;
- Re-calcular os *links* contidos no banco de dados desde o Ponto de Confiança C_i até o *link* R_n e verificar se os mesmos são equivalentes aos contidos no banco de dados.

A Figura 5.7 ilustra um exemplo de verificação da integridade do encadeamento.

5.5 Conclusão

Este capítulo apresentou os meios pelos quais um sistema de protocolação digital pode ser auditado. No método de datação absoluta, a AD só pode ser auditada através da inspeção no equipamento. Porém, se a AD utilizar um método de datação relativa, a AD pode ser auditada através da verificação do encadeamento. Este capítulo apresentou os procedimentos de auditoria propostos para o Método do Encadeamento Linear e para o Método da Árvore Sincronizada. Estes procedimentos visam aumentar a confiança do sistema de protocolação digital, visto que através de sua aplicação, o funcionamento da AD pode ser inspecionado.

Capítulo 6

Política de Protocolação

6.1 Introdução

A Política de Protocolação (PP) é um documento que estabelece as regras empregadas no processo de protocolação digital de documentos eletrônicos. Este documento tem como objetivo descrever, de maneira sucinta, o papel dos componentes do sistema de protocolação, bem como suas responsabilidades, obrigações e direitos desde a implantação da AD até o encerramento de suas atividades. Além disso, este documento proporciona um melhor entendimento do funcionamento do processo de protocolação digital por parte dos usuários, além de servir de exemplo para outras ADs que desejem elaborar sua própria Política de Protocolação. Esta PP foi elaborada após um estudo de um *Draft* de uma Recomendação Internacional (PINKAS; POPE; ROSS, 2003), o qual apresenta os requisitos mínimos para elaborar uma Política de Protocolação. Esta PP é aplicável a todos os requerentes, assinantes e terceiras partes confiáveis, os quais podem ser pessoas físicas ou jurídicas, entidades ou organizações que mantenham algum vínculo com a AD.

A seção 6.2 apresenta as disposições gerais deste documento. Na seção 6.3 é apresentada a terminologia utilizada nesta PP. As obrigações e as responsabilidades de cada componente do sistema estão descritas na seção 6.4. A seção 6.5 descreve as práticas que a AD deve adotar no provimento do serviço de protocolação digital. A seção

6.6 apresenta as considerações finais deste capítulo.

6.2 Disposições gerais

6.2.1 Direitos

A reprodução e distribuição desta Política de Protocolação é permitida de forma não exclusiva e sem pagamento desde que:

I seja feita referência aos direitos autorais;

II a reprodução seja íntegra e atribuída ao autor.

Para outras permissões de reprodução, um pedido deverá ser enviado ao endereço eletrônico ou físico da AD.

6.2.2 Publicações

Esta Política de Protocolação está disponível:

- Em formato eletrônico:
  - No endereço da AD na WEB;
  - Através do correio eletrônico pelo endereço da AD.
- Em papel, pelo endereço da AD.

6.2.3 Conflito de cláusulas

Em caso de conflito entre alguma cláusula da PP em relação a uma versão anterior, o usuário estará sujeito às cláusulas da versão mais atual, exceto quando as cláusulas desta forem proibidas por lei. Em hipótese alguma será aceita cláusula de versão anterior à PP vigente.

6.2.4 Direito a emendas

A AD reserva-se ao direito de realizar emendas na versão vigente da PP, se julgar necessário, e as publicará em um repositório. As emendas poderão ou não ocasionar a mudança de versão da PP. Tal mudança só ocorrerá quando houver uma reestruturação da PP. As emendas de menor impacto entram em vigor imediatamente após a sua publicação e as de maior impacto entram em vigor após 10 (dez) dias de sua publicação.

6.2.5 Leis aplicáveis

Em todo processo será de uso único as leis brasileiras, as quais regulamentam a interpretação desta PP, a fim de garantir a uniformidade da interpretação da mesma para todos os usuários.

6.2.6 Resolução de controvérsias

As controvérsias envolvendo a PP devem ser notificadas à AD visando a sua resolução imediata.

6.3 Terminologia

Para os propósitos deste documento, os seguintes termos se aplicam:

6.3.1 Abreviações

AD	Autoridade de Datação
DPP	Declaração de Práticas de Protocolação
PP	Política de Protocolação
UTC	*Coordinated Universal Time*

6.3.2 Definições

Parte confiável: Receptor de um recibo de protocolação que confia no recibo;

Assinante: Entidade que requisita o serviços de protocolação providos por uma AD e que concorda implícita ou explicitamente com seus termos e condições;

Recibo de protocolação: Objeto de dados que vincula a representação de uma informação com um momento específico do tempo, estabelecendo, dessa forma, uma evidência de que a informação existiu antes daquele momento específico;

Autoridade de Datação: Autoridade que emite os recibos de protocolação;

Declaração de Práticas e Divulgação: conjunto de declarações sobre as políticas e práticas de uma AD que merecem ser enfatizadas e divulgadas aos assinantes e partes confiáveis;

Declaração de Práticas de Protocolação: Declaração das práticas empregadas pela AD na emissão de recibos de protocolação;

Sistema de Protocolação: Composição de produtos de TI[1] e componentes organizados para dar suporte ao fornecimento de serviços de protocolação digital;

Política de Protocolação: Conjunto de regras que indicam a aplicabilidade de um recibo de protocolação para uma comunidade particular e/ou classe de aplicações com requisitos comuns de segurança;

***Coordinated Universal Time (UTC)*:** Escala de tempo administrada através de um tratado adotado pela comunidade mundial que designa *National Measurement Institutes* (NMIs) como fontes de tempo UTC. Nos Estados Unidos, o *National Institute of Standards and Technology* (NIST) e na Inglaterra, o *National Physical Laboratory* (NPL) são dois exemplos. Existem aproximadamente 50 centros similares de medidas que são responsáveis pelo tempo oficial no mundo;

[1]Tecnologia da Informação - termo abrangente para métodos de computação, processamento de informação e comunicação de dados

UTC(k): Escala de tempo realizada pelo laboratório "k"e mantida em acordo com UTC, com o objetivo de alcançar mais ou menos 100 ns.

6.3.3 Conceitos gerais

Serviços de protocolação: O serviço de protocolação é dividido em dois componentes:

- **Fornecimento de protocolação:** Serviço que gera os recibos;
- **Gerência da protocolação:** Serviço que monitora e controla a operação de um serviço de protocolação para garantir que o serviço está sendo provido como é especificado pela AD. Este serviço é responsável pela instalação e desinstalação do serviço de fornecimento de protocolação. Por exemplo, o serviço de gerência de protocolação garante que o relógio utilizado para protocolar está corretamente sincronizado com o UTC.

Autoridade de Datação: A autoridade na qual os usuários dos serviços de protocolação confiam (assinantes e partes confiáveis) para emitir os recibos. Mesmo que a AD utilize outros componentes para prover o serviço de protocolação, ela sempre garante o que está especificado na Política de Protocolação.

Assinante: O assinante pode ser uma organização compreendendo vários usuários finais ou pode ser um único usuário final. Quando o assinante é uma organização, algumas das obrigações que se aplicam à organização serão aplicadas aos usuários finais. A organização será responsabilizada, caso as obrigações de um usuário final não sejam cumpridas corretamente. Quando o assinante é um usuário final, ele é o responsável direto, se suas obrigações não forem cumpridas.

Política de Protocolação e Declaração de Práticas de Protocolação: Em geral, uma Política de Protocolação (PP) especifica "o que deve ser feito"num sistema de protocolação digital, enquanto uma Declaração de Práticas de Protocolação (DPP) especifica "como é feito". Uma PP é um documento menos específico do que uma DPP. Uma DPP é uma descrição mais detalhada dos termos e das condições, bem como

das práticas operacionais e administrativas de uma AD na emissão e na gerência do serviço de protocolação. A DPP de uma AD reforça as regras estabelecidas na PP. A DPP define como uma determinada AD atende aos requisitos técnicos e organizacionais identificados na PP. O objetivo de uma PP é significativamente diferente do de uma DPP. Uma PP é definida independentemente dos detalhes específicos de um ambiente operacional específico de uma AD, enquanto uma DPP é elaborada para uma estrutura organizacional, procedimentos operacionais, facilidades e ambiente computacional específicos de uma AD.

6.4 Obrigações e responsabilidades

6.4.1 Obrigações da AD

Geral: A AD deve garantir que todas as práticas de protocolação apresentadas neste documento, são implementadas de acordo com a Política de Protocolação. A AD deve garantir a conformidade com os procedimentos descritos nesta política, mesmo quando suas funcionalidade estão sob responsabilidade de sub-contratados.

Obrigações da AD com relação aos assinantes: A AD deve atender as declarações expressas nestes termos e condições, incluindo a disponibilidade e a precisão de seus serviços.

6.4.2 Obrigações do assinante

É recomendável que o usuário, ao obter o recibo de protocolação, verifique se o recibo foi assinado corretamente, se o certificado digital da AD não expirou ou foi revogado, além de verificar a validade da Cadeia de Certificação do certificado da AD até a AC Raiz, a qual deve ser confiável.

6.4.3 Obrigações da parte confiável

As partes confiáveis têm a obrigação de realizar as seguintes verificações antes de confiar em um recibo:

- Verificar se o recibo foi assinado corretamente e se a chave privada utilizada para assinar o recibo não foi comprometida até o momento da verificação;
- Considerar qualquer limitação no uso do recibo quando indicado na Política de Protocolação;
- Considerar qualquer precaução prescrita no contrato ou em qualquer outro lugar.

6.4.4 Responsabilidade da AD

A AD exclui qualquer responsabilidade, a menos que seja estipulada por lei aplicável. Além disso, a AD não é responsável por danos, atrasos ou falhas no desempenho de suas atividades resultantes de eventos de força maior, os quais estão além de seu controle, tais como: guerras, terremotos, fogo, enchentes e outros.

6.5 Práticas da AD

Durante o provimento do serviço de protocolação digital, a AD emprega as seguintes práticas.

6.5.1 Declaração de Práticas e Divulgação

Declaração de Práticas de Protocolação: A AD disponibiliza um documento no qual garante demonstrar a confiabilidade necessária para prover os serviços de protocolação. Em particular:

- Com o objetivo de determinar a necessidade de controles de segurança e de procedimentos operacionais, a AD realiza estimativa de riscos para avaliar seus recursos, bem como as ameaças a estes recursos;

- As declarações de práticas da AD identificam as obrigações de todas as organizações externas que dão suporte aos seus serviços, incluindo as políticas e as práticas aplicáveis;
- A AD disponibiliza aos assinantes e às partes confiáveis sua Declaração de Práticas, para que possa ser avaliada a conformidade com a Política de Protocolação;
- A AD divulga a todos os seus assinantes e potenciais partes confiáveis os termos e as condições referentes aos serviços de protocolação;
- A AD possui um grupo gerencial com autoridade para aprovar a Declaração de Práticas da AD;
- O gerente *senior* da AD garante que as práticas são implementadas adequadamente;
- A AD define um processo de revisão para as práticas, incluindo responsabilidades para manutenção da Declaração de Práticas da AD;
- Sempre que a AD pretende realizar uma alteração no documento de Declaração de Práticas de Protocolação, uma notificação é enviada, e depois que as alterações são aprovadas, o documento revisado é disponibilizado.

Declaração de Divulgação da AD: Trata-se de um documento que tem como objetivo divulgar para todos os assinantes e para potenciais partes confiáveis os termos e condições referentes à utilização de serviços de protocolação. Este documento inclui:

- A informação de contato da AD;
- A Política de Protocolação que está sendo aplicada;
- O algoritmo de *hash* que pode ser utilizado para representar uma informação que será protocolada;
- O tempo de vida esperado da assinatura utilizada para assinar o recibo de protocolação (depende do algoritmo de *hash*, do algoritmo de assinatura e do comprimento da chave);

- A precisão do tempo registrado no recibo de protocolação com relação ao UTC;
- Qualquer limitação na utilização do serviço de protocolação;
- As obrigações do assinante;
- As obrigações da parte confiável;
- Informações sobre como verificar o recibo de protocolação, de modo que a parte confiável possa considerar o recibo "razoalvelmente"confiável e qualquer limitação possível em relação ao período de validade;
- O período de tempo durante o qual os *logs* dos eventos serão armazenados;
- O sistema legal aplicável, incluindo qualquer declaração referente aos requisitos dos serviços de protocolação sob lei nacional;
- Limitações de responsabilidades;
- Procedimentos para reclamações e situações de disputa;
- Se a AD foi avaliada de acordo com a Política de Protocolação e se isto foi realizado por uma corporação independente;
- A disponibilidade de seu serviço, incluindo o tempo médio esperado entre falha do serviço de protocolação, o tempo médio de recuperação de uma falha e o fornecimento de recuperação de desastre, incluindo serviços de *backup*.

As informações que constituem a Declaração de Divulgação estão incluídas na DPP.

6.5.2 Gerenciamento de chaves

Geração do par de chaves da AD: A AD garante que todas as chaves são geradas sob circunstâncias controladas.

- A geração da chave de assinatura da AD é realizada em um ambiente físico seguro por pessoal que exerça uma função de confiança;

- A geração da chave de assinatura da AD é realizada dentro de um módulo criptográfico que atende os requisitos identificados na FIPS 140-2 nível 3 ou superior;
- O algoritmo de geração da chave da AD, o comprimento da chave privada e o algoritmo de assinatura utilizado para assinar os recibos são reconhecidos por um grupo supervisor nacional, ou em acordo com estado da arte atual.

Proteção da chave privada da AD: A AD garante que sua chave privada permanece confidencial e íntegra.

- A chave privada da AD é mantida e utilizada dentro de módulos criptográficos que atendam os requisitos identificados na FIPS 140-2 nível 3 ou superior;
- A AD não faz *backup* de sua chave privada para minimizar o risco de comprometimento.

Distribuição da chave pública da AD: A AD garante a integridade e a autenticidade de sua chave pública, bem como que os parâmetros associados serão preservados durante a distribuição às partes confiáveis.

- A chave pública da AD é disponibilizada a todas as partes confiáveis através do seu certificado digital;
- O certificado digital da AD é emitido por uma Autoridade Certificadora que opera sob uma Política de Certificação que provê um nível de segurança equivalente ou superior ao da Política de Protocolação.

Troca do par de chaves da AD: O tempo de vida do certificado da AD é menor do que o período de tempo considerado seguro, no que diz respeito ao algoritmo e ao comprimento da chave utilizados. Além disso, os registros referentes aos serviços de protocolação são armazenados por um período de no mínimo 1 (um) ano após a expiração da validade da chave da AD.

Fim do ciclo de vida do par de chaves da AD: A AD garante que sua chave privada não será utilizada após o fim de seu ciclo de vida.

- Procedimentos técnicos e operacionais são utilizados para garantir que uma nova chave será utilizada quando a chave da AD expirar;
- A chave privada da AD é destruída de modo que não possa mais ser recuperada;
- O sistema de geração de recibos rejeita qualquer tentativa de emissão de recibos se a chave privada da AD tiver expirado.

Gerência do ciclo de vida dos módulos criptográficos utilizados para assinar os recibos: A AD garante a segurança do módulo criptográfico por todo o seu ciclo de vida. A AD garante que:

- O módulo criptográfico utilizado para assinar os recibos não é violado durante o carga de informações no módulo;
- O módulo criptográfico utilizado para assinar os recibos não é violado enquanto fica armazenado;
- A instalação e a ativação da chave privada da AD no módulo criptográfico será realizada apenas por pessoal que possua funções de confiança e em um ambiente fisicamente seguro;
- O módulo criptográfico utilizado para assinar os recibos está funcionando corretamente;
- A chave privada armazenada no módulo criptográfico será destruída assim que o dispositivo for desativado.

6.5.3 Protocolação

Encadeamento: A AD garante a que os documentos protocolados são encadeados corretamente.

- A AD utiliza um método de datação híbrida;
- A AD fornece procedimentos de auditoria para fiscalizar o funcionamento da AD;
- A AD publica pontos de confiança periodicamente, com o objetivo de criar âncoras temporais.

Recibo de protocolação: A AD garante que os recibos são emitidos de maneira segura e incluem a data e a hora correntes.

- O recibo inclui:
  - Um identificador para o país em que a AD está estabelecida;
  - Um identificador da AD;
  - Um identificador da Política de Protocolação;
  - Um identificador único do recibo;
  - Uma representação da informação a ser protocolada.
- O valor do tempo utilizado pela AD ao protocolar os recibos é rastreável até um valor de tempo real distribuído por um laboratório UTC(k)[2];
- A informação de data e hora incluída no recibo é sincronizada com o UTC com uma precisão de 125 ms;
- Se for detectado que o relógio do servidor de protocolação está fora da precisão estabelecida, então os recibos não são emitidos;
- O recibo é assinado com uma chave gerada exclusivamente para este propósito, a chave privada da AD.

Sincronização do relógio com o UTC: A AD garante que o seu relógio está sincronizado com o UTC dentro da precisão declarada.

[2]O BIPM (*Bureau International des Poids et Mesures*) computa o tempo UTC baseado na representação do tempo UTC(k) local de um grande grupo de relógios atômicos em institutos de medição nacional e observatórios astronômicos nacionais por todo o mundo. O BIPM dissemina o UTC através de um circular mensalmente. Esta informação fica disponível no *website* (http://www.bipm.org) e identifica oficialmente todos os institutos que possuem escalas de tempo UTC(k) reconhecidas.

- A calibragem do relógio da AD é mantida, de modo que o relógio não fique fora da precisão declarada;
- O relógio da AD é protegido contra ameaças que possam resultar em mudanças não detectáveis no relógio;
- A AD garante que, se o tempo que é indicado no recibo flutuar ou saltar para fora da precisão estabelecida, isto será detectado;
- A AD garante que a sincronização do relógio é mantida quando um *leap second* ocorre. A mudança leva em consideração que o *leap second* ocorre durante o último minuto do dia em que é programado para ocorrer. Um registro mantém o momento exato (dentro da precisão declarada) em que esta mudança ocorreu[3].

6.5.4 Gerência e operação da AD

Gerência da Segurança: A AD garante que os procedimentos administrativos e gerenciais são aplicados adequadamente e correspondem com as melhores práticas reconhecidas.

- A AD retém responsabilidade por todos os aspectos de fornecimento do serviço de protocolação dentro do escopo da Política de Protocolação, mesmo que algumas funções sejam realizadas por terceiros sub-contratados;
- O gerenciamento da AD trata da questão da segurança da informação através de uma comissão responsável por definir a política de segurança das informações da AD. A AD garante a publicação e a comunicação desta política a todos os funcionários que são afetados por ela;
- A infra-estrutura de segurança de informação necessária para gerenciar a segurança dentro da AD sofre manutenção todo o tempo. Qualquer alteração que tenha impacto no nível de segurança provido deve ser aprovada pela comissão;

[3] *Leap second* é um ajuste no UTC pela subtração ou adição de um segundo extra no último segundo do mês. Preferencialmente isto é realizado no final de dezembro e junho, e em alguns casos, os meses de março e setembro são escolhidos.

- Os controles de segurança e os procedimentos operacionais para os sistemas e recursos de informação que fornecem o serviço de protocolação são documentados, implementados e passam por manutenção;
- A AD garante que a segurança da informação passa por manutenção quando a responsabilidade das funções da AD são realocadas para outra organização.

Gerência e classificação de recurso: A AD garante que suas informações e seus recursos recebem um nível adequado de proteção. A AD mantém um inventário de todos os recursos e atribui uma classificação para os requisitos de proteção consistente com uma análise de risco.

Segurança do pessoal: A AD utiliza práticas de contratação que visam manter a confiabilidade de suas operações.

- A AD emprega pessoal que possua conhecimento no assunto, experiência e qualificações necessárias para o serviço oferecido e apropriadas para a função do trabalho;
- A AD elabora um documento que lista cada função de segurança juntamente com a descrição do trabalho e as respectivas responsabilidades. Além disso, as funções de confiança das quais a segurança da AD depende são claramente identificadas neste documento;
- Existe uma diferenciação entre as funções gerais e as funções específicas da AD, pois cada qual requer diferentes habilidades e requisitos de experiência;
- O pessoal exerce procedimentos administrativos e gerenciais de acordo com os procedimentos de gerência da segurança de informação da AD;
- Para os cargos administrativos e gerenciais, o pessoal a ser contratado deve possuir:
  - Conhecimento da tecnologia de protocolação;
  - Conhecimento da tecnologia de assinatura digital;

  - Conhecimento dos mecanismos para calibragem e sincronização do relógio da AD com o UTC;
  - Familiaridade com procedimentos de segurança para pessoal;
  - Experiência com segurança da informação e análise de riscos.

- Todo o pessoal que exerce função de confiança não deve ter nenhum tipo de conflito de interesses que possa prejudicar a imparcialidade das operações da AD;
- Funções de confiança incluem papéis que envolvem as seguintes responsabilidades:
  - Oficiais de segurança: Abrange a responsabilidade por administrar a implementação das práticas de segurança;
  - Administradores do sistema: Autorizados a instalar, configurar e prestar manutenção nos sistemas da AD para gerência da protocolação;
  - Operadores de sistema: Responsáveis por operar sistemas da AD no dia-a-dia. Autorizados a executar *backup* e recuperação do sistema;
  - Auditores do sistema: Autorizados a visualizar os arquivos e os registros de auditoria dos sistemas da AD.
- O pessoal a ser contratado para exercer função de confiança é selecionado pelo gerente *senior* responsável pela segurança;
- A AD não seleciona para exercer função de confiança ou gerencial pessoal condenado por crime sério ou outra ofensa que afete sua compatibilidade com a função.

Segurança física e ambiental: A AD garante que o acesso físico a serviços críticos é controlado e que os riscos físicos a estes serviços são minimizados.

- Tanto para o serviço de fornecimento de protocolação quanto para o de gerência de protocolação:

  - Apenas as pessoas autorizadas têm acesso físico aos recursos relativos ao serviço de protocolação;
  - A AD dispõe de controles que são implementados para evitar perda, dano ou comprometimento dos recursos e interrupção das atividades do serviço de protocolação;
  - A AD também dispõe de controles que são implementados para evitar o comprometimento ou o roubo de informação ou equipamento de processamento de informação.

- A AD controla o acesso aos módulos criptográficos para atender os requisitos de segurança identificados na geração do par de chaves da AD e na proteção da chave privada da AD;
- Os equipamentos referentes à gerência de protocolação são operados em um ambiente que protege fisicamente os serviços de algum comprometimento decorrente de um acesso não autorizado ao sistema ou aos dados.
- A AD é protegida fisicamente através da criação de perímetros bem definidos de segurança em torno da gerência de protocolação. Qualquer parte do local que é compartilhado com outras organizações está fora deste perímetro;
- A AD dispõe de controles de segurança física e ambiental implementados para proteger os equipamentos onde estão os recursos do sistema e os recursos utilizados para dar suporte a sua operação. A política de segurança física e ambiental da AD para sistemas relativos à gerência de protocolação definem um nível mínimo de controle de acesso físico, proteção contra desastre natural, fatores de segurança contra incêndio, colapso da estrutura, vazamentos, proteção contra roubo, invasão e recuperação de desastre.
- A AD também dispõe de controles implementados para evitar que informações referentes aos equipamento, mídia ou *software* relacionados aos serviços de protocolação sejam levados para fora do local sem autorização.

Gerência das operações: A AD garante que os componentes são seguros e operam

corretamente, com um risco mínimo de falha.

- A integridade das informações e dos componentes do sistema da AD é protegida contra vírus e *softwares* maliciosos e não autorizados.
- O relato de incidente e procedimentos de resposta são empregados de forma que o dano dos incidentes de segurança e funcionamento defeituoso sejam minimizados.
- A mídia utilizada dentro dos sistemas da AD é manipulada com segurança para protegê-la de dano, roubo, acesso não autorizado ou obsoleto.
- Procedimentos são estabelecidos e implementados para todas as funções de confiança e administrativas que têm impacto sobre o serviço de de protocolação;
- Toda mídia é manipulada com segurança de acordo com os requisitos do esquema de classificação de informação;
- Para garantir que um poder adequado de processamento e armazenamento estará disponível, é realizada uma monitoração da demanda da capacidade e uma projeção dos requisitos de capacidade;
- A AD age de maneira coordenada para responder rapidamente aos incidentes e limitar o impacto de brechas de segurança. Para tanto, todos os incidentes são relatados o mais rápido possível;
- As operações de segurança são separadas das demais operações.

Gerência do acesso ao sistema: A AD garante que apenas pessoas autorizadas têm acesso ao sistema.

- Controles são implementados para proteger o domínio da rede interna da AD do acesso não autorizado;
- A AD administra o acesso de usuários (incluindo operadores, administradores e auditores) para manter a segurança do sistema, incluindo gerência da conta dos usuários, auditoria, modificação da hora ou remoção de acesso;

- A AD garante que o acesso a informação e funções do sistema de aplicação é restrito de acordo com a política de controle de acesso. Particularmente, o uso dos programas utilitários do sistema é restrito e fortemente controlado;
- O pessoal é apropriadamente identificado e autenticado antes do uso de aplicações críticas relacionas com a protocolação.
- As atividades do pessoal são registradas;
- A AD mantém os componentes da rede local em um ambiente físico seguro e suas configurações são periodicamente auditadas para atender os requisitos especificados pela AD;
- Monitoramento contínuo e aparelhos de alarme são utilizados para que a AD seja capaz de detectar, registrar e reagir rapidamente em situação de tentativa irregular e/ou não autorizada de acesso aos seus recursos.

Sistemas de desenvolvimento e manutenção: A AD utiliza sistemas e produtos que são protegidos contra modificação.

- É realizada uma análise dos requisitos de segurança nas fases de projeto e especificação e requisitos de qualquer projeto de sistema de desenvolvimento sob responsabilidade da AD;
- Procedimentos de controle de alterações são aplicados para *releases*, *softwares* de modificação e alterações emergenciais de qualquer *software* operacional.

Comprometimento dos serviços da AD: A AD garante que no caso de evento que afete a segurança de seus serviços, incluindo o comprometimento de sua chave privada ou detecção da perda de calibragem, informações relevantes serão disponibilizadas para os assinantes e para as terceira partes confiáveis. O plano de recuperação de desastre trata do comprometimento ou da suspeita de comprometimento da chave privada da AD ou da perda de calibragem do relógio, que podem afetar os recibos emitidos. Nestes casos:

- A AD disponibilizará a todos os assinantes e às partes confiáveis uma descrição do comprometimento que ocorreu;
- A AD não emitirá recibos de protocolação até que os passos de recuperação do comprometimento tenham sido executados;
- Sempre que possível, a AD disponibilizará a todos os assinantes e partes confiáveis informação que possa ser utilizada para identificar os recibos que podem ter sido afetados, a menos que isto afete a privacidade dos usuários da AD ou da segurança dos serviços da AD.

Término da AD: A AD garante que eventuais interrupções decorrentes da pausa dos serviços de protocolação serão minimizadas e, em particular, garante manutenção contínua da informação necessária para verificar a validade dos recibos.

- Antes de a AD finalizar seus serviços de protocolação, no mínimo, os seguintes procedimentos serão executados:
  - A AD disponibilizará a todos os assinantes e às partes confiáveis informações referentes ao seu término;
  - A AD finalizará a autorização de todos os sub-contratados;
  - A AD transferirá obrigações para uma parte confiável para manter os registros de eventos e os registros de auditoria necessários para demonstrar a correta operação da AD por um período razoável;
  - A AD manterá ou transferirá para uma parte confiável suas obrigações para disponibilizar sua chave pública e seu certificado às partes confiáveis por um período razoável;
  - A chave privada da AD será destruída, de maneira que não possa ser recuperada.
- A AD assegura estar preparada para cobrir os custos para atender estes requisitos mínimos em caso de falência;
- A AD executará os passos necessários para revogar seu certificado.

Conformidade com os requisitos legais: A AD garante conformidade com os requisitos legais. Em particular:

- Medidas técnicas e organizacionais são adotadas contra o processamento não autorizado e ilegal de dados pessoais e contra perda acidental, destruição ou dano a dados pessoais;
- A informação dos usuários que a AD tem armazenada é protegida de divulgação, a menos que o usuário esteja de acordo, por ordem judicial ou outro requisito legal.

Registro de informações referentes à operação do serviço de protocolação: A AD garante que toda informação relevante referente à operação dos serviços de protocolação é registrada por um período mínimo definido de tempo, em particular para o fornecimento de evidência para processos judiciais.

- Os eventos e dados a serem registrados em *logs* são documentados pela AD;
- A confidencialidade e a integridade dos registros correntes e arquivados referentes à operação dos serviços de protocolação são mantidos;
- Os registros referentes à operação dos serviços de protocolação são arquivados de maneira confidencial de acordo com práticas de divulgação;
- Registros referentes aos serviços de protocolação são mantidos por um período de tempo após da expiração da validade das chaves da AD;
- Dentre os eventos registrados pela AD estão:
  - Gerenciamento de chave;
  - Sincronização do relógio da AD com o UTC, incluindo detecção de perda de sincronização, re-calibragem e precisão do relógio;
  - Ciclo de vida do certificado da AD;
  - Ciclo de vida do par de chaves da AD.
- Os eventos são registrados de maneira que não é possível removê-los ou destruí-los facilmente dentro do período de tempo em que devem ser mantidos;

- Qualquer informação registrada sobre os assinantes são mantidas confidenciais, exceto quando o assinante concorda com a publicação dos seus dados.

6.5.5 Organizacional

A AD garante que sua organização é confiável.

- Políticas e procedimentos sob os quais a AD opera não são discriminativos;
- A AD disponibiliza seus serviços a todos os requerentes cujas atividades se enquadram na sua área declarada de operação e que concordam em obedecer as obrigações especificadas na Declaração de Divulgação da AD;
- A AD possui um sistema de qualidade e de gerência de segurança da informação apropriado para os serviços de protocolação por ela providos;
- A AD possui infra-estrutura adequada para cobrir as responsabilidades oriundas de suas operações;
- A AD possui estabilidade financeira e os recursos necessários para operar em conformidade com sua política;
- A AD emprega um número suficiente de pessoal, os quais possuem educação, treinamento, conhecimento técnico e experiência referente ao tipo, faixa e volume de trabalho necessários para prover os serviços de protocolação;
- A AD possui políticas e procedimentos para resolução de reclamações e disputas recebidas dos clientes ou de outras partes sobre a provisão dos serviços de protocolação ou de qualquer matéria relacionada;
- A AD possui acordos e relações de contratos apropriadamente documentados, onde a provisão dos serviços envolve sub-contratação, terceirização ou outra relação com uma terceira parte.

6.5.6 Taxas

A AD está livre para cobrar pelo serviço de protocolação e as taxas de cobrança pelo serviço serão definidas e estabelecidas pela AD e serão disponibilizadas.

6.6 Conclusão

Neste capítulo foram apresentadas as políticas que uma Autoridade de Datação deve utilizar com o objetivo de manter a confiabilidade do sistema. Através da elaboração e da divulgação de uma Política de Protocolação, os usuários têm condições de avaliar se a AD está provendo um serviço confiável, como é especificado no documento. Além disso, este documento provê um melhor entendimento do sistema de protocolação por parte dos usuários.

Capítulo 7

Análise da confiança em uma infra-estrutura distribuída de ADs

7.1 Introdução

Uma infra-estrutura distribuída de protocolação digital é composta por várias ADs que possuem seus encadeamentos sincronizados através de protocolações cruzadas. Este sincronismo é realizado através da protocolação do último *link* do encadeamento de uma AD em uma outra AD. Dessa forma é possível comparar documentos protocolados por ADs diferentes, visto que os encadeamentos estão unidos através de um ponto em comum chamado Ponto de Sincronismo.

Para realizar uma auditoria sobre uma AD que realizou uma protocolação cruzada, são necessárias algumas verificações adicionais. A seção 7.2 apresenta uma visão geral de um sistema de protocolação em que as ADs constituem uma infra-estrutura distribuída. Na seção 7.3 são descritos os procedimentos adicionais que devem ser executados durante uma auditoria. Finalmente, a seção 7.4 apresenta as conclusões deste capítulo.

7.2 Infra-estrutura distribuída de ADs

A Figura 7.1 ilustra uma infra-estrutura distribuída de ADs, a qual é composta por: Autoridades de Datação, usuários e o Diretório Público. As ADs que desejam realizar uma protocolação cruzada cadastram seus dados no Diretório Público. Entre os dados informados estão o seu endereço na *Internet*, localização, identificador, entre outros. Para sincronizar seu encadeamento, a AD consulta o Diretório Público para obter o endereço da AD desejada e gera uma requisição de protocolação para a mesma. Os usuários também consultam o Diretório Público para selecionar a AD para qual irão enviar sua requisição de protocolação.

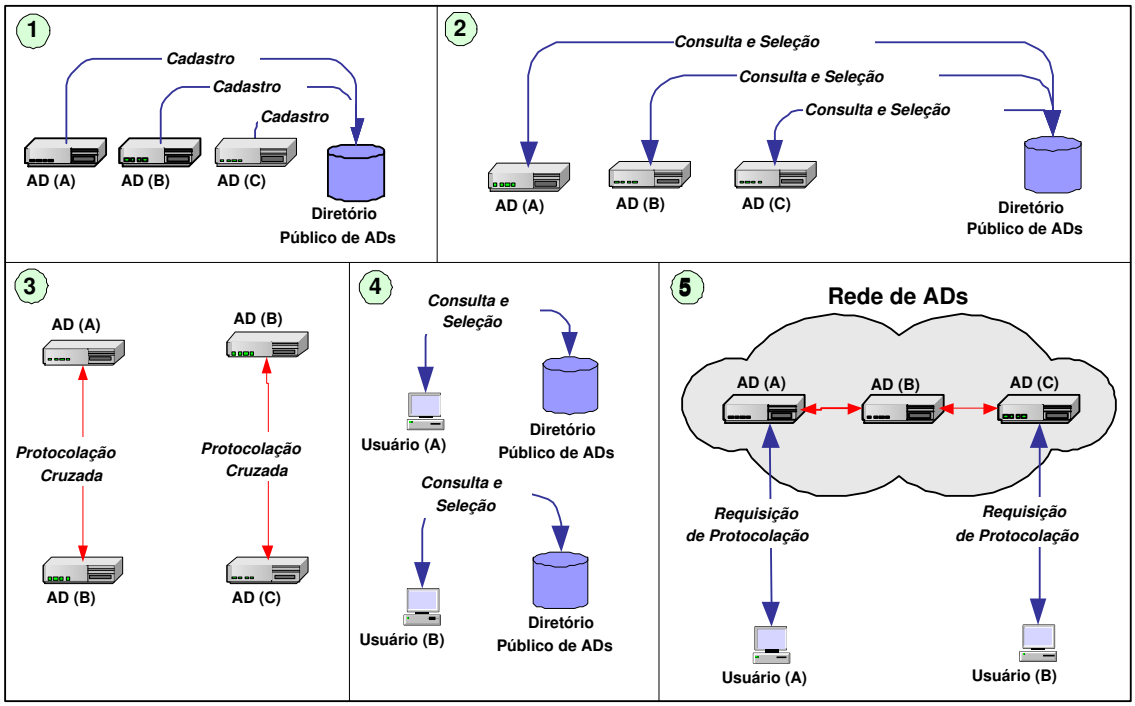


Figura 7.1: Infra-estrutura distribuída de ADs: 1. As ADs cadastram seus dados no Diretório Público. 2. As ADs consultam o Diretório Público para selecionar a AD com a qual irão sincronizar seu encadeamento. 3. Protocolação cruzada entre a AD (A) e a AD (B) e entre a AD(B) e a AD(C). 4. Os usuários consultam o Diretório Público para selecionar a AD para qual irão enviar a requisição. 5. Os usuários enviam a requisição de protocolação para a AD selecionada.

Na Figura 7.2 são apresentadas as mensagens que são trocadas entre as ADs durante uma protocolação cruzada. Primeiramente, a AD (A) gera uma requisição e

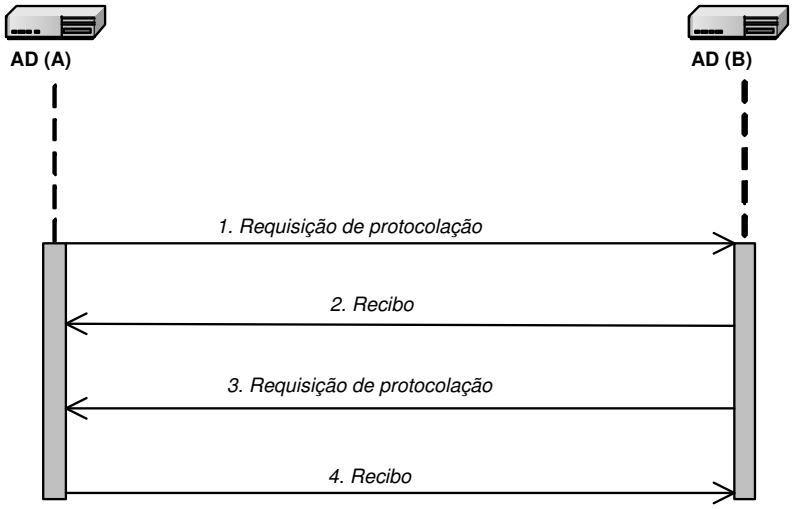


Figura 7.2: Protocolação Cruzada: 1. A AD (A) envia requisição de protocolação para a AD (B). Esta, por sua vez, reconhece que a requisição é referente a uma protocolação cruzada e encadeia o último *link* do seu encadeamento com a informação enviada pela AD (A). 2. Um recibo da protocolação é gerado e enviado para a AD (A). 3. A AD (B) também gera uma requisição e a envia para a AD (A). 4. Esta, por sua vez, reconhece que a requisição é referente a uma protocolação cruzada e também encadeia o último *link* do seu encadeamento com a informação a ser protocolada. Após isso, um recibo é gerado e enviado para a AD(B).

a envia para a AD (B). A informação a ser protocolada é o último *link* do encadeamento e não o resumo de um documento como ocorre normalmente. Após receber a requisição, AD (B) encadeia a informação a ser protocolada com o último *link* do seu encadeamento e envia um recibo para a AD (A). A AD (B) também envia uma requisição para a AD (A), contendo o último *link* do seu encadeamento. Finalmente, a AD (A) protocola esta informação e envia um recibo para a AD (B).

A Figura 7.3 ilustra um exemplo de protocolação cruzada. Neste exemplo, o último *link* do encadeamento da AD (A) é L_b e o último *link* do encadeamento da AD (B) é L_o. A AD (A) envia a requisição de protocolação para a AD (B), e esta, por sua vez, encadeia L_b com o seu último *link*, L_o, gerando assim o Ponto de Sincronismo Z_1. Um recibo é gerado e emitido para a AD (A). Após isso, a AD (B) envia uma requisição para a AD (A), que encadeia L_b com L_o e gera novo Ponto de Sincronismo Z_2. Os pontos Z_1 e Z_2 são iguais, visto que foram gerados a partir das mesmas informações, L_b e L_o. Por isso, esses pontos representam um ponto em comum no encadeamento.

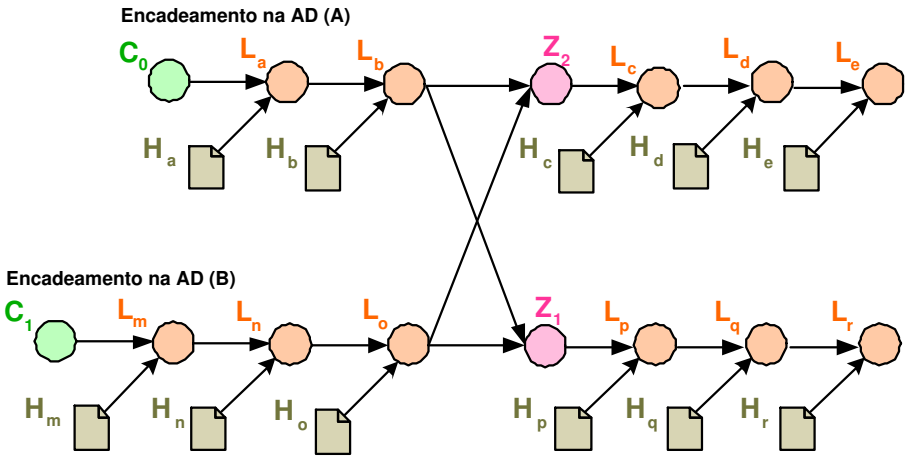


Figura 7.3: Encadeamento na protocolação cruzada

Os Pontos de Sincronismo não deixam de ser um *link* do encadeamento, e, portanto, fazem parte do recibo e do encadeamento. Entretanto, devem ser identificados como pontos de sincronismo.

7.3 Auditoria

Os procedimentos de auditoria apresentados no capítulo 5 consideram o encadeamento de uma única AD. Contudo, no caso de protocolação cruzada, o encadeamento passará a conter uma informação nova, o Ponto de Sincronismo, e, em razão disso, alguns procedimentos adicionais devem ser executados durante a auditoria.

7.3.1 Verificação da validade de um recibo de protocolação

- Para cada Ponto de Sincronismo presente no recibo, identificar a AD com a qual realizou-se a protocolação cruzada e verificar se o seu certificado digital é válido, bem como sua Cadeia de Certificação desde a AC que emitiu o certificado até a AC-Raiz, a qual deve ser confiável;

- Para cada Ponto de Sincronismo presente no recibo, é necessário re-calcular o encadeamento desde o Ponto de Sincronismo até o Ponto de Confiança da AD com a

qual a protocolação cruzada foi realizada.

7.3.2 Verificação da ordem de precedência entre dois documentos protocolados

Para cada Ponto de Sincronismo presente no recibo, identificar a AD com a qual realizou-se a protocolação cruzada e verificar se o seu certificado digital é válido, bem como sua Cadeia de Certificação desde a AC que emitiu o certificado até a AC-Raiz, a qual deve ser confiável. As demais verificações dependem se os documentos foram protocolados pela mesma AD ou por ADs diferentes.

- **Os dois documentos foram protocolados pela mesma AD:** é necessário apenas verificar o encadeamento desde o Ponto de Sincronismo até o Ponto de Confiança da AD com a qual a protocolação cruzada foi realizada;

- **Os documentos foram protocolados por ADs diferentes:** é necessário que tenha ocorrido uma protocolação cruzada entre as ADs que protocolaram os documentos, e, além disso, os documentos devem estar em uma posição favorável no encadeamento. A seguir serão apresentadas as diferentes posições em que os documentos podem estar no encadeamento:

  - **Os dois resumos estão após o Ponto de Sincronismo:** neste caso, será possível saber que os documentos foram protocolados após a protocolação cruzada, porém, o encadeamento não demonstrará qual documento foi protocolado primeiro. Nesta situação, a única maneira de verificar a precedência entre os dois documentos é com base na data e na hora da protocolação. Entretanto, para que a comparação seja válida, é necessário que as duas ADs utilizem uma fonte de tempo confiável e sincronizada.

  - **O primeiro resumo está antes do Ponto de Sincronismo e o segundo está após:** pode-se afirmar que o primeiro resumo foi protocolado primeiro, pois ao re-calcular o encadeamento, percebe-se que quando o segundo resumo foi

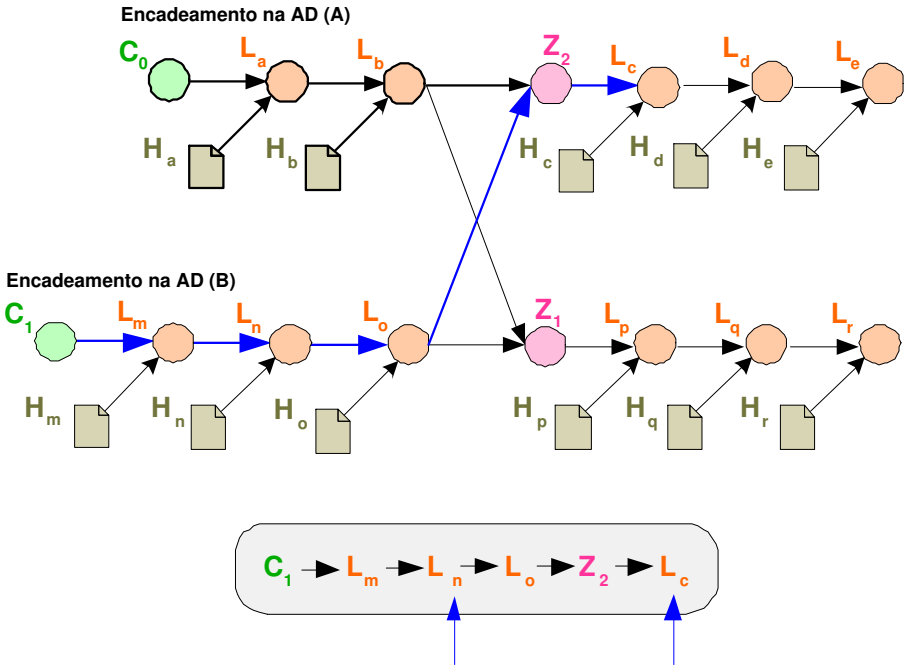


Figura 7.4: Comparação entre documentos protocolados por ADs diferentes

protocolado, o Ponto de Sincronismo já existia, e, conseqüentemente, o primeiro resumo já havia sido protocolado. A Figura 7.4 ilustra um exemplo em que dois documentos foram protocolados por ADs diferentes e encontram-se em uma posição que possibilita concluir qual deles foi protocolado primeiro.

7.3.3 Verificação da integridade do encadeamento armazenado no banco de dados da AD

- Para cada Ponto de Sincronismo presente no recibo, identificar a AD com a qual realizou-se a protocolação cruzada, verificar se o certificado digital é válido e verificar a Cadeia de Certificação desde a AC que emitiu o certificado até a AC-Raiz, a qual deve ser confiável;

- Para cada Ponto de Sincronismo contido no encadeamento, re-calcular os *links* desde o Ponto de Confiança correspondente a cada AD até o Ponto de Sincronismo.

7.4 Conclusão

Neste capítulo foi apresentada uma visão geral de uma infra-estrutura distribuída de protocolação digital, bem como alguns procedimentos adicionais que devem ser realizados no caso de auditoria sobre um encadeamento que inclui protocolação cruzada.

Capítulo 8

Considerações Finais

Documentos eletrônicos protocolados e assinados digitalmente podem ser considerados válidos sob o ponto de vista legal. Através do processo de protocolação pode-se provar que um documento existiu em um determinado instante do tempo no passado e que não foi alterado desde então. É fundamental que o serviço de protocolação seja confiável, de modo a garantir que a data anexada aos documentos é oficial e não será alterada. Neste sentido, a proposta deste trabalho é apresentar mecanismos que aumentem a confiabilidade do processo de protocolação digital.

O objetivo geral deste trabalho foi contemplado na sua totalidade, visto que um estudo da confiabilidade do sistema de protocolação digital foi realizado e foram propostos mecanismos para aumentar a confiança do sistema.

Este trabalho apresentou uma revisão bibliográfica sobre as diferenças entre os documentos tradicionais e os documentos eletrônicos. Através desta revisão constatou-se que para obter a equiparação sob o ponto de vista legal de ambas as formas de documento, é necessário que o documento eletrônico se adeque e apresente, no mínimo, os mesmos requisitos do documento tradicional. Ainda sobre o estudo do documento eletrônico, constatou-se que alguns países já elaboraram leis para regular a eficácia jurídica dos mesmos, enquanto no Brasil, existe apenas uma Medida Provisória, alguns Projetos de Lei e uma Lei Estadual.

O presente trabalho também apresentou uma revisão bibliográfica sobre

os sistemas de protocolação. Comparou-se a confiança provida por um sistema de protocolação de documentos tradicionais com a provida por um sistema de protocolação de documentos eletrônicos. Para realizar esta comparação, visitou-se a seção de Protocolo da Reitoria da UFSC. Constatou-se que a protocolação digital é mais confiável do que a protocolação tradicional, visto que nesta última normalmente não existe sincronização do relógio, lacre de segurança, registro de eventos ou auditoria.

O primeiro objetivo específico desse trabalho foi esclarecer de maneira didática e detalhada o Método da Árvore Sincronizada. Este objetivo foi alcançado e está relatado na seção 3.4 do capítulo 3. Este método foi proposto por Pasqual (2001) em sua dissertação de mestrado, porém a questão dos saltos no Método da Árvore Sincronizada não foi muito detalhada. Este capítulo descreveu o encadeamento dos documentos submetidos em cada rodada, além de esclarecer como ocorrem os saltos, que permitem reduzir o tamanho dos recibos.

O segundo objetivo específico foi identificar os aspectos relevantes da confiança em um sistema de protocolação digital. Este objetivo foi alcançado e está relatado no capítulo 4. Neste capítulo, primeiramente foram definidos os elementos que constituem a confiança de um sistema de protocolação. Em seguida, foram descritos os mecanismos já existentes que provêem confiança ao sistema. Também foram levantadas várias questões referentes ao assunto e, por fim, foram propostos alguns procedimentos para aumentar a confiança do sistema.

O terceiro objetivo específico foi a definição de procedimentos de auditoria que permitam verificar se a Autoridade de Datação agiu de forma honesta durante as protocolações. Este objetivo foi alcançado e está relatado no capítulo 5. Primeiramente foi definido o conceito de auditoria. Em seguida, foram apresentados procedimentos de auditoria para os métodos de datação: Absoluto, Método do Encadeamento Linear e Método da Árvore Sincronizada.

O quarto objetivo específico foi a elaboração de um documento chamado Política de Protocolação. Este objetivo foi alcançado e este documento está descrito no capítulo 6. Este documento descreve de maneira sucinta, o papel dos componentes do sistema de protocolação, bem como suas responsabilidades, obrigações e direitos desde

a implantação da AD até o encerramento de suas atividades. Além disso, apresenta as práticas adotadas pela AD na prestação do serviço de protocolação digital.

O quinto objetivo específico foi uma análise da confiabilidade de uma infra-estrutura distribuída de protocolação. Este objetivo foi alcançado e está descrito no capítulo 7. Este capítulo apresenta uma visão geral de uma infra-estrutura distribuída de protocolação e descreve os procedimentos adicionais que devem ser executados em uma auditoria quando o encadeamento inclui uma protocolação cruzada.

O sexto objetivo específico foi a elaboração de um documento chamado Declaração de Práticas de Protocolação. Este objetivo foi alcançado e este documento está descrito no apêndice B. Este documento descreve de maneira detalhada, o papel dos componentes do sistema de protocolação, bem como suas responsabilidades, obrigações e direitos desde a implantação da AD até o encerramento de suas atividades. Além disso, descreve com detalhes as práticas adotadas pela AD na prestação do serviço de protocolação digital.

Entre os resultados deste trabalho está a publicação de dois artigos científicos. O primeiro artigo foi publicado no I Forum sobre Segurança, Privacidade e Certificação Digital (COSTA, 2003b). O segundo artigo foi publicado no 5^o Simpósio Segurança em Informática (COSTA, 2003a) e foi premiado como segundo melhor artigo científico, recebendo o Prêmio Tércio Pacitti - Siemens - Menção honrosa. O apêndice D apresenta os dois artigos.

Através da utilização dos procedimentos propostos, a AD poderia disponibilizar um serviço de protocolação digital mais confiável e ser utilizada como um componente básico para o atendimento de requisitos de segurança de outros protocolos e aplicações.

8.1 Trabalhos futuros

As sugestões de trabalhos futuros como uma extensão do trabalho apresentado nesta dissertação referem-se primeiramente à adaptação da idéia de re-assinatura digital proposta por Notoya (2002) para o caso dos recibos emitidos por uma Autoridade

de Datação. Através desta adaptação, pode-se garantir a validade do recibo de protocolação por tempo indeterminado.

Um outro trabalho que pode ser desenvolvido futuramente é a validação formal dos procedimentos de auditoria propostos. O presente trabalho apresenta os procedimentos em uma ordem seqüencial de passos que devem ser executados, porém não foi realizada uma formalização dos mesmos.

Além disso, sugere-se que seja realizada uma análise da complexidade dos procedimentos de auditoria propostos, de forma a identificar o impacto em relação ao desempenho do sistema de protocolação digital.

Referências Bibliográficas

ADAMS, C. et al. Rfc 3161: Internet x.509 public key infrastructure time-stamp protocol (tsp). August 2001. Network Working Group Category: Standards Track.

ALEMANHA. *Federal Act Establishing the General Conditions for Information and Communication Services.* 1997. Disponível em <http://www.marcosdacosta.adv.br/>. Acesso em 21 de Abril de 2003.

AURÉLIO. *Dicionário Aurélio Eletrônico - Século XXI*. [S.l.]: Editora Nova Fronteira, 1999.

BORTOLI, D. L. *O Documento Eletrônico no Ofício de Registro Civil de Pessoas Naturais*. Dissertação (Mestrado) — Universidade Federal de Santa Catarina, Julho 2002.

BRASIL. *Projeto de Lei n^o 1.483 do Senado Federal, de 1999. Institui a fatura eletrônica e a assinatura digital nas transações de comércio eletrônico.* 1999. Disponível em <http://www.marcosdacosta.adv.br/>. Acesso em 21 de Abril de 2003.

BRASIL. *Projeto de Lei n^o 1.589/99 da OAB/SP. Dispõe sobre o comércio eletrônico, a validade jurídica do documento eletrônico e a assinatura digital, e dá outras providências.* 1999. Disponível em <http://www.marcosdacosta.adv.br/>. Acesso em 21 de Abril de 2003.

BRASIL. *Projeto de Lei n^o 672 do Senado Federal, de 1999. Dispõe sobre o comério eletrônico.* 1999. Disponível em <http://www.marcosdacosta.adv.br/>. Acesso em 21 de Abril de 2003.

BRASIL. *Proposta de política de governo eletrônico para o poder executivo federal. Proposta do Grupo Técnico de Novas Formas Eletrônicas de Interação*. 2000.

BRASIL. *Medida Provisória n^o 2.200-2. Medida Provisória que intituiu a ICP-Brasil.* Agosto 2001. Disponível em <http://www.senado.gov.br/>. Acesso em 02 de Dezembro de 2002.

BRY. *Declaração de Práticas de Protocolação*. [S.l.], 2001.

BRY. Fevereiro 2003. Disponível em <http://www.bry.com.br/>. Acesso em 25 de Fevereiro de 2003.

BULDAS, A. et al. Time-stamping with binary linking schemes. In: KRAWCZYK, H. (Ed.). *Advances on Cryptology — CRYPTO '98*. Santa Barbara, USA: Springer-Verlag, 1998. (Lecture Notes in Computer Science, v. 1462), p. 486–501. Disponível em: <citeseer.nj.nec.com/article/buldas98timestamping.html>.

CATARINA, S. *Lei n^o 12.137, de 20 de março de 2002. Dispõe sobre a protocolização digital de informações no âmbito da administração pública estadual e adota outras providências.* Março 2002. Disponível em <http://www.marcosdacosta.adv.br/>. Acesso em 23 de Outubro de 2003.

CENTER, N. C. S. *A Guide to Understanding Audit in Trusted Systems*. [S.l.], june 1998.

COSTA, V. et al. Confiança na tempestividade dos documentos eletrônicos: Auditoria da protocolação digital. 5^o *Seminário Segurança em Informática*, p. 9, Outubro 2003.

COSTA, V. et al. Protocolação digital de documentos eletrônicos. *I Forum sobre Segurança, Privacidade e Certificação Digital*, p. 12, Outubro 2003.

CYBERNETICA. *Protocols and data formats for time-stamping service*. [S.l.], 2002.

DEMÉTRIO, D. B. *Infra-estrutura de protocolação digital distribuída de documentos eletrônicos*. [S.l.], 2003.

DIERKS, T.; ALLEN, C. *RFC 2246: The TLS Protocol Version 1.0*. January 1999.

DIGISTAMP. Abril 2003. Disponível em <http://www.e-timestamp.com/>. Acesso em 15 de Abril de 2003.

DUSSE, S. et al. *RFC 2311: S/MIME Version 2 Message Specification*. March 1998.

DUSSE, S. et al. *RFC 2312: Daytime Protocol*. March 1998.

ESTÔNIA. *Digital Signature Act, de 2001. This Act provides the necessary conditions for using digital signatures and the procedure for exercising supervision over the provision of certification services and time-stamping services.* 2000. Disponível em <http://www.marcosdacosta.adv.br/>. Acesso em 21 de Abril de 2003.

EUROPÉIA, C. *Diretiva 1999/93/CE do Parlamento Europeu e do Conselho, de 1999. Institui um quadro legal comunitário para assinaturas eletrônicas e para serviços de certificação,a fim de garantir o funcionamento adequado do mercado interno.* 1999. Disponível em <http://www.marcosdacosta.adv.br/>. Acesso em 21 de Abril de 2003.

GHISLERI, A. S. *Sistema Seguro de Atendimento ao Cliente: Garantia da Qualidade de Serviço*. Dissertação (Mestrado) — Universidade Federal de Santa Catarina, 2002.

GIL, A. C. *Como elaborar projetos de pesquisa*. São Paulo: [s.n.], 1988.

HABER, S.; STORNETTA, W. S. How to time-stamp a digital document. *Lecture Notes in Computer Science*, v. 537, 1991. Disponível em: <citeseer.nj.nec.com/haber91how.html>.

HOUSLEY, R.; POLK, T. *Planning for PKI - Best Practices Guide for Deploying Public Key Infrastructure*. [S.l.]: Wiley Computer Publishing, 2001.

ICP-BRASIL. *Infra-estrutura de Chaves Públicas brasileira*. Abril 2003. Disponível em <http://www.icp.gov.br.br/>. Acesso em 17 de Abril de 2003.

IGNACZAK, L. *Um novo modelo de Infra-estrutura de Chaves Públicas para uso no Brasil utilizando aplicativos com o código fonte aberto*. Dissertação (Mestrado) — Universidade Federal de Santa Catarina, 2002.

JUST, M. Some timestamping protocol failures. *Proceedings of the Internet Society Synposium on Network and Distributed Security (DDSS '98)*, 1998.

KALISKI, B. Rfc 2315: Pkcs #7: Cryptographic message syntax. March 1998. Network Working Group Category: Informational.

KAZIENKO, J. F. *Assinatura Digital de Documentos Eletrônicos através da Impressão Digital*. Dissertação (Mestrado) — Universidade Federal de Santa Catarina, 2003.

KENT, S.; ATKINSON, R. *RFC 1825: Security Architecture for the Internet Protocol*. November 1998.

LABSEC. Setembro 2003. Disponível em <http://www.ufsc.br/labsec>. Acesso em 24 de Setembro de 2003.

LANDWEHR, C. E. Computer security. July 2001.

LIPMAA, H. *Secure and efficient time-stamping systems*. Tese (Doutorado) — University of Tartu - Estonia, July 1999.

LTD., B. *Dicionário Eletrônico Babylon*. version 3.1b. [S.l.]: Editora Nova Fronteira, 2001.

MARCACINI, A. T. R. *Documento Eletrônico como meio de prova*. 2000. Disponível em <http://augustomarcacini.cjb.net/textos/docelet2.html>. Acesso em 24 de Outubro de 2003.

MARQUES, J. F. *Instituições de Direito Processual Civil*. 3 ed. Rio de Janeiro: Forense, 1967.

MENEZES, A. J.; OORSCHOT, P. C. V.; VANSTONE, S. A. *Handbook of Applied Cryptography*. [S.l.]: CRC Press, 1999. 816 p.

MIGNONI, M. E. *Políticas e Declaração de Práticas de Certificação Digital para a UFSC*. Dissertação (Mestrado) — Universidade Federal de Santa Catarina, Junho 2002.

NETSCAPE. *The SSL Protocol Version 3.0*. Março 2003. Disponível em <http://wp.netscape.com/eng/ssl3/>. Acesso em 21 de Março de 2003.

NIST. *FIPS PUB 140-2 Security Requirements for Cryptographic Modules*. Dezembro 2002. Disponível em <http://csrc.nist.gov/cryptval/140-2.htm>. Acesso em 18 de Dezembro de 2002.

NOTOYA, A. E. *IARSDE - Infra Estrutura de Armazenamento e Recuperação Segura de Documentos Eletrônicos: Validade do documento eletrônico por tempo indeterminado*. Dissertação (Mestrado) — Universidade Federal de Santa Catarina, Março 2002.

ON. *Observatório Nacional*. Março 2003. Disponível em <http://www.on.br/>. Acesso em 21 de Março de 2003.

PASQUAL, E. S. *IDDE - Uma Infra-estrutura para a Datação de Documentos Eletrônicos*. Dissertação (Mestrado) — Universidade Federal de Santa Catarina, Abril 2001.

PASQUAL, E. S.; DIAS, J. D. S.; CUSTÓDIO, R. F. A new method for digital time-stamping of electronic document. In: FIRST (Ed.). *Proceedings of the FIRST 14th Annual Computer Security*. 212 West Washington, Suite 1804 Chicago, IL 60606: Phoebe J. Boelter Conference and Publication Services, Ltd., 2002.

PINKAS, D.; POPE, N.; ROSS, J. Policy requirements for time-stamping authorities. August 2003. Internet Group. Target Category: Informational.

PIRES, C. A.; DIAS, M. A. *Auditoria de uma Protocoladora Digital de Documentos Eletrônicos*. [S.l.], 2003.

PORTUGAL. *Decreto-Lei n^o 290-D/99, de 2 de agosto. Regula a validade, eficácia e valor probatório dos documentos electrônicos e a assinatura digital.* 1999. Disponível em <http://www.marcosdacosta.adv.br/>. Acesso em 21 de Abril de 2003.

ROVER, A. J. *Tópicos sobre regulamentação dos documentos eletrônicos*. [S.l.], 2002.

SANTOS, M. A. *Primeiras linhas de Direito Processual Civil: adaptadas ao novo código de processo civil*. 7 ed. São Paulo: Saraiva, 1982.

SCHNEIER, B. *Applied Cryptography - Protocols, Algorithms, and Source Code in C*. Second edition. [S.l.]: John Wiley and Sons, Inc., 1996.

SILVA DIAS, J. da; CUSTÓDIO, R. F.; DEMÉTRIO, D. B. Sincronização segura de relógio para documentos eletrônicos. In: *SBRC 2003*. [S.l.: s.n.], 2003.

STINSON, D. R. *Cryptography - Theory and Practice*. 2 ed. [S.l.]: Chapnan & Hall, 2002. 360 p.

SURETY. Abril 2003. Disponível em <http://www.surety.com/>. Acesso em 03 de Abril de 2003.

SYMMETRICOM. Fevereiro 2003. Disponível em <http://www.datum.com/>. Acesso em 25 de Fevereiro de 2003.

TIMEPROOF. Fevereiro 2003. Disponível em <http://www.timeproof.de/>. Acesso em 25 de Fevereiro de 2003.

UNIDAS, N. *Lei Modelo daA UNCITRAL sobre Comércio Eletrônico*. 1996. Disponível em <http://www.dct.mre.gov.br/>. Acesso em 21 de Abril de 2003.

UNIDOS, E. *Utah Digital Signature Act.* 1995. Disponível em <http://www.marcosdacosta.adv.br/>. Acesso em 21 de Abril de 2003.

UNIDOS, E. *California Government Code.* 1997. Disponível em <http://www.marcosdacosta.adv.br/>. Acesso em 21 de Abril de 2003.

UNIDOS, E. *Electronic Signatures in Global and National Commerce Act.* 2000. Disponível em <http://www.marcosdacosta.adv.br/>. Acesso em 21 de Abril de 2003.

Apêndice A

Glossário

Algoritmo criptográfico: também chamado de cifrador, é uma função matemática utilizada para cifragem e decifragem. A maioria dos algoritmos criptográficos utiliza uma chave, denotada por k, a qual pode assumir um grande número de valores. Esta faixa de valores possíveis é chamada de espaço de chaves. Ambas operações de cifragem e decifragem utilizam a chave k. No processo de cifragem tem-se que $E_{k_1}(M) = C$, ou seja, o texto cifrado C é resultante da aplicação do algoritmo de cifragem E sobre o texto original M, utilizando uma chave k_1. Já no processo de decifragem tem-se que $D_{k_2}(C) = M$, ou seja, através da aplicação do algoritmo de decifragem D sobre o texto cifrado C, utilizando uma chave k_2, obtém-se novamente o texto original M. Além disso, a seguinte propriedade é verdadeira: $D_{k_2}(E_{k_1}(M)) = M$ (SCHNEIER, 1996).

Algoritmo criptográfico (assimétrico) de chave pública: um algoritmo criptográfico que utiliza duas chaves relacionadas, uma chave pública e uma chave privada. As duas chaves têm a propriedade de que é computacionalmente inpraticável derivar a chave privada a partir da chave pública (NIST, 2002). Estes algoritmos são chamados de "chave-pública"porque a chave de cifragem pode ser publicada. Assim, qualquer pessoa pode utilizar a chave pública para cifrar, mas somente uma pessoa específica com a correspondente chave de decifragem pode decifrar a mensagem. Cifragem utilizando uma chave pública k é denotada por: $E_{k_1}(M) = C$. Apesar de

a chave púbica ser diferente da chave privada, a decifragem com a chave privada correspondente é denotada por: $D_{k_2}(C) = M$ (SCHNEIER, 1996).

Algoritmo criptográfico (simétrico) de chave secreta: um algoritmo criptográfico que utiliza uma única chave secreta para cifragem e decifragem (NIST, 2002). Requer que o emissor e o receptor combinem uma chave antes de iniciar a comunicação segura. Cifragem e decifragem com um algoritmo simétrico é denotado por: $E_k(M) = C$ e $D_k(C) = M$ (SCHNEIER, 1996).

Assinatura digital: o resultado de uma transformação criptográfica de um dado, que quando corretamente implementada, provê os serviços de: autenticação na origem, integridade dos dados e não-repúdio do assinante (NIST, 2002). A chave privada é utilizada para gerar a assinatura e a chave pública é utilizada para verificá-la. Na prática, a mensagem original não é assinada diretamente. Na verdade, primeiramente uma função *hash* é aplicada a mensagem e o resultado desta função é assinado. Se Alice utiliza sua chave privada para assinar uma mensagem, Bob pode verificá-la com a chave pública de Alice. Nota-se que Bob não precisa da chave privada de Alice para verificar a assinatura e, além disso, ele não possui a informação necessária para gerar uma assinatura válida (HOUSLEY; POLK, 2001).

Auditar: Ato de conduzir a revisão e o exame das atividades e dos registros de um sistema, de forma independente (CENTER, 1998).

Auditor: Pessoa autorizada e responsável por selecionar os eventos do sistema que serão auditados, além de configurar e analisar os registros que armazenarão os resultados de tais eventos (CENTER, 1998).

Autenticação: Deve ser possível para o receptor da mensagem verificar sua origem; um intruso não deve ser capaz de se fazer passar por outra pessoa (SCHNEIER, 1996).

Autoridade de Certificação: A Autoridade de Certificação (AC) é um bloco de construção básico da Infra-estrutura de Chaves Públicas. A AC é conhecida através de dois atributos: seu nome e sua chave pública. Além disso, executa quatro funções

básicas: emite certificados (isto é, os cria e os assina); mantém informações sobre o *status* dos certificados e emite Listas de Certificados Revogados (LCR); publica os certificados atuais e LCRs; e mantém arquivos com informações de *status* sobre os certificados por ela emitidos e que expiraram ou foram revogados (HOUSLEY; POLK, 2001).

Caminho de Certificação: Lista contendo o nome das ACs que estão hierarquicamente acima da AC que emitiu o certificado digital;

Certificado de chave pública: Declaração assinada digitalmente por uma AC, contendo, no mínimo: o nome da AC que emitiu o certificado; o nome do assinante para quem o certificado foi emitido; a chave pública do assinante; o período de validade operacional do certificado; o número de série do certificado, único em cada AC; e uma assinatura digital da AC que emitiu o certificado com todas as informações citadas acima (BRY, 2001, p. 13).

Chave criptográfica: parâmetro utilizado em conjunto com um algoritmo criptográfico, que determina: a transformação do texto original para o texto cifrado; a transformação do texto cifrado para o texto original; uma assinatura digital computada a partir de um dado; a verificação da assinatura digital computada a partir de um dado; um código de autenticação computado a partir de um dado; ou a troca de senhas compartilhadas (NIST, 2002).

Chave privada: uma chave criptográfica, utilizada com um algoritmo criptográfico de chave pública, que é unicamente associada com uma entidade e não pode ser publicada (NIST, 2002).

Chave pública: uma chave criptográfica utilizada com um algoritmo criptográfico de chave pública, que é unicamente associada com uma entidade e deve ser publicada (NIST, 2002).

Cifrar: Processo de transformação de um texto original em uma forma incrompreensível, usando um algoritmo criptográfico e uma chave criptográfica (BRY, 2001, p. 14).

Confiança: Segurança e bom conceito que inspiram as pessoas de probidade (AURÉLIO, 1999).

Confidencialidade: propriedade que garante que informações não serão acessadas por indivíduos, pessoas ou entidades não autorizadas (NIST, 2002).

***Coordinated Universal Time* (UTC)**: é administrado através de um tratado adotado pela comunidade mundial que designa *National Measurement Institutes* (NMIs) como fontes de tempo UTC. Nos Estados Unidos, o *National Institute of Standards and Technology* (NIST) e na Inglaterra, o *National Physical Laboratory* (NPL) são dois exemplos. Existem aproximadamente 50 centros similares de medidas que são responsáveis pelo tempo oficial no mundo. Essencialmente, se um recibo de protocolação for originado de uma dessas fontes oficiais de tempo, então a autoridade de tempo não pode ser questionada (NIST, 2002).

Criptografia: é a arte e a ciência de manter as mensagens seguras (SCHNEIER, 1996).

Critical Security Parameter (CSP): informações relacionadas à segurança, tais como, chaves criptográficas, senhas e PINs, cuja descoberta ou modificação podem comprometer a segurança de um módulo criptográfico (NIST, 2002).

Firmware: programas e dados que compõem um módulo criptográfico e que são armazenados em um *hardware*, como por exemplo, ROM, PROM, EPROM, EEPROM ou FLASH, e que não podem ser dinamicamente gravadas ou modificadas durante execução (NIST, 2002).

Infra-estrutura de Chaves Públicas: Arquitetura, organização, técnicas, práticas e procedimentos que suportam, em conjunto, a implementação e a operação de um sistema de certificação baseado em criptografia de chaves públicas (BRY, 2001, p. 15).

Integridade: propriedade que garante que uma informação não será modificada ou removida de maneira não autorizada e não detectada (NIST, 2002).

Internet Engineering Task Force: Força Tarefa de Engenharia na *Internet*. Organização que desenvolve padrões para transferência de informação na *Internet* (LTD., 2001).

Lista de Certificados Revogados: É uma ferramenta básica da Infra-estrutura de Chaves Públicas que distribui informação sobre o *status* de certificados de chave pública. Os LCRs (Lista de Certificado Revogados) contém uma lista de números seriais de certificados que apesar de não terem expirado não são mais confiáveis.

***Logs* de auditoria**: Conjunto de registros que provê evidências de que determinado processo foi realizado. Além disso, os *logs* podem ser utilizados para reconstruir uma transação original realizada no sistema (CENTER, 1998).

MD5: Algoritmo criptográfico utilizado para calcular o resumo de um arquivo digital.

Módulo criptográfico: o conjunto de *hardware*, *software* ou *firmware* que implementa funções de segurança, tais como, algoritmos criptográficos e geração de chaves (NIST, 2002).

***Personal Identification Number* (PIN)**: código ou senha alfanumérico utilizado para autenticar uma identidade (NIST, 2002).

Relógio datador: Máquina responsável por protocolar documentos tradicionais. Possui um relógio interno, o qual fornece as informações de data e hora que são impressas ao carimbar um documento.

Resumo: Número único calculado a partir do conteúdo de um arquivo. O resumo também é chamado de função *hash* e exemplos desta função são SHA-1 e MD5. Se pelo menos um caracter do conteúdo do arquivo for modificado e for calculado um resumo a partir do arquivo modificado, um número diferente será calculado. Além disso, a técnica utilizada nesta função garante que dois arquivos nunca gerarão o mesmo número como resumo.

RSA: Algoritmo de criptografia assimétrica, o qual pode ser utilizado para cifrar ou para calcular a assinatura digital de uma informação.

SHA1: Algoritmo criptográfico utilizado para calcular o resumo de arquivo digital.

Sigilo: Condição na qual dados sensíveis são mantidos secretos e divulgados apenas para as partes autorizadas (BRY, 2001, p. 16).

Apêndice B

Proposta de Declaração de Práticas de Protocolação para BRy

B.1 Introdução

A Declaração de Práticas de Protocolação (DPP) é um documento que tem como objetivo descrever, de maneira detalhada, como a AD implementa os procedimentos descritos na PP. Além disso, este documento proporciona aos usuários um melhor entendimento sobre o funcionamento do sistema. Com base na DPP, os usuários podem avaliar o grau de confiança do serviço provido pela AD. Por isso, recomenda-se que a AD também elabore um documento contendo a sua Declaração de Práticas de Protocolação e o disponibilize aos seus usuários. Esta DPP foi elaborada para o sistema de protocolação da BRy (2003) e tem como referência a Política de Protocolação proposta neste trabalho. Além disso, esse documento pode servir de exemplo para outras ADs que desejem elaborar sua própria DPP.

B.2 Disposições gerais

B.2.1 Direitos

A reprodução e distribuição desta Declaração de Práticas de Protocolação é permitida de forma não exclusiva e sem pagamento desde que:

I seja feita referência aos direitos autorais;

II a reprodução seja íntegra e atribuída ao autor.

Para outras permissões de reprodução, um pedido deverá ser enviado ao endereço eletrônico ou físico da AD.

B.2.2 Publicações

Esta DPP está disponível:

- em formato eletrônico:
  - no endereço da AD na WEB em http://www.bry.com.br/downloads/documentacao/dpp.pdf;
  - através do e-mail da AD, pdde@bry.com.br;
  - nos recibos de protocolação;
  - através de referência no certificado digital da AD. Esta referência está incluída no campo de extensões do certificado.
- em papel, pelo endereço da AD:

  BRy Tecnologia
  Rua Lauro Linhares - 2123
  Shopping Trindade - Torre B - sala 306
  Trindade - Florianópolis - SC - Brasil
  CEP: 88036-002 - Fone: (0xx48) 234-6696 334-8888

A Política de Protocolação, na qual a DPP se baseia está disponível:

- em formato eletrônico:
  - no endereço da AD na WEB em http://www.bry.com.br/downloads/documentacao/pp.pdf;
  - através do e-mail da AD.
- em papel, pelo endereço da AD.

B.2.3 Conflito de cláusulas

Em caso de conflito de alguma cláusula da DPP em relação a uma versão anterior, o usuário estará sujeito às cláusulas da versão mais atual, exceto quando as cláusulas desta forem proibidas por lei. Em hipótese alguma será aceita cláusula de versão anterior à DPP vigente.

B.2.4 Direito a emendas

A AD reserva-se o direito de realizar emendas na versão vigente da DPP, se julgar necessário, e as publicará em um repositório. As emendas poderão ou não ocasionar a mudança de versão da DPP. Tal mudança só ocorrerá quando houver uma reestruturação da DPP. As emendas de menor impacto entram em vigor imediatamente após a sua publicação e as de maior impacto entram em vigor após 10 (dez) dias de sua publicação.

B.2.5 Leis aplicáveis

Em todo processo será de uso único as leis brasileiras, as quais regulamentam a interpretação desta DPP, a fim de garantir a uniformidade da interpretação da mesma para todos os usuários.

B.2.6 Resolução de controvérsias

As controvérsias envolvendo a DPP devem ser notificadas à AD visando a sua resolução imediata. Primeiramente é realizado um registro da ocorrência, e em seguida são tomadas as providências necessárias, tais como, uma auditoria.

B.3 Terminologia

Para os propósitos deste documento, os seguintes termos se aplicam:

B.3.1 Abreviações

AD	Autoridade de Datação
DPP	Declaração de Práticas de Protocolação
PP	Política de Protocolação
UTC	*Coordinated Universal Time*

B.3.2 Definições

Parte confiável: Receptor de um recibo de protocolação que confia no recibo;

Assinante: Entidade que requisita os serviços providos por uma AD e que concorda implícita ou explicitamente com seus termos e condições;

Recibo de protocolação: Objeto de dados que vincula a representação de uma informação com um momento específico do tempo, estabelecendo, dessa forma, uma evidência de que a informação existiu antes daquele momento;

Autoridade de Datação: Autoridade que emite os recibos de protocolação;

Declaração de Práticas de Protocolação: Declaração das práticas que a AD emprega na emissão de recibos de protocolação;

Sistema de Protocolação: Composição de produtos de TI[1] e componentes organizados para dar suporte ao fornecimento de serviços de protocolação;

Política de Protocolação: Conjunto de regras que indicam a aplicabilidade de um recibo de protocolação para uma comunidade particular e/ou classe de aplicações com requisitos comuns de segurança;

Coordinated Universal Time (UTC): Escala de tempo administrada através de um tratado adotado pela comunidade mundial que designa *National Measurement Institutes* (NMIs) como fontes de tempo UTC. Nos Estados Unidos, o *National Institute of Standards and Technology* (NIST) e na Inglaterra, o *National Physical Laboratory* (NPL) são dois exemplos. Existem aproximadamente 50 centros similares de medidas que são responsáveis pelo tempo oficial no mundo;

UTC(k): Escala de tempo realizada pelo laboratório "k"e mantida em acordo com UTC, com o objetivo de alcançar mais ou menos 100 ns.

B.3.3 Conceitos gerais

Serviços de protocolação: O serviço de protocolação é dividido em dois componentes:

- **Fornecimento de protocolação:** Serviço que gera os recibos;
- **Gerência da protocolação:** Serviço que monitora e controla a operação de um serviço de protocolação para garantir que o serviço está sendo provido como é especificado pela AD. Este serviço é responsável pela instalação e desinstalação do serviço de fornecimento de protocolação. Por exemplo, o serviço de gerência de protocolação garante que o relógio utilizado para protocolar está corretamente sincronizado com o UTC.

Autoridade de Datação: A autoridade na qual os usuários dos serviços de protocolação confiam (assinantes e partes confiáveis) para emitir os recibos. Mesmo que a AD

[1]Tecnologia da Informação - termo abrangente para métodos de computação, processamento de informação e comunicação de dados

utilize outros componentes para prover o serviço de protocolação, ela sempre deverá garantir o que está especificado na Política de Protocolação.

Assinante: O assinante pode ser uma organização compreendendo vários usuários finais ou pode ser um único usuário final. Quando o assinante é uma organização, algumas das obrigações que se aplicam à organização serão aplicadas aos usuários finais. A organização será responsabilizada, caso as obrigações de um usuário final não sejam cumpridas corretamente. Quando o assinante é um usuário final, ele é o responsável direto, se suas obrigações não forem cumpridas.

Política de Protocolação e Declaração de Práticas de Protocolação: Em geral, uma Política de Protocolação (PP) especifica "o que deve ser feito"num sistema de protocolação digital, enquanto uma Declaração de Práticas de Protocolação (DPP) especifica "como é feito". Uma PP é um documento menos específico do que uma DPP. Uma DPP é uma descrição mais detalhada dos termos e das condições, bem como das práticas operacionais e administrativas de uma AD na emissão e na gerência do serviço de protocolação. A DPP de uma AD reforça as regras estabelecidas na PP. A DPP define como uma determinada AD atende aos requisitos técnicos e organizacionais identificados na PP. O objetivo de uma PP é significativamente diferente do de uma DPP. Uma PP é definida independentemente dos detalhes específicos de um ambiente operacional específico de uma AD, enquanto uma DPP é elaborada para uma estrutura organizacional, procedimentos operacionais, facilidades e ambiente computacional específicos de uma AD.

B.4 Obrigações e responsabilidades

B.4.1 Obrigações da AD

Geral: A AD deve garantir que todas as práticas de protocolação apresentadas neste documento, são implementados de acordo com a Política de Protocolação. A AD deve garantir a conformidade com os procedimentos descritos nesta política, mesmo

quando as funcionalidade da AD estão sob responsabilidade de sub-contratados.

Obrigações da AD com relação aos assinantes: A AD deve atender as declarações expressas nestes termos e condições, incluindo a disponibilidade e a precisão de seus serviços.

B.4.2 Obrigações do assinante

É recomendável que o usuário, ao obter o recibo de protocolação, verifique se o recibo foi assinado corretamente, se o certificado digital da AD não expirou ou foi revogado, além de verificar a validade da cadeia de certificação do certificado da AD até a AC Raiz, a qual deve ser confiável.

B.4.3 Obrigações da parte confiável

As partes confiáveis têm a obrigação de realizar as seguintes verificações antes de confiar em um recibo:

- Verificar se o recibo foi assinado corretamente e se a chave privada utilizada para assinar o recibo não foi comprometida até o momento da verificação;
- Considerar qualquer limitação no uso do recibo quando indicado na Política de Protocolação;
- Considerar qualquer precaução prescrita no contrato ou em qualquer outro lugar.

B.4.4 Responsabilidade da AD

A AD exclui qualquer responsabilidade, a menos que seja estipulada por lei aplicável. Além disso, a AD não é responsável por danos, atrasos ou falhas no desempenho de suas atividades resultantes de eventos de força maior, os quais estão além de seu controle, tais como: guerras, terremotos, fogo, enchentes e outros.

B.5 Práticas da AD

B.5.1 Declaração de Divulgação da AD

Estas informações têm como objetivo divulgar para todos os assinantes e potenciais partes confiáveis os termos e condições referentes à utilização de serviços de protocolação.

Informação de contato:

BRy Tecnologia
Rua Lauro Linhares - 2123
Shopping Trindade - Torre B - sala 306
Trindade - Florianópolis - SC - Brasil
CEP: 88036-002 - Fone: (0xx48) 234-6696 334-8888

Política de Protocolação: Política de Protocolação versão 1.0.

Algoritmo de *hash* utilizado no cálculo do resumo do documento: SHA-1, 160 *bits*.

Algoritmo de assinatura digital: RSA com SHA-1.

Tamanho da chave da AD: 1024 bits.

Tempo de vida esperado da assinatura digital: 5 anos.

Precisão do tempo com relação ao UTC: Depende do desempenho da rede, ficando em torno de 125 ms, que é a precisão assegura pelo NTP (*Network Time Protocol*).

Informações sobre como verificar o recibo de protocolação: Para verificar o recibo de protocolação, a parte confiável deve obter o certificado digital da AD e verificar sua validade, bem como a validade da Cadeia de Certificação até a AC Raiz. Além disso, deve-se verificar a assinatura digital da AD sobre o recibo. A parte confiável também deve verificar o encadeamento. Para tanto, é necessário identificar se o resumo do documento está contido no encadeamento e verificar se o Ponto de Confiança incluído no recibo foi publicado no Diretório Público. Após isto, os *links* contidos no recibo devem ser re-calculados.

Período de tempo durante o qual os *logs* dos eventos serão armazenados: Os *logs* são armazenados no banco de dados da AD e são exportados para um meio de armazenamento externo quando atingem um tamanho máximo. Assim como o encadeamento, os *logs* ficam armazenados por tempo indeterminado, visto que os usuários podem desejar verificar estas informações a qualquer momento.

A AD foi avaliada de acordo com a Política de Protocolação e isto foi realizado por uma corporação independente: Não.

Comunicação entre o assinante e a AD: A AD utiliza o formato definido na RFC 3161 (ADAMS, 2001) para requisição de protocolação e emissão de recibos.

Disponibilidade de seu serviço: Os serviços de protocolação digital de documentos eletrônicos fornecidos pela AD estão disponíveis 24 horas por dia, sete dias por semana. Porém, poderão ocorrer interrupções na disponibilidade do serviço devido a procedimentos administrativos, falhas na rede ou no equipamento. Se a AD estiver em uma *Intranet*, tanto o cliente quanto o servidor estariam na mesma rede, e, assim, a disponibilidade da rede seria de de 99,99%. Caso a AD aceite requisições da *Internet*, a disponibilidade da rede depende da conexão com a *Internet*, tanto do lado do usuário quanto do servidor. A conexão da BRy com a *Internet* tem 99,95% de disponibilidade. Entre os procedimentos administrativos que podem interromper a disponibilidade do serviço estão: publicação do ponto de confiança, auditoria, requisição de novo certificado digital e recuperação de falhas. O tempo médio esperado entre falhas do *software* é ilimitado, ou seja, livre de erros. Já o equipamento assegura um tempo médio entre falhas (MTBF[2]) de 100 mil horas. No caso de uma eventual falha, o equipamento é recolhido para manutenção e um outro equipamento é colocado em seu lugar ou o fluxo é direcionado para uma AD redundante. Se houver uma violação física da AD, o certificado digital é imediatamente revogado e é realizada uma pericia para determinar os motivos.

[2]MTBF (*Mean Time Between Failures*) é o tempo médio entre falhas do sistema e é igual a MTTF + MTTR, onde MTTF (*Mean To Failure*) é o tempo esperado até a primeira ocorrência de falha e MTTR (*Mean Time To Repair*) é o tempo médio para reparo do sistema.

Redundância dos recursos: A redundância é opcional e depende das exigências do assinante.

B.5.2 Gerenciamento de chaves

Geração do par de chaves da AD: A AD garante que todas as chaves são geradas sob circunstâncias controladas.

- A geração da chave de assinatura da AD é realizada em um ambiente físico seguro por pessoal que exerça uma função de confiança;
- A geração da chave de assinatura da AD é realizada dentro de um módulo criptográfico, o qual atende os requisitos identificados no FIPS 140-2 (NIST, 2002) nível 3.
- O algoritmo utilizado para assinar os recibos é o RSA e o comprimento da chave é de 1024 *bits*.

Proteção da chave privada da AD: A AD garante que sua chave privada permanece confidencial e íntegra.

- A chave privada da AD é mantida e utilizada dentro de módulos criptográficos que atendem os requisitos identificados na FIPS 140-2 (NIST, 2002) nível 3;
- Com o objetivo de minimizar o risco de comprometimento da chave privada da AD, não é realizado *backup* da mesma;

Distribuição da chave pública da AD: A AD garante que a integridade e a autenticidade de sua chave pública, bem como que os parâmetros associados serão preservados durante a distribuição às partes confiáveis.

- A chave pública da AD é disponibilizada às partes confiáveis em um certificado de chave pública. O certificado digital da AD é emitido por uma Autoridade Certificadora operada pela mesma organização que opera a AD;

- O certificado contendo a chave pública da AD é emitido por uma Autoridade Certificadora que opera sob uma Política de Certificados que fornece um nível de segurança equivalente ou superior a Política de Protocolação;
- O certificado também é distribuído nas protocolações, visto que os recibos contêm o certificado digital da AD.

Troca do par de chaves da AD: O tempo de vida do certificado da AD é configurável, porém, geralmente é de 1 (um) ano, para que seja menor do que o período de tempo considerado seguro, no que diz respeito ao algoritmo e ao comprimento da chave utilizados. Além disso, os registros referentes aos serviços de protocolação são armazenados por tempo indeterminado.

Fim do ciclo de vida do par de chaves da AD: A AD garante que sua chave privada não será utilizada após o fim de seu ciclo de vida. O sistema de protocolação está programado para não protocolar nenhum documento quando detectar que o certificado da AD expirou. Quando isso ocorre, um novo certificado digital é gerado. O Módulo Público permite que uma requisição de criação de certificado seja gerada e enviada para uma Autoridade Certificadora. Ao gerar um novo certificado digital, a chave privada anterior é destruída e uma nova chave é gerada. Este procedimento implica em uma paralisação do serviço de protocolação até que o novo certificado seja instalado.

Gerência do ciclo de vida dos módulos criptográficos utilizados para assinar os recibos: A AD garante a segurança do *hardware* criptográfico por todo o seu ciclo de vida. A AD garante que:

- O módulo criptográfico utilizado para assinar os recibos não é violado durante o carga de informações no módulo;
- O módulo criptográfico utilizado para assinar os recibos não é violado enquanto fica armazenado;

- A instalação e a ativação da chave privada da AD no módulo criptográfico é realizada apenas por pessoal que possui funções de confiança e em um ambiente fisicamente seguro;
- O módulo criptográfico utilizado para assinar os recibos está funcionando corretamente;
- A chave privada armazenada no módulo criptográfico é destruída assim que o dispositivo é desativado.

B.5.3 Protocolação

Encadeamento: A AD garante a que os documentos protocolados são encadeados corretamente.

- A AD utiliza um método de datação híbrida, visto que combina o Método de Datação Absoluta com o Método da Árvore Sincronizada. Estes métodos são apresentados com detalhes na seção 3.4 do capítulo 3.
- A AD fornece procedimentos de auditoria que permitem inspecionar o funcionamento da AD. O sistema de protocolação oferece uma operação que retorna o banco de dados da AD o os arquivos de *log* para que sejam auditados. Estas informações são protocoladas antes de serem exportadas. Como o banco de dados da AD, ou mesmo os arquivos de *log* podem ser muito grandes, a AD ficará indisponível durante a execução deste procedimento administrativo. Devido a isso, esta operação deve ser realizada fora dos horários mais utilizados pelos assinantes. Os procedimentos de auditoria para o Método da Árvore Sincronizada são apresentados com detalhes na seção 5.4 do capítulo 5.
- A AD publica pontos de confiança periodicamente, com o objetivo de criar âncoras temporais. Quando o Ponto de Confiança é exportado, uma cópia do banco de dados é realizada e esta informação é protocolada e disponibilizada para que seja armazenada em um meio externo, como um CD-Rom ou uma fita DAT. O último *link* do encadeamento passa a ser o novo de Ponto de Confiança

e os demais *links* são removidos. Este assunto é tratado com detalhes na seção 4.5 do capítulo 4.

Recibo de protocolação: A AD garante que os recibos são emitidos de maneira segura e incluindo a data e a hora correntes corretamente.

- O recibo inclui:
  - um identificador para a Política de Protocolação;
  - um identificador único do recibo;
  - data e hora da protocolação;
  - uma representação da informação que está sendo protocolada, neste caso, o *hash* da informação;
  - um identificador do país em que a AD está;
  - um identificador da AD, o qual é um *General Name* obtido do certificado digital da AD;
  - encadeamento desde o Ponto de Confiança até o documento protocolado.
- A informação de data e hora anexada no recibo é rastreável até um valor de tempo real distribuído pelo Observatório Nacional (ON, 2003);
- A informação de data e hora incluída no recibo é sincronizada com o UTC com uma precisão de 125 ms;
- Se for detectado que o relógio do servidor de protocolação está fora da precisão estabelecida, então os recibos não são emitidos;
- O recibo é assinado com uma chave gerada exclusivamente para este propósito, a chave privada da AD.

Sincronização do relógio com o UTC: A AD garante que o seu relógio está sincronizado com o UTC dentro da precisão declarada. AD utiliza o NTP (*Network Time Protocol*) para sincronizar seu relógio interno com o relógio do Observatório Nacional (ON, 2003), o qual gera a hora oficial no Brasil. Além disso, existe um sistema

de auditoria que periodicamente requisita a hora do relógio interno da AD e a compara como a hora oficial. Após a auditoria, o servidor de tempo pode emitir um certificado de atributo, no qual garante que o relógio da AD está correto e que essa AD está apta para continuar funcionando por um determinado período de tempo. A auditoria tem como principal função monitorar o relógio da AD, de modo que se for detectado que o relógio é defeituoso ou que a AD atua de forma maliciosa, seu tempo é corrigido, ou, em casos extremos, a AD é excluída da rede NTP. Além disso, o NTP está preparado para tratar o *leap second*[3].

B.5.4 Gerência e operação da AD

Gerência da Segurança: A AD garante que os procedimentos administrativos e gerenciais são aplicados adequadamente e correspondem com as melhores práticas reconhecidas.

- A AD retém responsabilidade por todos os aspectos de fornecimento do serviço de protocolação dentro do escopo da Política de Protocolação, mesmo que algumas funções sejam realizadas por terceiros sub-contratados;
- O gerenciamento da AD trata da questão da segurança da informação através de uma comissão responsável por definir a política de segurança das informações da AD. A AD garante a publicação e a comunicação desta política a todos os funcionários que são afetados por ela;
- A infra-estrutura de segurança de informação necessária para gerenciar a segurança dentro da AD sofre manutenção todo o tempo. Qualquer alteração que tenha impacto no nível de segurança provido deve ser aprovada pela comissão;
- Os controles de segurança e os procedimentos operacionais para os sistemas e recursos de informação que fornecem o serviço de protocolação são documentados, implementados e passam por manutenção;

[3] *Leap second* é um ajuste no UTC pela subtração ou adição de um segundo extra no último segundo do mês. Preferencialmente isto é realizado no final de dezembro e junho, e em alguns casos, os meses de março e setembro são escolhidos.

- A AD garante que a segurança da informação passa por manutenção quando a responsabilidade das funções da AD são realocadas para outra organização.

Gerência e classificação de recurso: A AD garante que suas informações e seus recursos recebem um nível adequado de proteção. A AD mantém um inventário de todos os recursos e atribui uma classificação para os requisitos de proteção consistente com uma análise de risco.

Segurança do pessoal: A AD utiliza práticas de contratação que visam manter a confiabilidade de suas operações.

- A AD emprega pessoal que possua conhecimento no assunto, experiência e qualificações necessárias para o serviço oferecido e apropriadas para a função do trabalho. Esses requisitos podem ser atendidos através de treinamento formal e crendenciais, experiência real ou uma combinação dos dois.
- A AD elabora um documento que lista cada função de segurança juntamente com a descrição do trabalho e as respectivas responsabilidades. Além disso, as funções de confiança das quais a segurança da AD depende são claramente identificadas neste documento;
- Existe uma diferenciação entre as funções gerais e as funções específicas da AD, pois cada qual requer diferentes habilidades e requisitos de experiência;
- O pessoal exerce procedimentos administrativos e gerenciais de acordo com os procedimentos de gerência da segurança de informação da AD;
- Para os cargos administrativos e gerenciais, o pessoal a ser contratado deve possuir:
  - Conhecimento da tecnologia de protocolação;
  - Conhecimento da tecnologia de assinatura digital;
  - Conhecimento dos mecanismos para calibragem e sincronização do relógio da AD com o UTC;
  - Familiaridade com procedimentos de segurança para pessoal;

  - Experiência com segurança da informação e análise de riscos.

- Todo o pessoal que exerce função de confiança não tem nenhum tipo de conflito de interesses que possa prejudicar a imparcialidade das operações da AD;
- Funções de confiança incluem papéis que envolvem as seguintes responsabilidades:
  - Oficiais de segurança: Abrange a responsabilidade por administrar a implementação das práticas de segurança;
  - Administradores do sistema: Autorizados a instalar, configurar e prestar manutenção nos sistemas da AD para gerência da protocolação;
  - Operadores de sistema: Responsáveis por operar sistemas da AD no dia-a-dia. Autorizados a executar *backup* e recuperação do sistema;
  - Auditores do sistema: Autorizados a visualizar os arquivos e os registros de auditoria dos sistemas da AD.
- O pessoal a ser contratado para exercer função de confiança é selecionado pelo gerente *senior* responsável pela segurança;
- A AD não seleciona para exercer função de confiança ou gerencial pessoal condenado por crime sério ou outra ofensa que afete sua compatibilidade com a função.

Segurança física e ambiental: A AD garante que o acesso físico a serviços críticos é controlado e que os riscos físicos a estes serviços são minimizados.

- Tanto para o serviço de fornecimento de protocolação quanto para o de gerência de protocolação:
  - Apenas as pessoas autorizadas têm acesso físico aos recursos relativos ao serviço de protocolação;
  - A AD dispõe de controles que são implementados para evitar perda, dano ou comprometimento dos recursos e interrupção das atividades do

serviço de protocolação. O local é publicamente identificado, o acesso físico é controlado por sistemas de segurança, tais como: cartões e chaves de acesso;

  - A AD também dispõe de controles que são implementados para evitar o comprometimento ou o roubo de informação ou equipamento de processamento de informação.

- A AD controla o acesso aos módulos criptográficos para atender os requisitos de segurança identificados na geração do par de chaves da AD e na proteção da chave privada da AD;
- Os equipamentos referentes à gerência de protocolação são operados em um ambiente que protege fisicamente os serviços de algum comprometimento decorrente de um acesso não autorizado ao sistema ou aos dados;
- A AD é protegida fisicamente através da criação de perímetros bem definidos de segurança em torno da gerência de protocolação. Qualquer parte do local que é compartilhado com outras organizações está fora deste perímetro;
- A AD dispõe de controles de segurança física e ambiental implementados para proteger os equipamentos onde estão os recursos do sistema e os recursos utilizados para dar suporte a sua operação. A política de segurança física e ambiental da AD para sistemas relativos à gerência de protocolação definem um nível mínimo de controle de acesso físico, proteção contra desastre natural, fatores de segurança contra incêndio, colapso da estrutura, vazamentos, proteção contra roubo, invasão e recuperação de desastre.
- A AD também dispõe de controles implementados para evitar que informações referentes aos equipamento, mídia ou *software* relacionados aos serviços de protocolação sejam levados para fora do local sem autorização. Existe um plano de contingência a ser executado em caso de corrupção ou perda de recursos computacionais, aplicativos e/ou dados. Este plano está disponível no endereço
  http://www.bry.com.br/downloads/documentacao/plano_contingencia.pdf.

Gerência das operações: A AD garante que os componentes são seguros e operam corretamente, com um risco mínimo de falha.

- A integridade das informações e dos componentes do sistema da AD é protegida contra vírus e *softwares* maliciosos e não autorizados;
- O relato de incidente e procedimentos de resposta são empregados de forma que o dano dos incidentes de segurança e funcionamento defeituoso sejam minimizados;
- A mídia utilizada dentro dos sistemas da AD é manipulada com segurança para protegê-la de dano, roubo, acesso não autorizado ou obsoleto;
- Procedimentos são estabelecidos e implementados para todas as funções de confiança e administrativas que têm impacto sobre o serviço de de protocolação;
- Toda mídia é manipulada com segurança de acordo com os requisitos do esquema de classificação de informação;
- Para garantir que um poder adequado de processamento e armazenamento estará disponível, é realizada uma monitoração da demanda da capacidade e uma projeção dos requisitos de capacidade;
- A AD age de maneira coordenada para responder rapidamente aos incidentes e limitar o impacto de brechas de segurança. Para tanto, todos os incidentes são relatados o mais rápido possível;
- As operações de segurança são separadas das demais operações.

Gerência do acesso ao sistema: A AD garante que apenas pessoas autorizadas têm acesso ao sistema.

- Controles são implementados para proteger o domínio da rede interna da AD do acesso não autorizado. Existe um *firewall* que protege a AD da rede externa. O administrador pode configurar com quem a AD irá se comunicar. O *firewall* fecha todas as portas, com exceção:

  - Porta 123: neste caso, a restrição de sincronismo é feita pelo próprio NTP;
  - Porta 318: para IPs que estão autorizados a utilizar o serviço de protocolação. O administrador pode configurar os IPs que podem protocolar diretamente;
  - Porta 443: disponível apenas para o administrador, o qual pode restringir a partir de qual IP ele irá gerenciar o equipamento;
  - Porta 4433: Sincronizador/Auditor, programa que é executado em paralelo ao NTP. É responsável por autenticar e liberar o uso do NTP. Neste caso, somente o IP do auditor está liberado.

- A AD administra o acesso de usuários (incluindo operadores, administradores e auditores) para manter a segurança do sistema, incluindo gerência da conta dos usuários, auditoria, modificação da hora ou remoção de acesso;
- A AD garante que o acesso a informação e funções do sistema de aplicação é restrito de acordo com a política de controle de acesso. Particularmente, o uso dos programas utilitários do sistema é restrito e fortemente controlado;
- O pessoal é apropriadamente identificado e autenticado antes do uso de aplicações críticas relacionas com a protocolação;
- As atividades do pessoal são registradas;
- A AD mantém os componentes da rede local em um ambiente físico seguro e suas configurações são periodicamente auditadas para atender os requisitos especificados pela AD;
- Monitoramento contínuo e aparelhos de alarme são utilizados para que a AD seja capaz de detectar, registrar e reagir rapidamente em situação de tentativa irregular e/ou não autorizada de acesso aos seus recursos. A AD dispõe de um Sistema de Detecção de Intrusão, monitoramento do controle de acesso e alarmes.

Sistemas de desenvolvimento e manutenção: A AD utiliza sistemas e produtos que são

protegidos contra modificação.

- É realizada uma análise dos requisitos de segurança nas fases de projeto e de especificação de requisitos de qualquer projeto de desenvolvimento sob responsabilidade da AD;
- Procedimentos de controle de alterações são aplicados para *releases*, *softwares* de modificação e alterações de emergência de qualquer *software* operacional.

Comprometimento dos serviços da AD: A AD garante que no caso de evento que afete a segurança de seus serviços, incluindo o comprometimento de sua chave privada ou detecção da perda de calibragem, informações relevantes serão disponibilizadas para os assinantes e para as terceira partes confiáveis. O plano de recuperação de desastre trata do comprometimento, da suspeita de comprometimento da chave privada da AD e da perda de calibragem do relógio, que podem afetar os recibos emitidos. Nestes casos:

- A AD disponibilizará a todos os assinantes e às partes confiáveis uma descrição do comprometimento que ocorreu;
- A AD não emitirá recibos de protocolação até que os passos de recuperação do comprometimento tenham sido executados;
- Sempre que possível, a AD disponibilizará a todos os assinantes e partes confiáveis informação que possa ser utilizada para identificar os recibos que podem ter sido afetados, a menos que isto afete a privacidade dos usuários da AD ou a segurança de seus serviços.

Término da AD: A AD garante que eventuais interrupções decorrentes da pausa dos serviços de protocolação serão minimizadas e, em particular, garante manutenção contínua da informação necessária para verificar a validade dos recibos de protocolação.

- Antes de a AD finalizar seus serviços de protocolação, os seguintes procedimentos são executados:
  - A AD disponibiliza a todos os assinantes e às partes confiáveis informações referentes ao seu término;
  - A AD finaliza a autorização de todos os sub-contratados;
  - A AD transfere obrigações para uma parte confiável para manter os registros de eventos e os registros de auditoria necessários para demonstrar a correta operação da AD por um período razoável;
  - A AD mantém ou transfere para uma parte confiável suas obrigações para disponibilizar sua chave pública e seu certificado às partes confiáveis por um período razoável;
  - A chave privada da AD é destruída, de maneira que não possa ser recuperada.
- A AD assegura estar preparada para cobrir os custos para atender estes requisitos mínimos em caso de falência;
- A AD executa os passos necessários para revogar seu certificado.

Conformidade com os requisitos legais: A AD garante conformidade com os requisitos legais.

- Medidas técnicas e organizacionais são adotadas contra o processamento não autorizado e ilegal de dados pessoais e contra perda acidental, destruição ou dano a dados pessoais.
- A informação dos usuários que a AD tem armazenada é protegida de divulgação, a menos que o usuário esteja de acordo, por ordem judicial ou outro requisito legal.

Registro de informações referentes à operação do serviço de protocolação: A AD garante que toda informação relevante referente à operação dos serviços de protocolação é registrada por um período mínimo definido de tempo, em particular para o fornecimento de evidência para processos judiciais.

- Os eventos e dados a serem registrados em *logs* são documentados pela AD;
- A confidencialidade e a integridade dos registros correntes e arquivados referentes à operação dos serviços de protocolação são mantidos;
- Os registros referentes à operação dos serviços de protocolação são arquivados de maneira confidencial de acordo com práticas de divulgação;
- Registros referentes aos serviços de protocolação são mantidos por um período de tempo após a expiração da validade das chaves da AD;
- Dentre os eventos registrados pela AD estão:
  - Gerenciamento de chave;
  - Sincronização do relógio da AD com o UTC, incluindo detecção de perda de sincronização, re-calibragem e precisão do relógio;
  - Saltos no Método da Árvore Sincronizada;
  - Protocolação cruzada;
  - Ciclo de vida do certificado da AD;
  - Ciclo de vida do par de chaves da AD.
- Os eventos são registrados de maneira que não é possível removê-los ou destruí-los facilmente dentro do período de tempo em que devem ser mantidos;
- Qualquer informação registrada sobre os assinantes são mantidas confidenciais, exceto quando o assinante concorda com a publicação dos seus dados.

B.5.5 Organizacional

A AD garante que sua organização é confiável.

- Políticas e procedimentos sob os quais a AD opera não são discriminativos;
- A AD disponibiliza seus serviços a todos os requerentes cujas atividades se enquadram na sua área declarada de operação e que concordam em obedecer as obrigações especificadas na Declaração de Divulgação da AD;

- A AD possui um sistema de qualidade e de gerência de segurança da informação apropriado para os serviços de protocolação por ela providos;
- A AD possui infra-estrutura adequada para cobrir as responsabilidades oriundas de suas operações;
- A AD possui estabilidade financeira e os recursos necessários para operar em conformidade com sua política;
- A AD emprega um número suficiente de pessoal, os quais possuem educação, treinamento, conhecimento técnico e experiência referente ao tipo, faixa e volume de trabalho necessários para prover os serviços de protocolação;
- A AD possui políticas e procedimentos para resolução de reclamações e disputas recebidas dos clientes ou de outras partes sobre a provisão dos serviços de protocolação ou de qualquer matéria relacionada;
- A AD possui acordos e relações de contratos apropriadamente documentados, onde a provisão dos serviços envolve sub-contratação, terceirização ou outra relação com uma terceira parte.

B.5.6 Taxas

A AD está livre para cobrar pelo serviço de protocolação e as taxas de cobrança pelo serviço são definidas e estabelecidas pela AD e são disponibilizadas no seu repositório. As taxas são passíveis de alterações.

Apêndice C

Protótipo de um sistema de auditoria para o Método do Encadeamento Linear

C.1 Introdução

Como foi visto anteriormente, as técnicas utilizadas nos sistemas de protocolação digital de documentos eletrônicos não garantem completamente a confiança do sistema. Em virtude disso, alguns procedimentos de auditoria devem ser realizados para inspecionar as atividades desenvolvidas pela AD. No capítulo 5 foram definidos procedimentos de auditoria para alguns métodos de datação.

Neste capítulo é apresentado um protótipo de um sistema de auditoria para ADs que utilizem como método de datação o Método do Método do Encadeamento Linear. Na seção C.2 são descritas as funcionalidades do sistema. A seção C.3 apresenta as considerações finais.

C.2 Apresentação

O protótipo de um sistema de auditoria para o Método do Encadeamento Linear foi implementado por dois alunos de graduação em seu Trabalho de Conclusão de Curso (PIRES; DIAS, 2003). A implementação do protótipo se baseou no sistema de protocolação digital comercializado pela BRy (2003).

No desenvolvimento do protótipo foram utilizadas as seguintes ferramentas: Sistema de Gerenciamento de Banco de Dados *Interbase 6*, linguagem de programação C++ e o ambiente de programação *Visual C++ 6.0*.

A seguir será apresentada uma demonstração do sistema desenvolvido. A Figura C.1 ilustra a tela principal do protótipo.

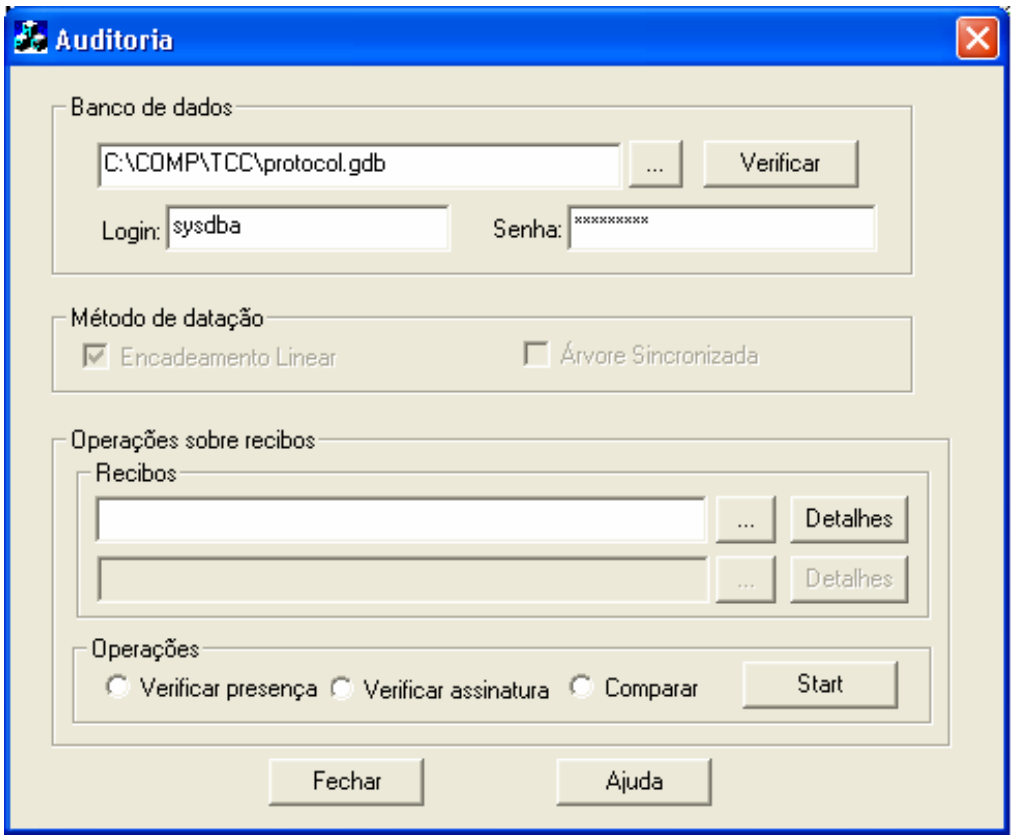


Figura C.1: Tela principal do sistema de auditoria

C.2.1 Verificação da validade de um recibo

Para visualizar os detalhes do recibo, o usuário deve, primeiramente, selecionar o banco de dados que contém o encadeamento e selecionar o arquivo que contém o recibo a ser auditado. Após selecionar o recibo, o usuário pode visualizar seus detalhes, como a data e hora da protocolação (campo *genTime*). Todos estes campos estão descritos na RFC 3161 (ADAMS, 2001). A Figura C.2 ilustra uma tela com as informações detalhadas de um recibo.

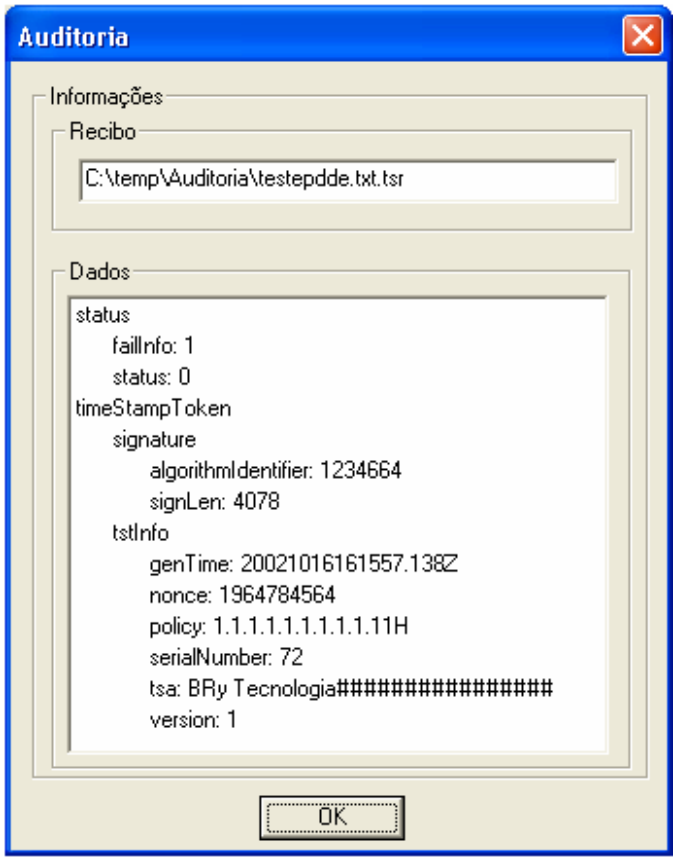


Figura C.2: Detalhes do recibo

Para verificar a validade do recibo, o usuário deve, após selecionar o arquivo que contém o recibo, clicar na opção "Verificar assinatura"e em seguida em "Start". Nesse momento, a assinatura digital da AD sobre o recibo estará sendo verificada. Após isso, o usuário deve clicar na opção "Verificar presença"e em seguida em "Start". Esta

ação fará com que uma pesquisa pelo recibo seja realizada.

C.2.2 Verificação da precedência entre dois documentos protocolados pela mesma AD

Para verificar entre dois recibos, qual foi protocolado primeiro, o usuário deve, após selecionar o banco de dados que contém o encadeamento, selecionar os dois recibos a serem comparados. Após isto, o usuário deve selecionar a opção "Comparar"e em seguida, clicar na opção "Start". O sistema irá verificar se os dois recibos estão presentes no encadeamento e informará qual deles foi protocolado primeiro, baseado na ordem temporal mantida no encadeamento.

C.2.3 Verificação da integridade do encadeamento armazenado no banco de dados da AD

O usuário deve selecionar o arquivo correspondente ao banco de dados que contém o encadeamento a ser auditado. Em seguida, deve preencher os campos *login* e senha, para que se autenticar perante o sistema. A opção "Verificar", permite que o usuário verifique a integridade do encadeamento. O sistema irá re-calcular todos os *links* que constituem o encadeamento e compará-los com os *links* armazenados no banco de dados.

C.3 Considerações

Este capítulo apresentou as funcionalidades oferecidas pelo protótipo de um sistema de auditoria de Autoridades de Datação desenvolvido no LabSEC. O sistema desenvolvido faz parte de um Trabalho de Conclusão de Curso e tem como objetivo oferecer um protótipo com código fonte livre, que implemente os procedimentos de auditoria para o Método do Encadeamento Linear propostos neste trabalho.

Apêndice D

Publicações

Dentre os resultados deste trabalho está a publicação de dois artigos científicos. O primeiro artigo, entitulado "Protocolação digital de documentos eletrônicos"(COSTA, 2003b), foi publicado no I Forum sobre Segurança, Privacidade e Certificação Digital. O segundo artigo, cujo título é "Confiança na tempestividade dos documentos eletrônicos: auditoria da protocolação digital"(COSTA, 2003a), foi publicado no 5^o Simpósio Segurança em Informática e foi premiado como segundo melhor artigo científico, recebendo o Prêmio Tércio Pacitti - Siemens - Menção honrosa.